Intelligence and Security Committee of Parliament

Report on the intelligence relating to the murder of Fusilier Lee Rigby

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

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

Ordered by the House of Commons to be printed on 25 November 2014

HC 795

This publication is available at
www.gov.uk/government/publications

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

Print ISBN 9781474112499

Web ISBN 9781474112505

Printed in the UK by the Williams Lea Group

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

ID: 20111405 11/14

Printed on paper containing 75% recycled fibre content minimum.

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

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

The Rt. Hon. Hazel Blears, MP
The Rt. Hon. Lord Butler KG GCB CVO
The Rt. Hon. Sir Menzies Campbell CH CBE QC, MP
The Rt. Hon. Paul Goggins, MP (until January 2014)
Ms Fiona Mactaggart, MP (from May 2014)
Mr Mark Field, MP
The Rt. Hon. George Howarth, MP
Dr Julian Lewis, MP
The Most Hon. The Marquess of Lothian QC PC

The Intelligence and Security Committee of Parliament (ISC) is a statutory committee of Parliament that has responsibility for oversight of the UK intelligence community. The Committee was originally established by the Intelligence Services Act 1994, and has recently been reformed, 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[1] of the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (GCHQ). The Committee also scrutinises the work of other parts of the UK intelligence community, including the Joint Intelligence Organisation and the National Security Secretariat in the Cabinet Office; Defence Intelligence in the Ministry of Defence; and the Office for Security and Counter-Terrorism in the Home Office.

The Committee consists of nine Members drawn from both Houses of Parliament. The Chair is elected by its Members. The Members of the Committee are subject to section 1(1)(b) of the Official Secrets Act 1989 and are routinely given access to highly classified material in carrying out their duties.

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

The Committee produces an Annual Report on the discharge of its functions. The Committee may also produce Reports on specific investigations. Prior to the Committee publishing its Reports, sensitive material that would damage national security is blanked out ('redacted'). This is indicated by *** in the text. The intelligence and security Agencies may request the redaction of material in a 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 a 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.

[1] *Subject to the criteria set out in section 2 of the Justice and Security Act 2013.*

CONTENTS

INTRODUCTION

1. On 22 May 2013, Fusilier Lee Rigby of the Royal Regiment of Fusiliers was brutally attacked and killed in Artillery Place, Woolwich. This was a tragic loss of a loving father and dedicated soldier who served his country with distinction.

2. Michael Adebolajo and Michael Adebowale were arrested at the scene of the attack and were subsequently convicted of his murder on 19 December 2013. On 26 February 2014, Adebolajo was sentenced to a whole-life term and Adebowale was sentenced to a minimum of 45 years.

THE ATTACK

- On 22 May 2013, Fusilier Rigby had been working at the Army recruiting office at the Tower of London. Having finished his shift, Fusilier Rigby left work to return to his accommodation at the Royal Artillery Barracks in Woolwich.
- At approximately 13:00 the attackers left Adebolajo's address in Lewisham, driving a blue Vauxhall Tigra towards Woolwich. They had an unloaded gun, a meat cleaver and several knives. At 13:30 their car was recorded on closed circuit television driving in the vicinity of Woolwich Barracks.
- At approximately 14:10 Fusilier Rigby arrived at Woolwich Arsenal station. From here, he walked along Wellington Street, crossing John Wilson Street before entering Artillery Place. At approximately 14:20 he crossed Artillery Road. Adebolajo drove directly at Fusilier Rigby, hitting him from behind at a speed of between 30 and 40 miles per hour.
- Following the collision, the car crashed into a signpost and came to a halt. Adebolajo and Adebowale then got out of the car and attacked Fusilier Rigby with knives, before dragging his body to the middle of the road. Adebolajo and Adebowale made several statements to members of the public, attempting to 'justify' their attack, and warning them to stay back when the police arrived.
- At 14:29 unarmed police arrived at the scene and set up a cordon, remaining behind it until 14:34 when armed police arrived and approached the attackers. Adebolajo and Adebowale rushed at the police, brandishing a knife and a gun respectively. Both were shot and subsequently arrested.

The Committee's Inquiry

3. Immediately following the attack, the intelligence community and the police launched an investigation into the two attackers. The priority was to establish whether they were part of a larger network and to assess the risk of further, connected attacks. The longer term task was to establish what knowledge the intelligence community had (or might have had) of the two men before the attack and, crucially, whether the attack could have been prevented.

4. It is greatly to the Agencies' credit that they have protected the UK from a number of terrorist plots in recent years (one or two serious plots each year have been disrupted), and we recognise the excellent work that they do on our behalf. Nevertheless, when there

is a terrorist attack it is essential that there is a thorough investigation to establish whether mistakes have been made and to ensure that any lessons are learned. The Intelligence and Security Committee of Parliament has investigated these issues.

5. The ISC received the results of the Agencies' internal inquiries relating to the two men in August 2013. Since then we have taken evidence from the Security Service (MI5),[2] the Government Communications Headquarters (GCHQ) and the Secret Intelligence Service (SIS). We have also taken evidence from the Metropolitan Police Service and from Ministers. We have considered the large volume of primary material relating to the case that we received from the three Agencies and the police. This comprised hundreds of highly classified documents, including the Agencies' corporate investigative records, file notes, emails and other intelligence reports.[3] In seeking to provide the Committee with all the available evidence, the Agencies have conducted the same level of search that they would do for proceedings in the law courts. This is the first time that this Committee has had such support from the Agencies and we recognise the considerable work that has gone into it.

6. This Report contains an unprecedented amount of detail about the way that MI5, SIS and GCHQ work. It is important that as much of this detail as possible is placed in the public domain. However, there are some matters which we cannot include in a public report, since to do so would either be illegal or would severely damage the Agencies' ability to protect the UK. In some cases the consequences are clear. For example:

- Any material which relates to the interception of communications cannot be published since under the Regulation of Investigatory Powers Act it is illegal to publish any information relating to the interception of communications.
- Any material which relates to a member of the public who is providing the Agencies with intelligence (an 'agent') cannot be published since to do so may endanger that individual's life. It would also make it less likely that other members of the public will come forward if they do not believe that the intelligence they provide will be treated in confidence or if they fear that they or their families will end up in danger. In order to achieve this level of protection and assurance, the principle of 'no comment' must extend to any and all aspects of MI5's work with agents, including neither confirming nor denying whether any individual was an agent or was approached to be an agent.

7. There are other categories of information where the Agencies have told the Committee that they consider that the disclosure of that material would damage their capabilities. The Committee has considered these on a case-by-case basis, taking into account the public interest in revealing the information and the public interest in protecting the country, before reaching a decision as to where the balance lies. For example:

- In certain cases, to publish material which relates to how the Agencies conduct operations would reveal techniques to those who seek to harm the UK. They could then change their behaviour to avoid detection.
- In other cases intelligence has been provided by an overseas agency. In these cases they 'own' the information and it is not the UK's to disclose without their

[2] *For ease, this Report refers to the Security Service as MI5 throughout.*

[3] *Under the Justice and Security Act 2013, the Committee has the right to consider operational material.*

permission. Were we to do so, that would be a clear breach of the terms of the contract under which it was provided. The UK would not be a 'trusted partner' in future – given the global nature of the threat we face, and the importance of every piece of intelligence, that would place the UK in even greater danger. For this Report, permission has been sought on a case-by-case basis and we are grateful to those agencies which have agreed to the publication of their information.

In each individual case it has been a difficult decision to reach. The Committee is conscious that it is the only body that can investigate intelligence matters on behalf of Parliament and the public. The responsibility is considerable and we therefore have sought in every instance to ensure that we are able to disclose as many of the facts as possible.

8. Whilst we have not been able to publish every piece of information that we have considered during our Inquiry, there are two points worth noting:

(i) No material has been redacted to avoid embarrassment to individuals or organisations.

(ii) None of the material redacted affects the substance of this Report in any way.[4]

[4] *Names of individuals, operations and projects have been replaced throughout to ensure anonymity and protect ongoing operations (to ensure the report remains readable, we have used the NATO phonetic alphabet for individuals; the names of trees for operations; and the names of rivers for projects).*

COULD IT HAVE BEEN PREVENTED?

9. In investigating what the Agencies knew about Michael Adebolajo and Michael Adebowale prior to the murder of Fusilier Lee Rigby, our priority has been to establish whether the attack could have been prevented.

10. We have examined, in very considerable detail, the decisions the Agencies made and the actions they took in the seven Agency operations in which either Adebolajo or Adebowale featured. We have discovered a number of errors, and this Report therefore contains criticisms where processes have not been followed or decisions have not been recorded. That, in itself, may not be surprising: any in-depth inquiry, with the benefit of time and hindsight, is always likely to reveal opportunities for improvement, particularly in an organisation such as MI5 where staff operate under significant pressure. However, what we have been seeking to determine is whether they would have made a difference, and what might have prevented the murder of Fusilier Lee Rigby. Based on the evidence we have seen, we do not consider that any of the Agencies' errors, when taken individually, were significant enough to have affected the outcome.

11. One event that gave us cause for concern was the delay in submitting an application for further intrusive techniques against Adebowale. If the application had not taken nearly twice as long as it should have – coincidentally, being sent to the Home Office only the day before the murder itself – MI5 would probably have had intrusive coverage of Adebowale in place during the days before, and on the day of, the attack. Nevertheless, from everything we have learned – in particular about both men's security awareness – we consider it improbable that any coverage would have revealed anything that might have helped prevent the attack on 22 May 2013. Retrospective analysis of Adebowale's communications supports our conclusion.

12. Whilst we have concluded that the errors identified would not, individually, have affected the outcome, we have also considered whether there was a cumulative effect – i.e. whether, taken together, they might have made a difference. We do know that they would have led to different investigative decisions. However, it is impossible to conclude that those changes – all dependent on one another – would have resulted in MI5 discovering evidence of attack planning. We do not consider that, given what the Agencies knew at the time, they were in a position to prevent the murder of Fusilier Lee Rigby.

13. We have also examined whether the Agencies should have known more at the time: i.e. whether they should have undertaken more intrusive action in order to discover more about the two men and their intentions. There were several occasions during our Inquiry when we were surprised that MI5 did not at those specific times place one or other of the men under surveillance or increase their coverage of them. However, on each occasion MI5 has said that they did not have sufficient cause to obtain authorisation for such actions: in order to take intrusive action they must meet the rigorous threshold set down in law, and be able to demonstrate that the action is both necessary and proportionate, in order to gain approval from the Home Secretary. These points demonstrate how high the threshold for intrusive action is in practice.

14. There are those who feel that the intelligence and security Agencies have too much power to intrude into an individual's privacy. However, when a terrorist attack happens, the question often asked is why the Agencies did not do more to prevent it. The balance

between these two concerns is one that we are considering further in our separate inquiry into privacy and security issues.

---

15. Our examination of the investigations into both Adebowale and Adebolajo has highlighted some of the broader issues around the handling of such investigations. We have identified a number of processes that require improvement, as well as evidence that MI5's and SIS's traditional attitudes and preferred approaches would benefit from re-examination. The Agencies must ensure that these lessons are learned.

16. In particular, we note the following eight issues:

(i) **Low priority operations**: MI5 has limited resources, and must continuously prioritise its investigations in order to allocate those resources. The majority of the investigations into Adebowale were low priority, based on the intelligence about him known at the time. As a result they suffered very significant delays (longer even than the average). The length of time taken in such investigations is unacceptable: MI5 must be able to progress low priority casework even when running high priority investigations.

(ii) **Recurring Subjects of Interest**: MI5 does not currently have a strategy for dealing with individuals such as Adebolajo who occur on the periphery of a number of investigations which are primarily directed at other Subjects of Interest. Investigative action must be necessary and proportionate, and an individual must have demonstrated behaviour or intent which poses a threat to national security. However, MI5 must nevertheless give some weight to the cumulative effect of an individual's 'history' where they have appeared on their radar in connection with numerous operations, since that in itself is of significance.

(iii) **The emerging threat from 'self-starting terrorists'**: In addition to the more complex plots directed by Al Qaeda, there is now an increasing threat from 'self-starting terrorists' – those who may be in contact with other extremists, but who are not tasked by Al Qaeda or other terrorist organisations. Identifying such individuals is difficult and poses a very real challenge for MI5. Their prioritisation system must be flexible enough to deal with individuals and not just networks, as has traditionally been the case.

(iv) **Increasing security consciousness**: It is clear that MI5 put considerable effort into establishing the risk that Adebolajo posed, as is right for a Subject of Interest in a Priority 1 investigation. However, this case clearly highlights the difficulties MI5 faces when investigating an individual who is determined to hide their intentions. Even with the benefit of post-event analysis, the Agencies have not discovered how Adebowale and Adebolajo communicated with each other to plan the attack. The Agencies will need to focus on developing new investigative methods as their targets become increasingly security conscious.

(v) **Intelligence at a local level**: Given the challenge of identifying 'self-starting terrorists', particularly those who are security conscious, MI5 will become increasingly reliant on intelligence from local communities. Given the importance of such intelligence, they will need to give further thought to working with the police to increase community engagement.

(vi) **Managing low level Subjects of Interest**: While MI5 focuses primarily on the highest priority individuals, there has not been an effective process in place to manage the large group of individuals who may also pose a risk to national security, but who are not under active investigation. Previous programmes run by MI5 and the police have failed and lessons must be learned from those failures if the latest initiative is to be any more successful.

(vii) **Radicalisation and *Prevent***: We have referred in our Report to the fact that *Prevent* programmes, from what we have seen, have not been given sufficient priority as a means of tackling the problem of those attracted by radical Islamist and terrorist ideologies. We have the impression that this mirrors the relatively low priority (and funding) given to *Prevent* in the CONTEST programme as a whole. This misses the value that *Prevent* can offer: successfully diverting individuals from the radicalisation path could have the single biggest impact on the rest of the CONTEST programme.

We have seen in recent months the numbers of young British men and women who have travelled to Syria and Iraq to engage in terrorism, driven by a warped understanding of Islam. The scale of the problem indicates that the Government's counter-radicalisation programmes are not working. Such programmes, and indeed the *Prevent* agenda more widely, do not form part of this Committee's core oversight remit. Responsibility for them lies with the Home Office and the Department for Communities and Local Government and therefore oversight is rightly the responsibility of the Home Affairs and Communities Select Committees. Nevertheless, from our work on this Inquiry, we are concerned that this issue does not appear to have received adequate scrutiny, far less the prioritisation it deserves. We would therefore strongly urge our colleagues on the relevant Select Committees to consider the problem of countering radicalisation and extreme Islamist ideology as a matter of urgency. This is overwhelmingly in the public interest given the threat our country currently faces.

(viii) **Jihadi tourism**: SIS has responsibility for disrupting the link between UK extremists and terrorist organisations overseas. They will also often have the lead when a British national is detained overseas on a terrorism-related matter. From our examination of their actions in relation to Adebolajo's detention overseas, we concluded that they should have been considerably more proactive in their approach.

Again, events over the last few months have shown this issue to be of critical importance. Hundreds of British citizens have sought to do the same and travel abroad to try to join a terrorist organisation. There were three areas where the Agencies failed in their response to Adebolajo's case: SIS's handling of his allegations of mistreatment; SIS's consideration of deportation or voluntary departure as providing a satisfactory resolution to a case of a UK citizen believed to be attempting to join a terrorist organisation overseas; and the lack of priority accorded to him upon his return to the UK by both MI5 and SIS. Recent events relating to British citizens fighting with terrorist groups in the Middle East and elsewhere have reinforced our very significant concerns in this regard.

---

17. Whilst our primary concern throughout the Inquiry was whether the Agencies acted appropriately given what they knew at the time, we have also considered material that has come to light after the attack. We have found only one issue which could have been decisive. This was the exchange – not seen until after the attack – between Adebowale and an individual overseas (FOXTROT) in December 2012. In this exchange, Adebowale told FOXTROT that he intended to murder a soldier. Had MI5 had access to this exchange, their investigation into Adebowale would have become a top priority. It is difficult to speculate on the outcome but there is a significant possibility that MI5 would then have been able to prevent the attack.

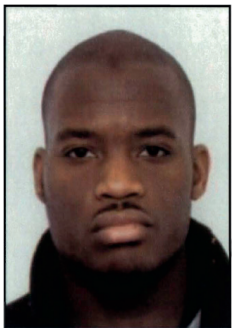
18. Given how significant this exchange could have proved, we have examined whether MI5 could have obtained access to it before the attack – had they had cause to do so (Adebowale was not under active investigation at the time the exchange took place). We consider it highly unlikely that the Agencies could have obtained it on their own. It would have required a particular chain of events: if GCHQ had issued the report linking an unknown individual (later identified as Adebowale) to another Subject of Interest (CHARLIE), or if MI5 had discovered Adebowale's contact with another individual (ECHO), then MI5 might have sought to increase their intrusive coverage of Adebowale sooner. However, even then there may have been only a very slim chance that MI5 would have had sight of the FOXTROT exchange.

19. The party which could have made a difference was the company on whose platform the exchange took place. However, this company does not appear to regard itself as under any obligation to ensure that its systems identify such exchanges, or to take action or notify the authorities when its communications services appear to be used by terrorists. There is therefore a risk that, however unintentionally, it provides a safe haven for terrorists to communicate within.

20. We have looked at this issue more broadly and discovered that none of the major US Communications Service Providers (CSPs) regard themselves as compelled to comply with UK warrants obtained under the Regulation of Investigatory Powers Act 2000 (RIPA). As a result, even had MI5 had reason to seek information under a RIPA warrant, the company concerned might not have responded (we note that overseas CSPs can provide information where there is an immediate threat to life; however, this does not help the Agencies when trying to establish what threat an individual may pose). This is an issue of great concern and we have considered in this Report the policy implications, legal and moral obligations, and what might be done to prevent a similar situation arising in the future. Whilst we note that progress has started to be made on this issue, with the Data Retention and Investigatory Powers Act 2014 and the appointment of the Special Envoy on intelligence and law enforcement data sharing, the problem is acute. The Prime Minister, with the National Security Council, should prioritise this issue.

21. The murder of Fusilier Lee Rigby was first and foremost a great personal tragedy for his family, and our thoughts are with them. In this Report we conclude that, while there are important lessons to be learned by the Agencies and Government, action is also necessary by the CSPs if the safety of the public is to be assured.

MICHAEL ADEBOLAJO



Name:	Michael Olumide Adebolajo
Nationality:	British
Date of birth:	10 December 1984
Convictions:	Various, including assault, possession of an air weapon and bail offences, 2008.
Role in the attack:	Convicted of the murder of Lee Rigby (cleared of attempted murder of police officers). Sentenced to a whole-life term.

Michael Adebolajo was investigated by MI5 on five separate occasions:

Operation ASH (Priority 1A) from May to September 2008: Network thought to have acquired items that could be used for terrorist purposes. Adebolajo in contact with members of the network.

Operation BEECH (Priority 3) from April to June 2011: Investigation focussing solely on Adebolajo (involvement in extremist activity and attempts to travel overseas).

Operation CEDAR (Priority 1B) from June to September 2011: Possible Al Qaeda in the Arabian Peninsula (AQAP) attack planning against the West. (Adebolajo a key contact.)

Operation DOGWOOD (Priority 1B; then Priority 2M) from September 2011 to November 2012: Continuing CEDAR investigation but focussing on two individuals (with whom Adebolajo was in contact).

Operation ELM (Priority 2H) from November 2012 up until the attack: Investigation into an associate of Adebolajo.

OPERATION ASH: FIRST IDENTIFICATION OF ADEBOLAJO

22. MI5's investigation into Michael Olumide Adebolajo spanned a number of years, from mid-2008 up until the murder of Fusilier Lee Rigby in May 2013. During this time he was investigated under five different MI5 operations.

23. Adebolajo first came to MI5's attention under Operation *** (hereafter referred to as Operation ASH) in mid-2008. This was a Priority 1A investigation into the activities of a Subject of Interest (SoI) named *** (hereafter referred to as SoI ALPHA), who was thought to have acquired items that could be used for terrorist purposes, and who had previously met members of Al Qaeda Core.[5]

MI5'S PRIORITISATION OF OPERATIONS

MI5 prioritise investigations according to the risk they carry. The priority level can change during the course of an investigation if MI5 detects any change in the risk.

There are four broad categories of priority for investigations:

- Priority 1 (P1a and P1b) is the highest, where there is intelligence to suggest attack planning.
- Priority 2 (P2H and P2M) is used where there is intelligence to suggest high or medium risk activity such as terrorist training.
- Priority 3 (P3) is assigned to investigations into uncorroborated intelligence.
- Priority 4 (P4) is used to investigate individuals where there is a risk of re-engagement with extremist activity.

Subjects of Interest to MI5

An SoI *"is an individual who is being investigated because they are suspected of being a threat to national security"*.[6] In addition to the overall investigation or network being prioritised, every SoI within that investigation or network is also prioritised.

SoIs are placed in Tiers (Tier 1, Tier 2 or Tier 3) to reflect their position and importance within an investigation. The three tiers are defined as:

- *Tier 1: Main targets of an investigation – targets will likely be involved in all aspects of the activities under investigation.*
- *Tier 2: Key contacts of the main targets – targets will likely be involved in a significant portion of the activities under investigation.*

[5] *Al Qaeda Core refers to the few hundred operatives in the Federally Administered Tribal Areas (FATA) of Pakistan and, occasionally, in Afghanistan, including the group's senior leadership (ISC Annual Report 2012–2013, page 6).*

[6] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

- *Tier 3: Contact of Tier 1 and Tier 2 targets – targets will likely be involved in only marginal aspects of the activities under investigation.*[7]

As of October 2014, MI5 was investigating several thousand individual SoIs who are linked to Islamist extremist activity in the UK.[8]

24. One of SoI ALPHA's close associates was an SoI named ***, who MI5 was investigating in order to determine how involved he was in SoI ALPHA's activities. In *** 2008, this individual organised an event assessed to have an extremist agenda. MI5 therefore sought to identify the individuals planning to attend the event and, in doing so, identified Adebolajo.[9] ***.

***

***.

***.[10, 11]

***.

25. After Adebolajo had been identified under Operation ASH, MI5 created a Corporate Investigative Record. This is the first step when an individual is designated an SoI. MI5 has told us that Corporate Investigative Records are used:

> *… in order to create a centrally retrievable summary of the intelligence held on an individual and to require the investigator to outline why any further intrusive enquiries are necessary and proportionate.*[12]

26. MI5 conducted enquiries with the police to establish whether they held any information on Adebolajo. The police response revealed that Adebolajo had been arrested in 2006 with a criminal associate, Ibrahim Hassan,[13] during a protest against the publication of cartoons perceived as insulting to the Prophet Mohammed. Adebolajo had also been arrested in 2007 under the Firearms Act (for carrying CS spray), and had previous arrests for assault.

27. In July 2008, MI5 created an 'Intelligence Summary' on Adebolajo. This summarised all known intelligence, including his basic details, police traces and MI5's current coverage. The summary contained three recommendations for future action:

---

7 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

8 *Written Evidence – MI5, 3 October 2014.*

9 *MI5 describes an individual as being fully identified when they have confirmed their full name, nationality and date of birth (MI5 Letter to the Committee – Interim Report, 28 June 2013).*

10 *Oral Evidence – MI5, 17 October 2013.*

11 *Oral Evidence – MI5, 17 October 2013.*

12 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

13 *Police records show that Adebolajo and Hassan associated with each other when they were both teenagers (as far as MI5 is aware, prior to either being involved in Islamist extremist activity). They maintained infrequent contact between 2006 and 2012, including Adebolajo visiting Hassan whilst he was in prison for terrorism offences in 2008–09. Shortly after the Woolwich attack, Hassan was interviewed by BBC Newsnight, in which he claimed that Adebolajo had been harassed by MI5. Immediately after appearing on BBC Newsnight, Hassan was arrested for offences under terrorism legislation (unrelated to the attack in Woolwich). He has since pleaded guilty to charges of encouraging terrorism and disseminating terrorist material, and has been sentenced to three years in prison. ***.*

(i) Acquire current call-related data on Adebolajo's telephones.

(ii) Attempt to identify a current home address for Adebolajo.

(iii) Attempt to identify Adebolajo's digital footprint.

28. However, the Committee's investigation discovered that the recommendations put forward by the desk officer were not carried out by the investigative team. The Committee questioned MI5 about this and they explained:

> *Shortly after this summary was written, the threat from* [SoI ALPHA and his associates] *increased significantly and the available resource was prioritised to those SOIs who posed the greatest threat… Adebolajo was not judged to be centrally involved in this activity.*[14]

29. The Committee questioned the Director General about the implications of this decision not to carry out the recommended actions. The Director General said that even if these recommendations had been carried out, "*it would have made no substantial difference*"[15] to later decisions regarding Adebolajo's case.

A. Adebolajo first came to MI5's attention through his association with other Subjects of Interest and his attendance at an event assessed to have an extremist agenda. We accept MI5's assessment that attendance at such events is relatively common. We would therefore not have expected MI5 to place an individual under intrusive surveillance purely on the basis of attendance at such an event.

B. Nevertheless, MI5 must take some action to assess individuals who attend such events in order to ascertain whether they pose a threat to national security, in which case more intrusive investigation would be justified. In the case of Adebolajo there were three recommended actions which were not carried out. The Committee, following the Director General's assessment, accepts that this may not have made any substantial difference in Adebolajo's case. However, the Committee considers that, where actions were recommended, they should have been carried out. If the investigative team had good reason not to carry out a recommended action, then this should have been formally recorded, together with the basis for that decision. We expect MI5 to rectify their procedures in this respect.

---

[14] *Written Evidence – MI5, 3 October 2013.*

[15] *Oral Evidence – MI5, 17 October 2013.*

OPERATION ASH: PROSCRIBED ORGANISATIONS

30. Under Operation ASH, MI5 cross-referenced Adebolajo's telephone number against call data that they held on other SoIs.[16] This established that Adebolajo's mobile phone had been in contact with SoIs in relation to Al Ghurabaa events. These contacts dated back to 2005.

31. Al Ghurabaa is one of the many iterations of the more commonly known Al Muhajiroun, a radical group with the objective of introducing Islamic law in the UK. Al Ghurabaa was proscribed in 2006.

PROSCRIBED ORGANISATIONS

Under the Terrorism Act 2000, the Home Secretary may proscribe an organisation *"if she believes it is concerned in terrorism. For the purposes of the Act, this means that the organisation:*

- *Commits or participates in acts of terrorism;*
- *Prepares for terrorism;*
- *Promotes or encourages terrorism (including the unlawful glorification of terrorism); or*
- *Is otherwise concerned in terrorism.*

Proscription makes it a criminal offence to:

- *Belong to or invite support for a proscribed organisation;*
- *Arrange a meeting in support of a proscribed organisation; and*
- *Wear clothing or carry articles in public which arouse reasonable suspicion that an individual is a member or supporter of the proscribed organisation."*[17]

***.[18]

***.[19] ***.

[16] *This means that, whilst MI5 was not at this time examining the current data from Adebolajo's telephones (e.g. who he was calling) they were able to determine, from cross-referencing his telephone number, that other SoIs had been in contact with Adebolajo's mobile telephone.*

[17] *'Proscribed terrorist organisations', Home Office, December 2013 (www.gov.uk).*

[18] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

[19] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013. The Committee notes the complex distinction between those groups which, whilst espousing 'radical' ideas, do not support participation in violent acts to further those ideas, in comparison with those groups which actively support violent acts to achieve their goals. For example, some groups may state that they disavow violence and consider it to be forbidden by the Sharia; however, they may also use the language of violent jihad, which could encourage others to engage in violent acts.*

32. The Committee asked MI5 whether suspected membership of a proscribed organisation automatically means an individual becomes a Subject of Interest. MI5 responded:

> *Investigations are not automatically triggered based on a particular activity… Should we identify a previously unknown individual as* [a] *member of a proscribed organisation, our investigative response and any consequent allocation of investigative resource would depend on the nature and context of the individual's reported activities. There are no set criteria or checklists for our action.*[20]

33. ***.[21]

34. ***.[22] However, the Committee notes that Al Ghurabaa (as a proscribed organisation) has been found to be *"concerned in terrorism"* and disseminating *"materials that glorify acts of terrorism",*[23] which suggests that its members are likely to pose some form of threat, whether in the UK or elsewhere.

35. After the Committee questioned MI5 as to their position on Al Ghurabaa/Al Muhajiroun, we were subsequently told that their assessment of the group has changed, in part due to Al Muhajiroun's public declaration of its support for the Islamic State of Iraq and the Levant (ISIL). MI5 assesses that this increases the risk posed by individuals affiliated to the group:

> ***.[24]

C. Extremist groups operate within a complex ideological landscape and therefore identifying the threat posed by such groups, and by their individual members, can be difficult. However, the Committee considers that, if there are reasonable grounds to suspect that individuals are members of a proscribed organisation, this should be sufficient to make them a Subject of Interest to MI5 or the police.

36. Given that Adebolajo was linked to Al Ghurabaa, the Committee questioned why the authorities did not pursue charges for membership of a proscribed organisation (a criminal offence under the Terrorism Act 2000). The Metropolitan Police Service (MPS) Assistant Commissioner for Specialist Operations (ACSO) underlined the difficulties in prosecuting such offences: there have been no successful prosecutions for membership of Al Muhajiroun.

37. This raises the question as to why organisations are proscribed if it is not possible to prosecute individuals for membership. The Committee questioned the Assistant Commissioner on this point. She stated that proscribing organisations does *"act as a deterrent"*[25] and that *"there have been some prosecutions in some cases"*.[26] ***.[27]

---

[20] *Written Evidence – MI5, 7 February 2014.*
[21] *Written Evidence – MI5, 5 November 2013.*
[22] *Written Evidence – MI5, 5 November 2013.*
[23] *'Proscribed terrorist organisations', Home Office, December 2013 (www.gov.uk).*
[24] *Written Evidence – MI5, 22 May 2014.*
[25] *Oral Evidence – Metropolitan Police Service, 31 October 2013.*
[26] *Oral Evidence – Metropolitan Police Service, 31 October 2013.*
[27] *Oral Evidence – Metropolitan Police Service, 31 October 2013.*

38. The Home Secretary also recognised the difficulties around proscribed organisations and explained that, as a result:

> *… one of the things the extremism taskforce has been looking at is the question of whether there is something below proscription that we could be doing in relation to groups, banning orders and extra powers in relation to individuals as well.*[28]

D. We are told that it is difficult to prosecute individuals for membership of proscribed organisations. Nevertheless, given the deterrent effect and the value in drawing attention to individuals who hold extremist views, the Committee considers that there is benefit in continuing to proscribe organisations.

E. We welcome the Home Secretary's attempt to find a solution 'below proscription'. This should take into account the differences between the various extremist groups that exist in the UK. However, the Government should first consider, as a matter of urgency, whether the existing legislation could be amended to enable effective prosecutions.

[28] *Oral Evidence – Home Secretary, 21 November 2013.*

OPERATION ASH: CLOSURE

39. In late 2008, Operation ASH was closed because the main SoI had been disrupted.[29] Since he was only a contact of one of SoI ALPHA's associates (himself of diminishing interest by early 2009), MI5 did not pursue active investigation of Adebolajo further.

40. We have considered whether the decision not to pursue Adebolajo further was justified. At this stage, all MI5 knew was that he had been attending extremist events and that he was in contact with other individuals who were members of a proscribed organisation. This would not necessarily meet the level required (in terms of necessity and proportionality) for further investigative action.

'NECESSARY AND PROPORTIONATE'

There are strict limitations on what MI5 is allowed to do when investigating an individual, and MI5 must abide by several legal constraints when considering any action. All action MI5 takes must be considered necessary and proportionate in light of what they know at the time.

For example, MI5 can only use 'intrusive techniques' (such as intercepting telephone communications) against an individual if there is sufficient justification on national security grounds. In addition, a warrant must be obtained which authorises precisely what action will be taken. Such warrants are issued by the Secretary of State and are valid for up to a maximum of six months.[30]

Less intrusive techniques, such as directed surveillance (watching an individual in public), must be authorised through MI5's internal authorisation system. Whilst some criticise the intelligence and security Agencies for being too intrusive, in fact they have a high threshold for justifying investigative action.

41. Whilst we believe the decision to stop investigating Adebolajo at that time was reasonable, the Committee found no formal written record documenting or explaining the decision: we examined the Operation ASH Closure Note[31] (which is undated) and found that there is no mention of Adebolajo whatsoever. This was the second occasion on which we found record-keeping to be inadequate: it is an issue that arose on a number of occasions during our investigation and is covered in more detail at paragraph 184.

Adebolajo on Programme AMAZON

42. One of the actions taken when Operation ASH was closed was to assess whether any of the SoIs should be referred to other programmes. As a result, in October 2008 Adebolajo's details were transferred onto *** (hereafter referred to as Programme AMAZON), a joint national initiative between MI5 and the police which was intended to

[29] *A definition of 'disruption' is at paragraph 132.*
[30] *Although they can be renewed if there is justification to do so.*
[31] *A Closure Note is a formal note documenting the end of an investigation.*

monitor individuals who met certain criteria and *"subscribed to the Al Qaida ideology of global jihad"*.[32] (More detail on Programme AMAZON is included in the next section.)

- In late 2008, Adebolajo was listed (***) on Programme AMAZON because of his links to Operation ASH SoIs.
- Whilst an individual was on Programme AMAZON, their details were regularly cross-checked against police and MI5 databases for new intelligence. MI5 has said that, while Adebolajo was on Programme AMAZON, occasional indirect coverage of him was obtained in early 2009 and 2010 through his contact with another SoI.[33] During the period in which Adebolajo was on Programme AMAZON, he was assessed at regular intervals and his classification varied. There were four categories in Programme AMAZON; more detail is provided in the next section. (***.)[34]

43. The Committee asked how the decisions were reached to change the classification of Adebolajo on Programme AMAZON. The Committee has been told that the decision-making would have been agreed at regular formal meetings, and that the Programme AMAZON database would have been updated to reflect any changes. However, it appears that the meetings which determined Adebolajo's classification and reclassification were not minuted. The Committee asked the Assistant Commissioner about this and she said:

> *… we don't actually have the record of why they decided that, or what they took into account when they were having the meeting at that time. We just don't have that record, I'm afraid.*[35]

44. The Committee notes that, while Adebolajo's inclusion in Programme AMAZON was clearly an attempt to monitor the risk he posed, there was no consideration given to the possibility of Adebolajo being referred to the *Prevent* programme. *Prevent* is one of the four elements of the Government's counter-terrorism strategy and is intended to provide practical help, advice and support to individuals, either to prevent them from being drawn into terrorism or to steer them away from extremist views. We note that in 2008 the *Prevent* programme was in its infancy and intervention activity was limited. Referral to *Prevent* (through the Channel project – more details at paragraph 209) may not therefore have been feasible at this time. However, by 2009 there was a Channel project located in ***, where Adebolajo was thought to be living. Consideration should therefore have been given to this as an option. This is an important issue to which we return later in this Report (at paragraph 220).

---

[32] *Written Evidence – MI5, 10 March 2014.*

[33] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013. ***. (Written Evidence – MI5, 3 October 2013.)*

[34] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013. At this point, the Metropolitan Police Counter-Terrorism Command (SO15) and MI5 also discussed whether to remove Adebolajo from the Programme AMAZON scheme.*

[35] *Oral Evidence – Metropolitan Police Service, 31 October 2013.*

MANAGING LOW LEVEL SUBJECTS OF INTEREST

45. One of the issues that has arisen during the course of the Committee's Inquiry is how MI5 and the police manage 'low level' SoIs – individuals who are not necessarily deemed enough of a security risk to appear in a Priority 1–4 investigation, but in whom MI5 and the police still have an interest. There have been a number of initiatives to manage such individuals, none of which appear to have been entirely successful.

Programme AMAZON (2007–2010)

46. Programme AMAZON[36] was a joint national initiative between MI5 and the police. The Committee was originally told that it was intended to manage low level or peripheral SoIs who fell below the threshold for active P1–4 investigation, but who:

> *… were known or believed to have historically been linked to activities including extremist facilitation, radicalisation or the distribution/possession of extremist media.*[37]

OBJECTIVES OF PROGRAMME AMAZON

The police have told the Committee that, for an individual to be included on Programme AMAZON, they had to meet both the following criteria:

- The individual subscribes to Al Qaeda ideology (either as an individual or part of a group).
- The individual is known or believed to be involved in: attack planning; facilitation of extremist activity; supporting a network; radicalisation; or distribution or possession of extremist material.

Potential new Programme AMAZON subjects were considered at a Casework Review Meeting (CRM), where it was decided: whether the individual met the Programme AMAZON criteria; the risk they posed; a plan to manage the risk; a date for further review of the individual; and an interim 'owner' for the individual, pending subsequent review.

Within London, this process was managed by an SO15 (the MPS Counter Terrorism Command) Programme AMAZON unit, which had *"specific responsibility for allocating subjects for review, interacting with* [MI5] *as part of the review process and managing the CRM process"*.[38]

47. Individuals on Programme AMAZON were assessed through regular reviews of police and MI5 databases for new intelligence. Any intelligence updates were considered at meetings attended by both the police and MI5, and the risk individuals posed was reassessed as appropriate.

---

[36] *The national roll-out of Programme AMAZON (***) began in May 2007, but it was not established within SO15 in London until late 2008.*

[37] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

[38] *Written Evidence – Metropolitan Police Service, 30 August 2013.*

LONDON PROGRAMME AMAZON GRADING

The following categories and definitions were used to grade the risk posed by individuals on Programme AMAZON:

> [Category 1] (***): *The subject is linked to a network, or individual poses a threat to life/property in the UK or overseas, i.e. the individual or network aspires to mount an attack or is seeking weapons and/or training that would enable it to mount an attack.*
>
> [Category 2] (***): *The subject is linked to a network that, or as an individual, is actively involved in extremism* (sic) *but there is no evidence of intention or capability to mount an attack.*
>
> [Category 3] (***): *The subject is or has been linked to extremists or has extremist tendencies but there is no evidence of current activity.*
>
> [Category 4] (***): *Further work is needed to establish what links if any the subject has to extremism.*[39]

48. The Committee was surprised to find that the definitions of Category 1 and Category 2 on Programme AMAZON were similar to those used to describe an SoI under active MI5 investigation. We therefore sought clarification from MI5. Eventually the Committee was told that in fact there was an overlap, as those classified as Category 1 or Category 2 on Programme AMAZON were often also subject to MI5 investigation.[40] The Committee questioned MI5 on the value of an individual being both in Programme AMAZON and a subject of MI5 interest. MI5 told the Committee:

> *As a process* [Programme AMAZON] *was judged by MI5 to add value on understanding those individuals who were peripheral to investigations and posed a lower level of threat. Although* [Programme AMAZON] *not only included those individuals who sat below the threshold for MI5 investigation, as a management tool MI5 saw its value lay in this area.*[41]

49. The police told the Committee that Programme AMAZON was *"deliberately broad to ensure that all those who presented a risk were identified"*.[42] However, they have assured the Committee that *"whilst there may have been an 'overlap' in definition there was no 'overlap' in process"*.[43] Nevertheless, the Committee was also told that Programme AMAZON was brought to an end later in 2010 *"in part due to the complexities caused by the volume of subjects"*.[44] The ACSO said:

---

39 *Written Evidence – Metropolitan Police Service, 30 August 2013.*

40 *Although the Committee notes that in Adebolajo's case he was initially classified as the highest threat on Programme AMAZON, even though MI5's investigation into him had closed.*

41 *Written Evidence – MI5, 10 March 2014.*

42 *Written Evidence – Metropolitan Police Service, 23 April 2014.*

43 *Written Evidence – Metropolitan Police Service, 23 April 2014.*

44 *Written Evidence – Metropolitan Police Service, 30 August 2013. In 2008, SO15 was responsible for 3,131 Programme AMAZON subjects. In July 2010, SO15 was responsible for 893 Programme AMAZON subjects.*

It was, I suppose, decided that it had high aspirations. But where we then had our resources placed, it was not possible to make it work properly.[45]

This suggests that it was the comprehensive nature of the scheme that led to its failure.

50. The Committee was also told that one of the problems with Programme AMAZON was that it had not effectively assessed individuals in their own right:

> [Programme AMAZON] *was very much focused on networks. Although it looked at individuals and made an assessment on individuals, it was their relationship to a network and that network's activity. It is possibly one of the difficulties with* [Programme AMAZON]*, was that focus on the relationship between the individual and the network, and then the network's activity in terrorism-related behaviour; rather than the individual per se and their direct threat.*[46]

This focus on networks, rather than on the threat posed by a particular individual, is an issue we will return to later (paragraph 143).

Programme BELAYA and Programme CONGO (2008–2012)

51. Two comparable projects, *** and *** – hereafter known as Programme BELAYA and Programme CONGO – were created at the same time as Programme AMAZON, in 2008. When Programme AMAZON was brought to an end in 2010, these two projects effectively subsumed Programme AMAZON's role in managing low level SoIs.

(i) Programme BELAYA was intended to generate a better understanding of local issues[47] through a focus on 'People' and 'Places'. However, again, Programme BELAYA *"did not achieve its objectives"*.[48] In particular, *"it was found lacking in formal structures or processes to generate a product which resulted in action"*.[49] It also encountered similar problems with the number of individuals the scheme was intended to manage, and therefore did not develop much beyond an intelligence database.

(ii) Programme CONGO was developed to build upon the 'People' strand of Programme BELAYA, to identify individuals of emerging risk. It also sought to manage individuals falling below the threshold for full investigation, but for whom some form of ongoing assessment was required.[50] However, SO15 found that *"the volume of individuals that met the* [Programme CONGO] *criteria was too great to apply the process effectively"*.[51]

52. Both Programme BELAYA and Programme CONGO were formally suspended in the months leading up to the Olympics (although the police have been unable to provide the Committee with the precise date of when this occurred). They remained suspended whilst a new scheme, *** – hereafter known as Programme DANUBE – was developed.

---

45 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*
46 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*
47 *Written Evidence – MI5, 10 January 2014. (***.)*
48 *Written Evidence – Metropolitan Police Service, 30 August 2013.*
49 *Written Evidence – Metropolitan Police Service, 30 August 2013.*
50 *Written Evidence – Metropolitan Police Service, 30 August 2013.*
51 *Written Evidence – Metropolitan Police Service, 10 December 2013.*

This meant that from the period leading up to the Olympics until late 2013 there was no scheme in place to manage low level SoIs.

Programme DANUBE (2013 – present)

53. DANUBE is a national programme, developed jointly by the police and MI5. It began operating in late 2013. The Committee has been told that the process will consist of three different elements, which provide a "*more holistic view of risk"*:

> ***.[52]

54. The Committee has been told that *"the new jointly owned* [DANUBE] *process has evolved in recognition that earlier initiatives did not adequately manage the risk from peripheral SoIs"*.[53] The Committee questioned the Assistant Commissioner as to why she thought this new process would be more successful than its predecessors. The Assistant Commissioner gave several reasons, including greater resourcing, closer partnership working and national coverage. She said:

> *It will give us a much better picture overall of where all the threat and risk is, which is agreed between us both* [the police and MI5].[54]

55. It is worth noting that Programme AMAZON was also a joint, national initiative; it therefore remains unclear to the Committee how the Programme DANUBE process will be an improvement on Programme AMAZON, beyond the additional resources. Furthermore, this is not a new issue; in the Committee's Report into the London terrorist attacks on 7 July 2005, the Committee noted the importance of understanding radicalisation at the local level. Given the difficulties experienced by the previous schemes, Programme DANUBE should have been designed specifically to address those failures: we are not yet convinced that this is the case.

F. Clearly, MI5 must focus primarily on the highest priority individuals. However, that leaves a large group of individuals who may also pose a risk to national security, but who are not under active investigation. Previous attempts by MI5 and the police to manage this group have failed: we have not yet seen any evidence that the new programme, established in late 2013, will be any better. This is an important issue and the Committee will continue to take a close interest in it in order to ensure that the necessary improvements are made.

---

[52] *Written Evidence – Metropolitan Police Service, 30 August 2013.*

[53] *Written Evidence – MI5, 10 March 2014.*

[54] *Oral Evidence – Metropolitan Police Service, 31 October 2013.*

ADEBOLAJO'S ARREST IN KENYA

56. By November 2010, Adebolajo had been assessed to be of only low level interest for a number of months. However, on 22 November 2010, the Kenyan police reported to the MPS officer based in Nairobi[55] that they had arrested Adebolajo the previous day. He had been arrested with a group of five Kenyan youths and was assessed to have been attempting to travel into Somalia to join Al Shabaab (a Somalia-based terrorist group).[56]

57. The MPS officer (Counter-Terrorism and Extremism Liaison Officer – CTELO) informed the SIS East Africa representative[57] and both SIS and MI5 in London were notified of Adebolajo's arrest and detention. Prior to this, SIS and MI5 had been unaware that Adebolajo had travelled to Kenya.[58]

58. However, during its Inquiry, the Committee discovered within the primary material references which indicated that relevant information might have been available to the Agencies prior to Adebolajo's arrest in Kenya. The first of these references was contained within an MI5 File Note of May 2011 and was based on information obtained by SIS after Adebolajo's arrest. [59] ***.

***.[60]

59. ***.

***

***.

***.[61]

60. The second reference that the Committee discovered in the primary material was a police document which stated that the CTELO had knowledge of potentially relevant information before Adebolajo's arrest: he had become aware a week beforehand that ***.[62] We asked the police whether this information was the same as the information referred to in the MI5 File Note from May 2011. However, it has proved difficult to unravel whether these two documents are referring to the same information, when the information was received and from whom.

- When we asked the police where the information had come from, they told us: *"The* [reporting] *was not received by the CTELO, but was believed to have been passed to* [an SIS East Africa representative]… *The existence of this* [reporting], *although held by SIS, was shared knowledge..."*[63]

[55] *The MPS officer is known as the Counter-Terrorism and Extremism Liaison Officer (CTELO). They are primarily responsible for police-to-police engagement within a particular country.*
[56] *Written Evidence – MI5, 30 August 2013.*
[57] ***.
[58] *Adebolajo's overseas travel was not being monitored, as such intrusive action would not have been justified based on the available intelligence.*
[59] *Primary Material (Adebolajo), MI5, 3 May 2011.*
[60] *Oral Evidence – SIS, 24 October 2013.*
[61] ***.
[62] *Primary Material (Adebolajo), Metropolitan Police Service, 19 November 2010 (sic).*
[63] *Written Evidence – Metropolitan Police Service, 10 December 2013.*

- However, this does not correspond with SIS's version of events. SIS told the Committee that they received the information from the CTELO. They also said that they only received it two days after Adebolajo was arrested: SIS stated that the first they knew of a British national in Kenya was when they were informed of Adebolajo's arrest on 22 November.

- The Committee was concerned at the discrepancy between the evidence from the police and SIS, as both organisations seemed to be suggesting that they had received this information from the other. We further questioned SIS as to their recollection. SIS responded that: *"Additional searches initiated by SIS in London and* [regionally] *have again returned no documents to indicate that* [prior to Adebolajo's arrest] *SIS was aware of any* [information] *relating to* ***."[64]

- They sought to explain the discrepancy: *"Although SIS's results conflict with the account given by the CTELO in the Police report it is possible that information was received by* [an SIS East Africa representative]*, shared with the CTELO but not recorded substantively."*[65]

- We returned to the police, who asked the CTELO for further clarification of his recollection of events. The Committee was told that the officer *"… recalls that he was verbally informed about this information and that it was regarded in the office more as… rumour, rather than corroborated or actionable* [information]*"*.[66]

The only thing that is clear about this information is that it was not documented. SIS has said that it lacked detail and was uncorroborated but, given that it was information that related to a British citizen trying to gain entry to Somalia (a key concern for SIS), we would have expected it to have been recorded at the very least.

G. The Committee is concerned that SIS and the police provided conflicting accounts with regards to information that might have been available to them prior to Adebolajo's arrest. The problem is compounded by the fact that neither SIS nor the police kept adequate records. In any case concerning a British national suspected of involvement in terrorism (whether in the UK or overseas) it is essential that all information – whether corroborated or not – should be properly recorded. That failed to happen on this occasion.

---

64 *Written Evidence – SIS, 14 January 2014.*
65 *Written Evidence – SIS, 14 January 2014.*
66 *Written Evidence – SIS, 14 January 2014.*

SIS INVOLVEMENT: OPERATIONAL LEAD

61. Before investigating SIS's role in the specific case of Adebolajo's arrest in Kenya, it is important to understand SIS's counter-terrorism role overseas:

(i) SIS told the Committee that when a British national is detained in a country such as Kenya on a terrorism-related matter, SIS *"would* [often] *take the operational lead… unless it is considered necessary to deploy an officer… with specialist training/ knowledge"*.[67]

(ii) The Chief explained that SIS has a specific role in relation to 'jihadi tourism'[68]: *"So SIS's responsibility… is to ensure… we disrupt the link between UK extremists and terrorist organisations, and that is our focus."*[69]

(iii) SIS explained that this is a key aspect of their work in relation to Kenya:

One of the main purposes… is to break the link between UK extremists and terror organisations in Somalia; and that is the thrust of [SIS work in relation to Kenya]*… it is right at the centre of our operational preoccupations, as we have said: British citizens travelling to Somalia. ****.[70]

COUNTER-TERRORISM WORK IN RELATION TO KENYA

There are various organisations both in the UK and Kenya that undertake counter-terrorism work in relation to Kenya:

SIS: The main function of SIS activity in relation to Kenya is counter-terrorism work. ***.

Police Counter-Terrorism and Extremism Liaison Officer (CTELO): CTELOs work in close partnership with a range of HMG[71] partners in-country. They are primarily responsible for police-to-police engagement within a particular country. In Kenya, the CTELO is an SO15 Liaison Officer, based in the British High Commission in Nairobi.

Kenyan Police anti-terrorism unit: This unit (***) is the unit responsible for conducting counter-terrorism policing in Kenya. The Committee was initially told that *"SIS does not have direct contact with* [this unit] *but an effective relationship is managed by an SO15 officer (CTELO) based out of the British High Commission in Nairobi"*.[72]

---

67 *Written Evidence – SIS, 19 November 2013.*
68 *One of the threats currently facing the Agencies is from 'jihadi tourism', particularly in relation to Syria and Iraq.*
69 *Oral Evidence – SIS, 24 October 2013.*
70 *Oral Evidence – SIS, 24 October 2013.*
71 *Her Majesty's Government.*
72 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

Kenyan National Intelligence Service (NIS): This is both the domestic and foreign intelligence agency of Kenya. Its mission is to detect and identify any potential threat to Kenya, to advise the President and Government of any security threat to Kenya, and to protect the security interests of Kenya.

***** (hereafter referred to as 'ARCTIC'):** This is a counter-terrorism unit which has a close working relationship with HMG. ARCTIC is covered at paragraph 467 of this Report.

62. However, despite often having the operational lead, during Adebolajo's arrest and detention in Kenya SIS appears to have had very limited involvement:

- SIS was notified of Adebolajo's arrest on 22 November. Adebolajo was a British national who had been arrested on suspicion of trying to travel to Somalia and was assessed to be seeking to join Al Shabaab. SIS therefore reported the issue to their Head Office, who reviewed the information on Adebolajo held by HMG. However, they did not seek to interview Adebolajo, ask to be involved in any interview by the Kenyans, or feed in any questions to be put to him.
- On 23 November 2010, an SIS East Africa representative arranged a meeting with a senior Kenyan police officer (***) to ask about Adebolajo's arrest and detention. During this meeting, SIS asked for assurances about Adebolajo's treatment whilst in detention. The Kenyan police gave these general assurances but noted that Adebolajo had already been interviewed (the previous day).
- SIS did not seek to investigate Adebolajo's case further. Following their meeting with the Kenyan police, there is no record of any further action undertaken by SIS with regards to Adebolajo's arrest and detention.[73]

63. When we questioned SIS as to why they did not take any substantive action in response to Adebolajo's arrest, the Chief acknowledged that their *"involvement was minimal"*[74] but said:

> *… So it is a fairly short space of time and it would not really have merited a huge investigation at that stage, because the Kenyans had it pretty well taped.*[75]

64. SIS's minimal involvement is surprising: Adebolajo had been arrested by the Kenyan police and he was suspected of being a British extremist seeking to join a terrorist organisation in Somalia. Taking SIS's own description of their role (breaking the link between UK extremists and terror organisations in Somalia) and the statement that this link is right at the centre of their operational preoccupations, it is difficult to understand their passive approach to Adebolajo's arrest.

H. SIS has told the Committee that they often take the operational lead when a British national is detained in a country such as Kenya on a terrorism-related matter. They have also told the Committee that they have responsibility for disrupting the link between UK extremists and terrorist organisations overseas, and that in Kenya

---

[73] *Following their meeting with the Kenyan police, SIS representatives ensured that all relevant information on his deportation was passed to Head Office for use on his return to the UK.*

[74] *Oral Evidence – SIS, 5 December 2013.*

[75] *Oral Evidence – SIS, 24 October 2013.*

this is at the centre of their operational preoccupations. The Committee therefore finds SIS's apparent lack of interest in Adebolajo's arrest deeply unsatisfactory: on this occasion, SIS's role in countering 'jihadi tourism' does not appear to have extended to any practical action being taken. SIS must ensure that their procedures are improved so that this does not happen again. This is particularly important given the current challenges faced by the Agencies in countering 'jihadi tourism' in Syria and Iraq.

ADEBOLAJO'S RETURN TO THE UK: OPERATION BEECH

65. We have been told that the specific offence for which Adebolajo was arrested remains unclear. While he had been arrested with a group of five Kenyan youths and was assessed to have been attempting to travel into Somalia to join Al Shabaab, Adebolajo was not convicted of any offences by the Kenyan authorities. A review by SO15 of the Kenyan police files revealed that it had not been possible for the Kenyan police to obtain evidence of a specific terrorist offence. He was placed before a Kenyan court due to a breach of immigration law,[76] but was offered the option of leaving Kenya voluntarily rather than face trial.[77]

66. On 24 November, Adebolajo chose to leave Kenya voluntarily in order to avoid deportation, and he arrived back in the UK on 25 November. On Adebolajo's return, he was immediately interviewed by an SO15 officer, at MI5's request, on the morning of 25 November (from 06:00 to 08:55). This interview was conducted under Schedule 7 of the Terrorism Act 2000, known as a 'Port Stop'.

PORTS EXAMINATION UNDER SCHEDULE 7 OF TERRORISM ACT 2000

The police have the power to stop, detain, question and search anyone who is present at a port entering or leaving the UK and is suspected of terrorism-related activity. The examination can last up to a maximum of nine hours, after which the person must be released or arrested.

The purpose of an examination is to investigate whether a person is, or has been, involved in the commission, preparation or instigation of acts of terrorism. This is usually achieved through questioning the individual and searching their possessions.

During November 2010, hundreds (***) of Schedule 7 examinations were conducted by SO15 ports officers at Heathrow Airport, resulting in the submission of *** intelligence reports.

67. The Committee questioned the MPS Assistant Commissioner about Adebolajo's Port Stop. The Assistant Commissioner said:

> *… it was relatively rare for somebody to be arrested in Kenya or Somalia and, potentially, you know, going to Al Shabaab… that sort of thing was a rare occurrence. This was not a completely routine port stop.*[78]

68. During his interview, Adebolajo claimed that he had been mistreated by the Kenyan authorities whilst he was detained. He claimed that he was beaten, and threatened with electrocution and rape on more than one occasion. SO15 included these allegations in their record of the interview, which they sent to MI5 who passed them on to SIS (requesting that SIS pass them to the FCO). The Committee has a number of serious concerns over

[76] *At the time of this incident, Kenya did not have specific criminal legislation for dealing with terrorism; ***. (Written Evidence – Metropolitan Police Service, 10 December 2013.)*

[77] *The Committee is aware of allegations that HMG actively sought Adebolajo's return to the UK because he may have been able to provide intelligence to the Agencies (this is addressed at paragraph 117).*

[78] *Oral Evidence – Metropolitan Police Service, 31 October 2013.*

the way Adebolajo's allegations of mistreatment were dealt with; these are addressed in more detail in the last chapter.

69. The SO15 officer's broad assessment of Adebolajo during the Port Stop interview was that he was *"reticent"* and provided only superficial answers. Adebolajo *"conveniently couldn't remember"* much information, and was *"found to lie, or at least bend the truth"*.[79]

(i) He claimed his mobile phone had been stolen, and that he did not have an email address (despite having details of other people's email addresses in his pockets).

(ii) He said that while in Nairobi he had met three males from London (***) with whom he spent the majority of his time (two to three weeks). However, he fell out with them and thought they had stolen his belongings. The SO15 interviewer noted that he *"conveniently couldn't remember the full names of the people he had spent his time with in Kenya"*.[80] Adebolajo also claimed that the first time he had met the men with whom he was arrested was while travelling to Lamu.

70. The SO15 officer provided the following comment after his interview with Adebolajo:

> *It is believed that Adebolajo had already planned to meet* *** [two of the three males from London] *before leaving the UK and was either introduced to the group he was arrested with whilst in Kenya or had again been in contact with them prior to his trip… It is further believed Adebolajo will attempt to travel again in the future…*[81]

71. SO15 passed the report of their Port Stop interview to MI5 to take forward any further action. The Committee is impressed by the SO15 officer's assessment of Adebolajo and believes that his interview with Adebolajo was well conducted.

MI5 actions after his arrest

72. As soon as MI5 had been told on 22 November 2010 of Adebolajo's arrest, they opened a Trace.

---

[79] *Primary Material (Adebolajo), Metropolitan Police Service, 25 November 2010.*
[80] *Primary Material (Adebolajo), Metropolitan Police Service, 25 November 2010.*
[81] *Primary Material (Adebolajo), Metropolitan Police Service, 25 November 2010.*

TRACES AND LEADS

A **Trace** is a request for a check across MI5 indices to determine potential links to Islamist extremist activity that does not immediately meet the potential for Lead development.

A **Lead** is the term to describe all intelligence or information that is not linked to an ongoing investigation that, following initial assessment, suggests activities of national security concern.[82]

All Leads go through a formal triage process:

> [Leads] *are tested for links to existing investigations and forwarded to the appropriate team where those links exist. Alternatively, where they do not relate to existing investigations, Leads are tested for credibility and a new investigation is launched if appropriate.*[83]

For more information on Traces, Leads and the Triage Team please see Annex A.

Adebolajo's name was also added to the Home Office Warnings Index to flag up any attempts at further travel overseas.

HOME OFFICE WARNINGS INDEX

The Home Office Warnings Index was introduced in 1995 and is used to ascertain whether passengers are of interest to the Border Agency, the police or other government departments. The Index will show whether a passenger is wanted by the police or has previously been removed from the UK by the Border Agency.

73. In addition, on 1 December 2010, MI5 wrote to an SIS East Africa representative stating that they were carrying out billing enquiries on Adebolajo's stolen mobile telephone and UK mobiles. Under a section entitled 'Ongoing Actions', they asked SIS for their view on whether ***, one of Adebolajo's contacts, could have been a Kenya-based SoI known to MI5 and SIS, who was subject to an ongoing investigation into individuals who were radicalising UK-based extremists and facilitating their travel overseas for extremist purposes (Operation ***, hereafter known as Operation HOLLY).[84] There was no response from SIS to this request.

74. Given that MI5 had written to SIS concerning a potential link to this ongoing investigation, we asked MI5 whether they had considered adding Adebolajo to Operation HOLLY in December 2010. MI5 explained that this potential link would not have been strong enough for them to have investigated Adebolajo under Operation HOLLY at that point. (MI5 further stated that, while Adebolajo was later found to have *"had contact with a number of SoIs across different investigations",* including a number of Operation

[82] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
[83] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
[84] ***.

HOLLY Subjects of Interest (SoIs), *"there was no intelligence to suggest that this* [contact with Operation HOLLY SoIs] *related to their extremist activities".*)[85]

75. MI5 decided to open a separate investigation focussing solely on Adebolajo's activities (named Operation ***, hereafter known as Operation BEECH). However, this operation was not opened until 2 April 2011: a delay of four months.

Delays in opening an investigation

76. The Committee was concerned that the four-month delay in opening an investigation into Adebolajo may have been, in part, because MI5 had opened a Trace, rather than a Lead, on Adebolajo.[86] The significance of this is that Leads are subject to a formal triage process and, by virtue of their joining the Leads Processing Queue, there is a timetable for dealing with them. The Committee questioned MI5, who said:

> *… it could have moved from a Trace to a Lead at any point during that period, in fact, but it didn't. It didn't, in our judgement, stop us doing anything, so we did the basic checks that you can do under both a Trace and a Lead… The fact that it didn't get to an investigation… between the end of November and the beginning of December and April, when* [Operation BEECH] *was open, had more to do with everything else that was going on at the time.*[87]

77. MI5 has told us that the primary reason for the delay in opening the investigation into Adebolajo was due to pressures from other investigations:

> *The time taken moving Adebolajo into an investigation was due to a number of high priority investigations running at the time. This included two investigations in the IOC* [including an investigation into] *a network in England and Wales* [involved in] *attack planning targeting the UK and which resulted in executive action.*[88]

---

85 *Written Evidence – MI5, 5 November 2013. Information on Adebolajo's detention in Kenya and his return to the UK was shared with the Operation HOLLY investigative team.*

86 *Given that Adebolajo's arrest clearly suggested 'activities of national security concern' (he had just returned from Kenya having been suspected of trying to travel to Somalia to join Al Shabaab) this would surely have met the potential for Lead development.*

87 *Oral Evidence – MI5, 17 October 2013.*

88 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013. Executive action can mean Terrorism Act (TACT) searches, overt approaches and potentially (but not necessarily) an arrest.*

INTELLIGENCE OPERATIONS CENTRE

An Intelligence Operations Centre (IOC) is opened in order to carry out either a major covert investigation or a post-incident investigation. Members of staff from other investigative teams are moved into an IOC in order to staff it through shift patterns and to meet the increased demands of the investigation. Sometimes this can mean going into a 24-hour working pattern.

A large-scale IOC has an inevitable impact on the resources available for other investigations, ***.[89] An IOC will take priority in terms of the investigative tools available, such as surveillance and audio coverage.

- The first IOC during this period (IOC ASTER) opened in August 2010 following intelligence to indicate attack planning in Europe. ASTER closed in January 2011. (***).[90]
- The second IOC during this period (IOC BLUEBELL) opened in November 2010 to investigate a UK-based network which had expressed an interest in bomb making. (***).[91]
- As a result of this second IOC, a large number of investigations (***) were suspended. The IOC used a high proportion of all technical operations resource available (***). This IOC was closed in January 2011 following arrests taken against the SoIs.

The Committee notes that both IOC ASTER and IOC BLUEBELL were closed in January 2011, suggesting that the impact of an IOC continues for some months after it is closed. The overall impact of IOCs on MI5's capability is discussed in more detail later in this Report, at paragraph 258.

78. The delays in dealing with low priority cases are an issue that we have encountered on several occasions during the course of our Inquiry (we discuss this in more detail at paragraph 252).

Operation BEECH

79. When Operation BEECH was finally created in April 2011, it was a Priority 3 investigation focussing on Adebolajo's involvement in extremist activity and, in particular, any attempts to travel overseas. ***.

80. MI5 made initial enquiries, including financial and open source enquiries, to confirm where Adebolajo was living, as well as conducting telephone data analysis and checks with the police. On 14 April 2011, the investigative team linked Adebolajo to a GCHQ report from January 2010 which listed the historic contacts of an individual of interest who later became a high profile and senior AQAP extremist. (***.) However, the content of Adebolajo's communication with the extremist was not sought: this 'missed contact' is discussed in further detail later in the Report (paragraph 344).

[89] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
[90] *Written Evidence – MI5, 3 October 2013.*
[91] *Written Evidence – MI5, 3 October 2013.*

I. We note our concern at the four-month delay in opening an investigation into Adebolajo following his return from Kenya. Where an individual is believed to have been seeking to join a terrorist organisation overseas, there should be no such delays. This must be addressed as a matter of urgency.

Communications data

81. One of the first tools available to an investigative desk officer is to analyse the individual's communications data, as this often illuminates further lines of enquiry and might justify more intrusive techniques. In May 2011, MI5's retrospective analysis of Adebolajo's call data linked him to a number of SoIs. The most significant of these were two Yemen-based Subjects of Interest (SoIs), named *** (hereafter known as SoI BRAVO) and *** (hereafter known as SoI CHARLIE).

82. BRAVO and CHARLIE were Tier 1 SoIs being investigated under Operation *** (hereafter known as Operation CEDAR) due to their possible links with AQAP in Yemen (***).[92] As a result of these links, in June 2011 MI5 closed Operation BEECH to allow investigations into Adebolajo to continue under Operation CEDAR. Adebolajo was prioritised as a Tier 2 SoI within Operation CEDAR, to reflect the fact that MI5's interest in him *"stemmed from his contact with lead SoIs* [BRAVO] *and* [CHARLIE]*"*.[93]

OPERATION CEDAR: BRAVO AND CHARLIE

Operation CEDAR was opened in February 2011 as a Priority 1B investigation. Its aim was to investigate reporting which indicated that AQAP was involved in external attack planning, possibly against western targets.[94]

The intelligence was fragmentary but it included the possibility of severe threats:

- ***;
- ***;
- ***.[95]

One strand of the investigation focussed on two individuals with links to the UK, SoIs BRAVO and CHARLIE, who were linked to AQAP external attack planners in Yemen. ***.

In total, *** SoIs were investigated under Operation CEDAR. At one point in 2011, Operation CEDAR was MI5's highest priority operation.

83. MI5 believed that Adebolajo was a primary contact of BRAVO and CHARLIE, and we have seen from the primary material evidence of the close nature of the relationship between the three SoIs.[96] (***.)

92 ***.

93 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

94 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

95 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

96 *MI5 does not know how Adebolajo came to know BRAVO and CHARLIE, ***.*

84. Given that Adebolajo was assessed to be a contact of BRAVO and CHARLIE, a significant volume of resource was deployed against Adebolajo during this period. MI5 told us that:

> **** increased our concern about his activities.*[97]

Surveillance

85. MI5 used surveillance to establish where Adebolajo was living. From May to September 2011 there were a total of *** surveillance deployments against Adebolajo conducted by MI5 and the police, which revealed that Adebolajo was living in London (***). ***. During this period, regular surveillance reports were produced.

86. Surveillance showed Adebolajo meeting ***, an SoI *"investigated for radicalising UK-based individuals and facilitating their travel overseas for terrorist purposes"*.[98] It also revealed Adebolajo's security-consciousness – for instance, he was observed using *** telephone kiosks to make calls despite having a mobile telephone. MI5 has said that:

> *… analysis of communications data relating to these telephone kiosks established that Adebolajo was contacting other known UK based SOIs.*[99]

87. However, MI5 assess that there were multiple other occasions on which Adebolajo used telephone kiosks when he was not under surveillance, and therefore they were unable to *"fully establish the extent and nature of his contact with extremists"*.[100]

Agent tasking

88. Agent tasking is authorised under the Regulation of Investigatory Powers Act 2000. The Committee has been told that, ***:

> **** there was no intelligence during this period to suggest that Adebolajo was planning to travel overseas or carry out any additional operational activity.*[101]

Liaison with the police

89. In August 2011, MI5 passed intelligence to the police regarding Adebolajo's *"possible intention to be involved in the London riots, ***"*.[102] MI5 asked to be informed if Adebolajo was arrested because this might provide them with an opportunity to 'disrupt' him.[103] In the event, however, Adebolajo was not arrested.

90. Also in August 2011, MI5 requested the assistance of the National Terrorist Financial Investigative Unit (NTFIU) after suspicions that Adebolajo was engaged in fraudulent activity. ***:

---

97 *Written Evidence – MI5, 5 November 2013.*
98 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
99 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
100 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
101 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
102 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
103 *'Disruption' is the term MI5 uses to describe "actions taken to manage risks posed by SoIs or networks"; for instance, arresting and imprisoning an individual (Written Evidence – MI5, GCHQ and SIS, 30 August 2013).*

***.[104]

91. ***. The NTFIU had identified no criminal activity linked to the accounts and decided not to submit a formal request for further information because it was not deemed necessary or proportionate.

Further intrusive coverage

92. In addition to the measures already outlined, MI5 successfully applied for further intrusive coverage of Adebolajo's activities. ***.[105] ***.[106,107] ***.[108] During their investigation under Operation CEDAR, MI5's attempts to seek information relating to Adebolajo were given a top priority (***).[109]

***:

93. On 9 May 2011, MI5 made an urgent application for further intrusive coverage[110] against Adebolajo. The application justified the urgency by explaining:

> *Operation [CEDAR] is currently the highest priority investigation of the Security Service.*[111]

94. The techniques used by MI5 resulted in some intelligence of interest, including information relating to the relationship between Adebolajo and SoI CHARLIE. ***.[112] ***.

95. In August 2011, MI5 sought approval for the use of further techniques: ***. Based on what they did obtain, however, MI5 told the Committee:

> *… none of the material identified from Adebolajo's* *** [activities] *were of intelligence interest.* ***.[113]

***:

96. On 13 June 2011, MI5 made an urgent application for the use of additional techniques against Adebolajo ***.[114]

97. Throughout this period, MI5 noted that Adebolajo was a *"difficult SOI to investigate"*[115] due to his security-consciousness ***.

---

104 *Primary material (Adebolajo), MI5, 4 August 2011.*
105 ***.
106 ***.
107 ***.
108 *Written Evidence – MI5, 10 January 2014.*
109 *Written Evidence – MI5, 31 January 2014.*
110 ***.
111 *Primary Material (Adebolajo), MI5, 10 May 2011.*
112 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
113 *Written Evidence – MI5, 31 January 2014.*
114 *Written Evidence – MI5, 17 February 2014.*
115 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

Intelligence gathering operation

98. In summer 2011, MI5 mounted an operation (***) to obtain further information relating to Adebolajo, in order to increase coverage of his activities. Such operations can be described as *"a collection of techniques used by* [MI5] *to gain* [covert] *access to an SoI ***"*.[116] ***.[117]

Summary of Operation CEDAR

99. Whilst Adebolajo had been under intensive surveillance for a number of months, this had not revealed that he was involved in any attack planning. However, MI5 told the Committee that *"comparatively little was known about Adebolajo's contacts and interaction with other UK-based Islamist extremists"*[118] and MI5 considered their coverage to be incomplete. In a Strategic Intelligence Group[119] Note in September 2011, MI5 commented:

> *There is no intelligence to suggest that* [Adebolajo] *is actively involved with attack planning in the UK... However,* [Adebolajo] *has clearly demonstrated extremist tendencies in the past, highlighted by his attempt to travel to Somalia likely to engage in extremist activity. Due to his communications security and unpredictable behaviour, our level of coverage around his current activities is not sufficient to provide assurances that he has disengaged from extremist activity.*[120]

J. The Committee accepts that during 2011 MI5 put significant effort into investigating Adebolajo and employed a broad range of intrusive techniques. In the event, none of these revealed any evidence of attack planning.

---

116 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

117 ***.

118 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

119 *The Strategic Intelligence Group sits within MI5's investigative structure and is designed to "provide assessments which inform resource allocation and challenge the assumption of investigators" (Written Evidence – MI5, GCHQ and SIS, 30 August 2013).*

120 *Primary Material (Adebolajo), MI5, 23 September 2011.*

MOVE TO OPERATION DOGWOOD

100. In September 2011, a Case Review[121] of Operation CEDAR was conducted, which recommended splitting it into a number of different operations. Adebolajo was placed into one of these, Operation *** (hereafter known as Operation DOGWOOD; initially a P1B operation, subsequently P2M). He was classed as a Tier 2 Subject of Interest (SoI). The Case Review summarised that Operation DOGWOOD would investigate reporting that linked SoIs BRAVO and CHARLIE to AQAP:

> ***.[122]

Adebolajo's links to SoIs BRAVO and CHARLIE were also one of the strands to be investigated under Operation DOGWOOD.

101. SoI BRAVO was considered a high priority target for MI5, and was the primary focus of Operation DOGWOOD. Investigation into SoI BRAVO led MI5 to consider his possible involvement in AQAP-linked activity in the UK.

> ***.[123]

102. Coverage of BRAVO and Adebolajo indicated little contact between them (***). Whilst the investigation into Adebolajo under Operation DOGWOOD found no indication that he was currently taking part in Islamist extremist activity,[124] MI5 remained concerned about their level of coverage of Adebolajo.

Technical operation

103. In December 2011, to address this concern, MI5 initiated a technical operation against Adebolajo.[125] ***:

> ***.[126]

104. However, this did not produce any intelligence of significance. Therefore, when the technical operation unexpectedly failed in May 2012, it was not reinstated.

105. Throughout 2012, MI5 maintained coverage of Adebolajo but, by late autumn 2012, had not found any intelligence to indicate involvement in activities of national security concern. The Operation DOGWOOD Case Review noted:

> *There has been no reporting to indicate that* [Adebolajo] *is currently engaging in Islamist extremist behaviour. He has made some progress towards stabilizing his life, through obtaining his driving licence and applying to study accounting.*

---

121 *"Case Reviews are a quarterly review process which investigative teams and their senior management use as the mechanism to formally review investigative strategy and progress (including disruptive impact and level of coverage), in addition to investigative objectives going forward." (Written Evidence – MI5, 10 March 2014.)*

122 *Primary Material (Adebolajo), MI5, September 2011.*

123 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

124 *MI5 has told the Committee that the majority of their intelligence coverage illuminated Adebolajo's behaviour; for example, the fact that he had "an aggressive and controlling personality". (Written Evidence – MI5, GCHQ and SIS, 30 August 2013.)*

125 *The Home Secretary had granted approval for the technical operation in August 2011, but it was not until December 2011 that the opportunity arose to undertake it.*

126 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

However, he has also increased his association with individuals who remain of security concern, including *** [an SoI in Operation ELM].[127]

106. MI5 believed by this point that Adebolajo's *"social associations with Op* [ELM] *targets* [could] *be monitored through coverage of those individuals to identify any activity of security concern"*.[128]

107. Therefore, by October 2012, MI5 ceased the bulk of their intrusive coverage of Adebolajo and planned to close their investigation into him.[129]

---

127 *Primary Material (Adebolajo), MI5, Q2 2012. Operation ELM is assessed in more detail in paragraph 129. It is also important to note that, by November 2012, Adebolajo no longer associated with the other two primary SoIs in Operation DOGWOOD – and indeed one of them no longer posed a threat (***).*

128 *Primary Material (Adebolajo), MI5, 22 October 2012.*

129 ***.

WHAT ELSE COULD MI5 HAVE DONE?

108. The Director General of MI5 has said that, given that Adebolajo was under intensive surveillance for a significant period of time, MI5 was:

> *… up against the limits* ***.[130]

Furthermore, MI5 stated:

> *From an investigative perspective, we threw the kitchen sink at it,* *** *we had a broad range of investigative capabilities* [deployed against Adebolajo].[131]

109. It is clear that MI5 put considerable effort into establishing Adebolajo's intent, as is right for a Subject of Interest (SoI) in a P1 investigation.

110. The Committee questioned MI5 as to whether they could have done anything more in relation to Adebolajo; for instance, deploying another technique available to MI5 which they did not use in this case (***). MI5 told the Committee that there is no record to indicate that they considered this approach ***:

> ***.[132]

111. MI5 has told the Committee that *"while there was resource we were not deploying against Adebolajo during* [Operation DOGWOOD]*"*, this was entirely appropriate, given that *"the nature of the intelligence case against Adebolajo did not come close to meriting this level of resource and concomitant risk"*.[133] As we have noted previously, MI5 carefully assesses the need for all intrusive action: in evaluating whether it is necessary and proportionate they must consider whether it can be expected to produce anything of relevance. They must also prioritise it against other operations requiring resources.

Security awareness

112. Adebolajo's case clearly demonstrates the difficulties MI5 faces when investigating an individual who is determined to hide their intentions. MI5 has said that Adebolajo was very careful about his communications security over a long period of time. They told the Committee:

> *Intelligence coverage of Adebolajo under* [Operation DOGWOOD] *did not indicate any ongoing Islamist extremist activity but he remained extremely security-conscious.*[134]

113. Whilst Adebolajo's security-consciousness could be attributed to extremist intent, an alternative interpretation considered by MI5 was that it could have been due to his involvement in illegal drugs activity. MI5 said that:

> *** *we were not certain whether his security-conscious manner was because of his extremist activities or due to continuing involvement in drug crime.*[135]

---

130 *Oral Evidence – MI5, 17 October 2013.*
131 *Oral Evidence – MI5, 17 October 2013.*
132 *Written Evidence – MI5, 7 February 2014.*
133 *Written Evidence – MI5, 5 November 2013.*
134 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
135 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

114. The Committee asked MI5 whether they use any particular techniques when investigating an SoI who is particularly security-conscious. MI5 responded:

> *SoIs have employed and will continue to employ a multitude of different methods of varied sophistication to try and evade the attention of the authorities. MI5 is continually developing techniques to enable us to gain the necessary coverage of an SoI's activities proportionate to the threat they pose but we rarely have complete coverage.*[136]

115. Adebolajo's case also highlights the difficulty of deciding when to cease coverage of an individual where little intelligence of national security concern has been found, but on whom coverage is believed to be insufficient.

> *DR JULIAN LEWIS, MP: … you get this chap. He is caught in Kenya. It is judged that in all probability, he was trying to join Al Shabaab. He comes back rather alerted, it seems to me. A police officer interviews him and judges that he is a liar and you consistently find, under the most intensive scrutiny, that he is highly security-conscious. And yet at the end of the day, because you have not come up with anything positive, you say: well in that case, we either drop him… or something like that. It is just that degree of security-consciousness of itself, you are telling us, shouldn't justify keeping him on your radar.*
>
> *MI5 DIRECTOR GENERAL: Not on its own. I think your point would be absolutely on the nail, if we'd sort of made that decision after a period of weeks of investigation. But we did two years because of the sort of person he was and the background, and that in itself is a very unusual thing for us to do, to live with a high priority target that long and with this extent of resource, until we were satisfied that we should… on a risk basis, we were able to put it down. So over two years, no sign of terrorist intent on his part.*[137]

116. Overall, regarding Adebolajo's case, MI5 commented:

> *Looking back at Adebolajo, we can see an example of somebody who was a determined individual, is entirely capable, as others are, of concealing their intentions from us; and in his case, he is an example of somebody who was not deterred by intervention… We cannot see everything, even under intrusive coverage and some determined people can hide and are not deterred, are unfortunately characteristics of the reality of counterterrorism work that we are dealing with…*
>
> *I am absolutely confident that we took well based decisions about him, throughout the period of five years that we knew about him. I am also confident that there is nothing else that we could have reasonably done about him.*[138]

K. MI5 rarely have complete coverage of their targets, even those who are under intensive investigation. In some circumstances they may not have sufficient intelligence indicating extremist intent to justify continued investigation. Where they are aware that their coverage is incomplete, we recognise that the decision to stop investigating such an individual will always be difficult.

---

136 *Written Evidence – MI5, 7 February 2014.*
137 *Oral Evidence – MI5, 17 December 2013.*
138 *Oral Evidence – MI5, 17 December 2013.*

ALLEGATIONS OF RECRUITMENT AND HARASSMENT

117. The Committee is aware of numerous allegations in the media that MI5 harassed Adebolajo, and had been trying to recruit him as an informer (an agent) in the years before the murder. The allegations include the claim that MI5 had 'freed' Adebolajo from jail after his arrest in Kenya, in order for him to return to the UK to act as an agent for MI5; and speculation that persistent pressure from the security services 'pushed him over the edge' towards committing the brutal murder.

118. The Committee has thoroughly investigated these allegations. During our Inquiry, we inspected hundreds of pages of primary material from MI5, SIS, GCHQ, the Metropolitan Police Service and other organisations, and we cross-examined witnesses.

Allegations of recruitment

119. Agents are one of MI5's most important sources of intelligence. MI5 often approaches Subjects of Interest (SoIs) in order to try to recruit them as agents. MI5 states that the key factors in assessing an individual's suitability as a potential reporting agent are their access to intelligence, their motivation to work with the Service and their personal qualities.

120. MI5 has explained that recruiting an SoI as an agent is a positive outcome for MI5, as not only does this mean that there will be a reduction in the risk posed by that SoI, but MI5 will also have increased visibility of their activity. They will also become a valuable source of intelligence. ***.

121. Agent handling for International Counter Terrorism in MI5 is handled by a specific team (***). They are responsible for the identification, recruitment, running and aftercare of individuals who are in a position to report on SoIs (agents or CHISs[139]). ***. Investigators often refer current or former SoIs to agent handling sections for potential recruitment as agents.

122. In relation to the allegations that MI5 had been trying to recruit Adebolajo as an agent, MI5 has argued that it would be damaging to national security to comment on such allegations. All allegations concerning MI5's recruitment of agents – whether true or not – fall under their 'Neither Confirm Nor Deny' (NCND) policy.

123. We questioned the Agencies extensively on their NCND policy. MI5 told us that the NCND policy is crucial for protecting the safety of current and former agents, and to ensure that they – and any individual considering helping the Agencies – can be confident that such work will remain absolutely confidential, whatever the circumstances. MI5 also told us that:

> *For the NCND policy to work effectively, consistency of response is of the utmost importance. For example, if we were to depart from NCND to confirm that an individual who was approached was NOT recruited, that would soon lead to a strong inference that an individual had been recruited where an NCND response was given. Only by employing the policy uniformly can national security be protected.*[140]

[139] *Covert Human Intelligence Sources.*
[140] *Written Evidence – MI5, 3 October 2014.*

124. While we would have liked to publish the full facts, given the public interest in such allegations, we have accepted that we cannot comment publicly on the allegations that MI5 had been trying to recruit Adebolajo as an agent, although we have reported on this matter in the classified version of our Report to the Prime Minister.

Allegations of harassment

125. With regard to allegations that Adebolajo was harassed, we are able to confirm that, during the course of our Inquiry, we have found no evidence that there was any harassment of Adebolajo by MI5. Although we cannot publish any details of these two aspects of our investigation, the full facts are included below in the classified version of our Report to the Prime Minister.

***

***.

***.[141]

***.[142]

***.[143] ***:

***.[144]

***.[145]

***.

***.

***

***.[146]

***.[147] ***:

***.[148]

***.[149]

[141] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013. ***.*
[142] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
[143] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
[144] ***.
[145] *Oral Evidence – MI5, 17 October 2013.*
[146] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
[147] ***.
[148] *Oral Evidence – MI5, 12 December 2013.*
[149] *Oral Evidence – MI5, 17 October 2013.*

L. To publish any information in response to allegations that MI5 harassed Adebolajo or tried to recruit him as an agent would damage national security – irrespective of the substance of such allegations. Despite the considerable public interest in this case, it is nevertheless essential that we do not comment on the allegation that MI5 had been trying to recruit Adebolajo as an agent. In relation to allegations of harassment, we can confirm that we have investigated all aspects of MI5's actions thoroughly, and have not seen any evidence of wrongdoing by MI5 in this area.

Assessments of Adebolajo's mental health

126. Given the media allegations, the Committee also questioned whether MI5 had considered Adebolajo's mental health while investigating him. The Committee asked if MI5 had made a formal assessment of Adebolajo's mental health. MI5 confirmed that they had not. The Committee questioned MI5 as to whether they felt Adebolajo's experiences in Kenya might have had an impact on his mental health. The Director General replied that he thought not:

> [Adebolajo] *was very secretive and, in the common sense, a bit paranoid; it is not used in a mental health sense. And so we knew those things about him. They characterised him throughout his life and our knowledge of him. And they are not… I do not think all that behaviour is peculiar to his detention in Kenya and what happened after that, because his history of violence and erratic behaviour goes way back.*[150]

127. The Director General also confirmed that, after the attack in Woolwich, psychiatrists made a clinical judgement about Adebolajo's suitability to be interviewed and subsequently to stand trial; these assessments confirmed that he was fit to stand trial, and was not suffering from mental illness.

128. As a result of their review of their actions in this case, MI5 has identified this area as something which could be improved. (Lessons learned are addressed at Annex B.)

---

[150] *Oral Evidence – MI5, 17 October 2013.*

***

***.[151]

***.[152] ***.

***.[153]

***.[154]

***.

***.

***.[155]

***.[156] ***.

[151] *Oral Evidence – MI5, 17 October 2013.*
[152] *Primary Material (Adebolajo), MI5, 14 March 2012.*
[153] *Primary Material (Adebolajo), MI5, 5 April 2012.*
[154] *Written Evidence – MI5, 5 November 2013.*
[155] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
[156] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

OPERATION ELM: POSSIBLE DISRUPTION AND END OF COVERAGE

129. In October 2012, just at the time MI5 was considering closing their investigation into Adebolajo, they received new information suggesting that he might have been acting as a contact for Al Shabaab. This information was linked to a Subject of Interest (SoI) named *** (hereafter known as SoI DELTA), who was being investigated under a separate operation called *** (known as Operation ELM in this Report). As a result, Adebolajo was transferred into Operation ELM in November 2012.

***

***:

***.[157]

***:

***.[158]

Reinstatement of intrusive coverage

130. Under Operation ELM, MI5 reinstated intrusive coverage of Adebolajo on 3 December 2012: ***. This was intended to:

> *… establish, in detail, his updated pattern of life activity and the nature and extent of any contact with other SoIs.*[159]

131. However, during this final period of investigation "*no indication of intelligence of national security concern was identified".*[160] Adebolajo did not associate with other Operation ELM SoIs and communicated with SoI DELTA only occasionally. MI5 therefore assessed that Adebolajo was *"unlikely to be aware of the aims of* [SoI DELTA]*".*[161] Coverage indicated that Adebolajo was spending most of his time involved in drug dealing.

Disruption opportunities: violent confrontation and drug dealing

132. MI5 focussed on ways of disrupting Adebolajo through his criminal activities by working with the police.

[157] *Primary Material (Adebolajo), MI5, 26 October 2012.*
[158] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
[159] *Written Evidence – MI5, 7 February 2014. ***.*
[160] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
[161] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

DISRUPTION OPPORTUNITIES AND WORKING WITH THE POLICE

MI5 has explained that *"'disruption' is how we term actions we take to manage risks posed by SoIs or networks"*.[162]

This can range from short term tactical disruptions (e.g. prosecution for road tax evasion) to major covert operational activity aimed at arresting and imprisoning an individual:

> *The type of disruption will be based on consideration of opportunity, the risk posed by the SoI, the likely impact on their activity by the disruption, and the proportionality of the resourcing required to effect it.*[163]

MI5 and the police work closely together when considering potential disruption opportunities. Usually, MI5 will request that the police provide support through appointing a Senior Investigating Officer (SIO) who will assist in the management of the investigation, lead the police interaction and develop a joint tactical strategy with MI5.

This management process is then usually formalised through a Joint Operational Team (JOT), comprising an MI5 lead, police SIO and specialists from MI5, the police or any other relevant agency.

Violent confrontation

133. In November 2012, Adebolajo was part of *"a larger group of individuals who were* [involved in] *a violent confrontation* ***.[164]

134. The Metropolitan Police Service stopped and arrested some of those involved in the violence. The Committee has been told:

> *… the assembled group, including *** Adebolajo, were stopped en route to Woolwich Dockyard on 6 November 2012. ***. Adebolajo was one of a number of associates who were stopped but not arrested during the disruption.*[165]

135. Following the disruption, it was noted that *"Adebolajo's details will be passed to* [another police unit]*"*.[166] Whilst this might have offered a potential disruption opportunity, it did not happen. When the Committee questioned the police on this point, the police maintained that *"there was never any question of Adebolajo's details being passed to* [the other police unit] *because he was not the* [central figure in the confrontation]*… There was no express or tacit agreement to pass the details of Adebolajo to other police units."*[167] The police have told us that this option would only have been considered if the disruption *** had been unsuccessful. As the violent confrontation was disrupted (***) the referral of Adebolajo was deemed unnecessary by the police. His details were not therefore

---

162 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
163 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
164 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
165 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
166 ***.
167 *Written Evidence – Metropolitan Police Service, 10 December 2013.*

passed to the other police unit. However, the fact that this position was not recorded raises questions about communication and the effective recording of decisions.

Drug dealing

136. Coverage of Adebolajo under Operation ELM (and previous investigations) indicated that he was involved in drug dealing. Therefore, on 15 February 2013, MI5 notified SO15 that they believed Adebolajo was involved in the *"procurement and distribution"*[168] of controlled drugs. MI5 saw this *"as a possible opportunity for a low level disruption of Adebolajo"*.[169]

137. On 27 March 2013, a sanitised form of words for dissemination within the police was provided to SO15 by MI5:

> *Michael Olumide Adebolajo (10/12/1984) of* [full home address] ***, *engages in drug dealing activity.*[170]

This information was channelled through to the local police in Romford, ***. However, during this process *"the house number in the original form of words was accidentally omitted"*.[171] As a result, the police officer tasked to investigate concluded on 10 April 2013 that no further action could be taken:

> *NFA* [No Further Action]*/Closed… Cannot find* [house] *number… and this is a long road… For info at this stage.*[172]

138. This could have been resolved if the police had reported back to MI5 the results of their actions, as MI5 could then have ensured that the police had the correct address. When questioned about this by the Committee, the Assistant Commissioner said:

> *We absolutely concede that there was an error and that didn't help the local borough. However, even if they had the address perfectly, I think it is quite doubtful, given the kind of volume of the drug dealing intelligence that any borough receives all the time, that in the absence of any other information in their systems about drug dealing, which there was none, they would have been able to progress this very far or would have progressed it very far.*[173]

139. It is worth noting that both MI5 and the police consider that the likelihood of any executive action at the time was minimal. As part of the investigation following the murder of Fusilier Lee Rigby, a search warrant was executed at his home address (***). However, *"no drugs or evidence of drug use was found at the address"*.[174]

140. In this instance the disruption opportunity was not successful. This led the Committee to think about the use of disruption opportunities more generally. We asked the Home Secretary whether she considered that MI5 and the police should use disruption

---

168 *Written Evidence – Metropolitan Police Service, 30 August 2013.*
169 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
170 *Written Evidence – Metropolitan Police Service, 30 August 2013.*
171 *Written Evidence – Metropolitan Police Service, 30 August 2013.*
172 *Primary Material (Adebolajo), MI5, Metropolitan Police Service, 10 April 2013.*
173 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*
174 *Written Evidence – Metropolitan Police Service, 30 August 2013.*

opportunities more. The Home Secretary agreed that there was a question as to whether MI5's investigations and criminal investigations could work better together:

> *I think we also need to look at the way in which the police are able to prioritise when they've got somebody who in these particular incidents, some people who have been involved in drugs but were also on periphery of some CT* [counter-terrorism] *investigations, and the extent to which it's possible to bring that information together and perhaps give people a higher priority from the policing side, because of that element of potential terrorist involvement or that they've been involved in those sorts of investigations. So that's another area which we need to look at.*[175]

M. The Committee considers that there is insufficient co-ordination between MI5 and police investigations. Disruption based on criminal activities offers a potential opportunity to reduce the threat posed by extremists. MI5 and the police must improve both the process and the level of communication.

Reduction of intrusive coverage

141. As discussed in paragraph 136, intrusive coverage of Adebolajo indicated that he was spending most of his time drug dealing. There was no intelligence to indicate anything of national security concern. Adebolajo was therefore demoted from a Tier 1 to a Tier 2 SoI and, finally, to a Tier 3 SoI in February 2013, and intrusive coverage of him was cancelled on 11 April 2013.[176] This was the last action taken with respect to Adebolajo before the attack, just over a month later.

142. Giving evidence to the Committee, the Director General commented:

> *We had an informed view, from which we could say: actually, nothing to see here on violent extremism, beyond the fact that he moves in these circles and associates with people that we do need to be very concerned about. But he was doing that with sufficient frequency and numbers of contacts that we felt we ought to persist and persist and persist, until we had run out of bases completely which was, timing-wise unfortunately, early in – it was March 2013.*[177]

N. Intrusive coverage of Adebolajo from December 2012 to April 2013 showed that he was involved in drug dealing. However, it did not provide any intelligence of national security concern: on this basis, MI5 had to cancel their coverage in April 2013. MI5 cannot continue intrusive coverage against an individual unless it is necessary and proportionate to do so. On this occasion, based on the intelligence they had, it was not.

---

175 *Oral Evidence – Home Secretary, 21 November 2013.*

176 ***.

177 *Oral Evidence – MI5, 12 December 2013.*

DEALING WITH RECURRING SUBJECTS OF INTEREST

143. Adebolajo was investigated under five separate operations in total, with all of these bar one (Operation BEECH) assessing him in relation to his connections with wider networks of extremists, rather than 'in his own right'.[178] The Director General told us that:

> *… it is fairly common to see SoIs feature in different investigations over a period of years. Unless an SoI is disrupted through imprisonment, recruitment or their own withdrawal from extremist activities, it is not unusual for an SoI to be investigated under different auspices as the nature and significance of their activity changes.*[179]

144. Nevertheless, in Adebolajo's case MI5 does not seem to have addressed whether the cumulative effect of having appeared in five different investigations should have been enough, on its own, for investigation into Adebolajo to have continued even when his links to those specific operations had ceased.

145. As a result of their internal review after the attack, MI5 has identified that the way they deal with 'recurring Subjects of Interest' is an area needing further work:

> *We will seek to develop criteria for identifying when recurring SoI's meet the threshold for investigation in their own right… there is still scope for MI5 to improve the way in which we handle those SoIs who move repeatedly between investigations.*[180]

When giving evidence to the Committee on this subject, the Director General said:

> *… that is one of the things we are looking at in the lessons learned, about whether we can do something that brings more focus to people, who there is no reason why they should ever be at the bull's eye. But in repeated cases, they keep appearing somewhere in the concentric rings. What do we do about them objectively is something that we would like to see some stronger process around.*[181]

146. When the Home Secretary gave evidence she commented on the wider question of:

> *… how you identify what I would call the cumulative effect of people who were on the periphery of various investigations, particularly those who perhaps go in and out, who are sort of on the radar for one thing, then perhaps on the radar for something else, and how you're able to join that up into judgments about people who, on the face of it, appear to be at the low level but potentially, if you look across everything that they're doing, perhaps should be at a higher level.*[182]

She questioned:

> *… whether that cumulative impact can be sufficiently taken into account and whether there is a need to find some way of being able to better identify those individuals.*[183]

---

178 *Adebolajo was usually prioritised within these operations as a lower tier SoI, rather than as the main target of the operation.*
179 *Written Evidence – MI5, 5 November 2013.*
180 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
181 *Oral Evidence – MI5, 17 October 2013.*
182 *Oral Evidence – Home Secretary, 21 November 2013.*
183 *Oral Evidence – Home Secretary, 21 November 2013.*

147. This is one of the key issues that have arisen from our assessment of MI5's investigations into Adebolajo.[184] The cumulative intelligence obtained on Adebolajo revealed that he had been linked to a number of different (and apparently unconnected) extremist networks and Subjects of Interest; he had links to a proscribed organisation; he had attended an event which was assessed to have had an extremist agenda; and he had been suspected of attempting to travel overseas to join a terrorist organisation. He had also been the subject of intermittent reporting suggesting an involvement in extremism. MI5 took the decision to stop investigating Adebolajo in April 2013 based primarily on his relationship with SoIs within the most recent operation (Operation ELM). Although they did take his investigative history into account, there is a question as to the extent to which the cumulative effect was assessed.

148. While investigative action must be necessary and proportionate, and an individual must have demonstrated behaviour or intent which poses a threat to national security, MI5 must nevertheless give greater emphasis to the cumulative risk posed by individuals who have appeared on MI5's radar in connection with numerous operations. (MI5 identified this as an action within their internal review – see Annex B.)

O. MI5 does not currently have a strategy for dealing with Subjects of Interest who occur on the periphery of several investigations. This is a key issue which has arisen during the course of our Inquiry which must be addressed by MI5. The Committee recommends that where individuals repeatedly come to MI5's attention, through their connections with a wide range of Subjects of Interest, MI5 must take this 'cumulative effect' into account. They should ensure that interactions between Subjects of Interest are highlighted when making investigative decisions.

[184] *The issue of considering individuals in their own right rather than in relation to a network is also relevant when considering the threat from 'lone actors' – more detail on this can be found at paragraph 232. It is worth noting that the police also identified a focus on networks rather than individuals as one reason why the Programme AMAZON scheme failed; this issue is one that has repercussions across a wide spectrum of the police and intelligence and security Agencies' work.*

MICHAEL ADEBOWALE

Name:	Michael Oluwatobi Adebowale
Nationality:	British
Date of birth:	6 May 1991
Convictions:	Drugs-related offences in 2007–08.
Role in the attack:	Convicted of the murder of Lee Rigby (cleared of attempted murder of police officers). Sentenced to life, with a minimum of 45 years in prison.

Michael Adebowale was investigated by MI5 on two separate occasions:

Operation FIR (Priority 2M) from August 2011 to June 2012: Multiple lead investigation into UK-based individuals with an interest in extremist media.

Operation GUM (Priority 3) from January 2012 up until the attack: Investigation into Adebowale, following his extremist rhetoric and potential dissemination of extremist media.

INITIAL INTELLIGENCE: EXTREMIST MATERIAL ONLINE

149. Michael Oluwatobi Adebowale came to MI5's attention as a result of his interest in online extremist material. He was investigated by MI5 under two different low priority operations, from 2011 up until the attack.

150. The first intelligence received by MI5 in relation to Adebowale was in 2011. Intelligence received from GCHQ indicated that an unknown individual had shown interest in extremist media online. (***.)[185]

151. After receiving the GCHQ report, MI5 took forward the intelligence as a Lead[186] in order to identify the individual concerned. The Lead was assigned to Operation *** (hereafter known as Operation FIR), a Priority 2M 'multiple lead' operation which aimed to identify UK-based individuals who had shown an interest in extremist media (***). Such individuals were assessed to determine if they posed a threat to national security and, if so, were referred to their own investigation.

152. ***:

> ***.[187]

UMBRELLA OPERATIONS

Operation FIR was a 'multiple lead' operation (also known as an 'umbrella operation'). Whilst the majority of MI5's operations investigate particular individuals or networks, umbrella operations are instead designed to capture, process and investigate leads based around a particular theme (***). MI5 has advised that approximately 10% of their investigations are 'umbrella operations' such as Operation FIR.

153. Operation FIR was worked on by a small number of investigative officers (***). These individuals were responsible for a number of investigations (***). Each of these investigations contained varying numbers of Subjects of Interest.

Extremist media and Inspire magazine

154. Of the many extremist publications available on the internet, the primary English language publication is *Inspire*, which is the online magazine of AQAP.[188] During this Inquiry, and previously, the Committee has considered the role of online extremist media, and the impact of *Inspire* magazine in particular. *Inspire* was created by AQAP as a way of disseminating extremist information on the internet in English. It appears that the influence of *Inspire* has grown considerably over time: MI5 now places greater weight on it as a contributing factor to extremism than they did in 2011. An internal MI5 assessment of *Inspire* in 2012 said:

---

185 ***.

186 *See Annex A for the definition of a Lead. The individual was subsequently found to be Adebowale.*

187 *Primary Material (Adebowale), MI5, September 2012.*

188 *Al Qaeda in the Arabian Peninsula is an Al Qaeda-affiliated extremist group based in Yemen. The group is highly active, devising new methods to conduct attacks. It also has a significant media and propaganda presence.*

Inspire seeks to promote home-grown 'lone actor' attacks, providing the ideological backing and practical instruction for users to commit attacks.[189]

MI5's Strategic Intelligence Group provided the following assessment of *Inspire* in 2013:

[It] *presents a variety of risks to the UK, including providing *** instruction for violent attacks.*[190]

155. MI5 has told the Committee of the link between *Inspire* and individuals involved in planning UK attacks:

… we can now say that Inspire has been read by those involved in at least seven out of the ten attacks planned within the UK since its first issue [in 2010]. *We judge that it significantly enhanced the capability of individuals in four of these ten attack plots…*[191]

156. The Committee questioned the Agencies as to whether *Inspire* should be viewed solely as a threat or whether it might also offer an intelligence opportunity. GCHQ responded that, ***:

… overall this is a threat, this is pernicious. It radicalises, it exhorts violent action and it gives recipes or instructions on how to do so.[192]

157. ***:

***.[193]

***.

(i) Interest in extremist media

158. There is a wide range of media which is extremist in nature. Where MI5 is aware of intelligence that individuals might have an interest in, or have read, extremist media of concern, they may carry out investigations to assess the level of threat these individuals might pose. However, MI5 would not carry out any intrusive investigation of an individual purely on the basis of such interest (for example, if they have read *Inspire* magazine). MI5 told the Committee:

… it would not be sufficient to qualify [for intrusive coverage]*… That would not be proportionate.*[194]

---

189 *Primary Material (Adebowale), MI5, 14 June 2012.*

190 *Written Evidence – MI5, 23 April 2014.*

191 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013. Inspire is only one of many examples of extremist material which have featured in investigations into terrorism: the Metropolitan Police Service has a database of seized terrorist material which comprises 3,000 distinct records. Inspire does not feature in the top 20 most commonly found files within this database. (Written Evidence – Metropolitan Police Service, 10 December 2013.)*

192 *Oral Evidence – GCHQ, 24 October 2013.*

193 *Oral Evidence – MI5, 10 October 2013.*

194 *Oral Evidence – MI5, 10 October 2013.*

While MI5 accepts that there is a *"potential risk posed by those who access* [extremist media]*"*, they also caution that *"It does not follow that everyone who* [does so] *then engages with violent extremism"*.[195]

(ii) Engagement with extremist media

159. MI5's Operation FIR seeks to identify and assess individuals who have also sought to engage with extremist media; ***.

160. ***:

> ***.[196]

***.

161. ***.

162. ***.[197]

163. The Committee asked MI5 how seriously they viewed such engagement with extremist material online. The Director General explained that, while they would want to identify such individuals and assess the threat they pose, such engagement (***) would still not, in itself, be sufficient to justify intrusive surveillance into someone:

> ***. *That is not enough.*[198]

(In addition to engaging with extremist media, individuals may also try to disseminate it further: this is addressed in paragraph 294 of the Report.)

P. Engagement with extremist media should be taken extremely seriously. For example, *Inspire* magazine provides advice and guidance to individuals on how to commit terrorist attacks in the UK. In most cases, engaging with extremist media such as *Inspire* should be sufficient grounds to justify intrusive action.

---

195 *Written Evidence – MI5, 31 October 2013.*
196 *Written Evidence – GCHQ, 15 November 2013.*
197 *Oral Evidence – GCHQ, 28 November 2013.*
198 *Oral Evidence – MI5, 12 December 2013.*

OPERATION FIR: DELAYS AND THE DIGINT TEAM

164. Once MI5 received the intelligence from GCHQ, they started trying to identify the individual concerned (***). MI5 provided the following timetable of events:

- On 5 August 2011 the Operation FIR investigative team tasked MI5's Digital Intelligence (DIGINT) team to identify the individual concerned.
- By September 2011, the DIGINT team had enough information for the investigative team to identify the individual as Michael Adebowale.
- By November 2011 the DIGINT team had finished their enquiries.
- However, it was not until April 2012 (five months later) that the Operation FIR investigative team started investigating Adebowale.

165. MI5 has told the Committee that the delay was due to a number of reasons, including the complexity of the request, the priority of the case, and the level of resources assigned to it. However, eight months seems an unacceptable length of time to identify and start investigating an individual who potentially posed a threat to national security. In response to our concerns, MI5's Director General said that, overall, the time it took to identify Adebowale was *"normal"* for a low priority investigation:

> *… because these cases at this level, P3, are very often paused or suspended or set aside while higher priority work was going on… In terms of how long that took, the fact is that it was not material because… when we had it all together and had done more inquiring and looked at it, we closed it. So… we were right to treat it as a low priority at the time.*[199]

166. Whilst, with the benefit of hindsight, it might have been the right decision, MI5 could not have known this at the time. The Committee has a number of specific concerns with this part of the investigation, which are covered in the following sections:

(i) Time taken to identify Adebowale;

(ii) GCHQ support to MI5 in identifying the individual as Adebowale;

(iii) Records management; and

(iv) Management of 'umbrella' operations.

(i) Time taken to identify Adebowale

167. MI5 has explained that the first step of their investigation was to try to identify the individual who had the interest in extremist media online. This was done by MI5's Digital Identification Team (DIT) within the DIGINT team.

[199] *Oral Evidence – MI5, 10 October 2013.*

DIGITAL INTELLIGENCE

Digital intelligence (DIGINT) is a phrase used by MI5 to refer to intelligence or information acquired from digital sources (***).

MI5's DIGINT team leads on these capabilities. The team undertakes analysis of digital activities which focus on UK-based individuals with no, or limited, links overseas. ***.

168. The DIGINT team classed the Lead as a routine request, in line with the investigation team's prioritisation of the case.[200] MI5 has told the Committee that within three working days the DIGINT team had begun enquiries ***. This timescale was within MI5's internal service level agreement for routine requests.

169. The Committee has been told that identifying an individual in such circumstances is not necessarily a simple process. Factors influencing the completion times include:

- how long it takes to acquire the relevant information (***);[201]
- the volume of higher priority requests; and
- the capacity within the DIGINT team (which varies according to staffing levels, training, leave and other commitments).[202]

170. As set out above, the DIGINT team's enquiries could have enabled the investigative team to identify Adebowale by September 2011, but the DIGINT team did not complete their enquiries until November 2011. MI5's Director General explained that the reason it took until November for the DIGINT team to complete all their enquiries was partly due to the complexity of the task:

> *… there is a whole range and series of enquiries they are doing. That process by September had got as far as producing Adebowale's name and identity; but there were other things that they were still pursuing, which then finished in November.*[203]

171. The Committee asked for more detail on what had caused this particular delay. MI5 responded that work had been held up between September and November because information from one particular source had not been received:

> *The DIGINT team made* [five] *requests for* [information] **** on 18 August 2011. Results had been received for four of* [these requests] *by 27 September 2011 which would have enabled full identification of Adebowale. We initially received no response* [to the final request] **** and had to resubmit the request on 04 November 2011. This response was received on 16 November 2011.*[204]

172. The Committee questioned whether such a long timescale was usual and MI5 provided the following context:

---

200 *Urgent or priority requests are dealt with first; routine enquiries are placed in a 'queue' to be dealt with in turn.*

201 ***.

202 *Written Evidence – MI5, 3 October 2013.*

203 *Oral Evidence – MI5, 10 October 2013.*

204 *Written Evidence – MI5, 7 February 2014. ***.*

- In August 2011, the month that MI5's DIGINT team was tasked to identify the individual, they were tasked with hundreds (***) of similar identification tasks.
- The average completion time for the tasks during this period was 69 days for all aspects of the response (although pieces of information may have been obtained and passed to investigative teams before the completion point).

173. This average figure of 69 days is broadly consistent with the time taken for the DIGINT team to identify Adebowale (from August to November 2011). The Director General nevertheless recognised that the average of 69 days to complete identification tasks was slow:

> *So it takes as long as it takes. I had always wanted it to be short. So am I content with it? No.*[205]

The Director General assured the Committee that the process could be much quicker if the identification was considered urgent rather than routine:

> [If] *there was a P1 case that meant that we had significant urgency behind it, then we could do it much, much quicker.*[206]

Q. In low priority cases, it takes MI5's DIGINT team an average of 69 days to complete identification tasks, such as identifying an individual who has sought to engage with extremist material online. Whilst we accept that these are low priority cases, two months is nevertheless too long. This process must be improved as a matter of urgency.

(ii) GCHQ support to MI5 in identifying the individual as Adebowale

174. MI5's Director General explained that MI5's DIGINT team often needed expert assistance to complete their enquiries:

> *GCHQ is the… centre of excellence on this.* [So] *we rely on GCHQ to provide the capabilities. We apply some of them, some of the tools ***. We draw on their help a bit. ***. Sometimes it is – it can be a very elaborate thing to pursue, because of the sheer diversity of* [online activity].[207]

175. MI5's own access to communications data information, and the additional expertise that MI5 analysts can request from GCHQ to assist with enquiries, was described to us in the following way:

> [MI5] *Analysts can seek management authorisation to request communications data (where RIPA is in force ***). They may also seek management authorisation to query GCHQ SIGINT events data (Related Communications Data, not content)* ***.[208]

176. In terms of Operation FIR, the Committee noted from the primary material that the desk officer repeatedly highlighted the need for more GCHQ resource, in order to be able

[205] *Oral Evidence – MI5, 12 December 2013.*
[206] *Oral Evidence – MI5, 12 December 2013.*
[207] *Oral Evidence – MI5, 12 December 2013.*
[208] *Written Evidence – MI5, 7 February 2014. SIGINT stands for Signals Intelligence.*

to complete their tasks. We note that this concern was mentioned in five Operation FIR Case Reviews over the course of a year, suggesting that it was a continual problem. There is no evidence that these concerns were ever addressed by MI5. The Director General said:

> *This is a product of how far pressures on resource spreads down the large stack of our casework… From our point of view, we are able to get GCHQ's active support on… the higher end of our investigations where they rightly focus… So I think you are seeing an expression of appetite from the Desk Officer in the layer of our casework where GCHQ help thins out.*[209]

177. When questioned about this issue by the Committee, GCHQ said that they had not been aware of any concerns from MI5 about lack of GCHQ support:

> *I do not know where this comment comes from. It was not fed through to us in this way… it was not flagged up that we were doing anything wrong. There has been a sort of evolution of the amount of resource that we have put in and how we work with the DIGINT team.*[210]

GCHQ confirmed that they have now increased staff resources (***).

GCHQ's prioritisation of resources

178. This question of the support provided by GCHQ to MI5's DIGINT team highlights the wider issue of how MI5 and GCHQ work together on domestic counter-terrorism operations.

179. While GCHQ's largest single tasking is the provision of support to counter-terrorism operations (where there is an international element),[211] this nevertheless represents only a third of their total effort. MI5's Director General explained that this meant that MI5 had to rigorously prioritise which operations they sought GCHQ's help with. He told the Committee:

> … *all of our* [top priority] *cases have GCHQ support and most of the* [second tier] *cases, but that is normally about as far as we can extend GCHQ's intrusive and active help*.[212]

180. The Committee has been told that in the first quarter of 2013, GCHQ was able to support the majority (***) of MI5's highest priority 'grid' operations (***). GCHQ has explained that:

> *the* [remainder] *of operations which we did not support would have been because there was no unique value GCHQ could add: no foreign end, or discernible electronic communications, for example.*[213]

---

209 *Oral Evidence – MI5, 10 October 2013.*

210 *Oral Evidence – GCHQ, 24 October 2013.*

211 *GCHQ's contribution is to illuminate overseas strands, such as attack planning or co-ordination from overseas, facilitation routes and networks, extremist training camps, or travel plans of key extremist figures.*

212 *Oral Evidence – MI5, 10 October 2013.*

213 *Written Evidence – MI5, 3 October 2013. GCHQ's decision to provide support takes into account factors such as whether they will be able to access the communications; whether there are any technical issues ***; and if any linguistic capabilities are needed (and available) to translate them.*

Where GCHQ did support MI5's operations, GCHQ reporting (***) comprised about ***% of the overall intelligence contribution.

181. A further issue is whether the division between GCHQ's work on overseas interception and MI5's work on domestic terrorism is as clear cut as it once was. The Home Secretary told the Committee that she felt the role of GCHQ was evolving, and that the balance between GCHQ and MI5 resource and expertise in areas such as digital intelligence may change in future as a result:

> [In terms of] *the role of GCHQ and the relative role of GCHQ domestically and internationally… this is something that… has been changing, but I think actually there will be a point at which there is a genuine question to be asked about where that role should sit and what the balance between those two should be, and in a sense, depending on that answer, depends on the extent to which it would be necessary to retain the capability within the Security Service.*[214]

(iii) Records management

182. Even once the DIGINT team had identified Adebowale in November 2011, there was a further delay of five months before the Operation FIR team began their investigation into Adebowale in April 2012.

183. MI5 has been unable to establish the reason for this delay – largely because, although they know that the DIGINT team completed their enquiries in November 2011, they do not know when the results of those enquiries were passed back to the FIR investigative team. MI5 explained that this was because:

> *… the document on which the intelligence is recorded and developed by the DIGINT team is a single document that gets iteratively updated as more information is added.*[215]

This single document was shared by the investigator and the DIGINT team, and there is therefore no audit trail to establish at what point responsibility passed back from the DIGINT team to the investigative team.

184. In both Adebolajo's and Adebowale's cases, the Committee has seen numerous examples where MI5 has been unable to confirm from their records what information was known at a particular point in time, and when decisions were taken. We have identified three records management issues in particular:

(i) **Drafts not kept:** As can be seen from this particular instance, MI5's records management system updated this 'live' working document without keeping earlier versions of the document or recording when updated drafts were created. We have also seen examples of other documents, such as applications to the Home Secretary, where earlier versions were not kept. There is therefore not always a clear chronology, to enable an understanding of when changes were made and why.[216]

---

214 *Oral Evidence – Home Secretary, 21 November 2013.*
215 *Oral Evidence – MI5, 10 October 2013.*
216 *Oral Evidence – MI5, 10 October 2013.*

(ii) **Lack of narrative:** Investigative officers were not required to record all investigative decisions (in particular when they decided not to do something).

(iii) **Lack of dates:** Numerous documents we examined in the primary material do not have a specific date: some have the quarter in which they were written; some have no date at all.[217]

185. MI5's Director General has accepted that records management is an issue in some circumstances:

> *… a particular one where that has caused us a problem in being able to understand the chronology was in relation to the DIGINT intelligence collection document, which is a spreadsheet which is updated and then you lose the previous version. I absolutely accept that that's something that we should – we need to move on with, to a way in which we can see back into the history of it and what happened. And we are – part of our lessons learned is to change that. So I think we absolutely take that…On the narrative question and around the investigation, we agree with that too.*[218]

186. MI5 has told the Committee that they are changing their records management process as a result of these concerns:

> *As part of our efforts to continually improve our recording of investigative decisions, in April 2013, we decided on the introduction of a new policy which states that investigative decisions should be recorded as part of the Investigative Narrative on our Intelligence Platform (IP)… where we store our corporate records. This process is now being implemented into the training of all new investigative desk officers.*[219]

187. The Director General expanded on this to explain that the new system of narrative recording will include:

> *Decisions about suspension, decisions about shifting resources away, why – to have that in the record, as part of a narrative in the investigation, is something that we are implementing.*[220]

R. We recognise the pressures that investigative teams are under. Nevertheless, MI5 must maintain comprehensive records and ensure that there is a complete audit trail.

(iv) Management of 'umbrella' operations

188. While MI5's Director General assessed the timescale for Adebowale's case as 'normal' for a low priority investigation, MI5 has nevertheless recognised that the way 'umbrella operations' like Operation FIR are run increases the likelihood of delays:

> *The fact that multiple lead operations often contain SOIs who have no direct links to each other can make it challenging to manage investigative progress against every*

---

217 *MI5 has explained that the electronic versions of documents have dates linked to them electronically, to show when they were created, written and last updated.*

218 *Oral Evidence – MI5, 12 December 2013.*

219 *Written Evidence – MI5, 31 October 2013.*

220 *Oral Evidence – MI5, 12 December 2013.*

SOI contained in the operation and to assess the differing risks they present. At times there is therefore a lack of consistency across investigative teams about how they should be reviewing the leads and associated risks within multiple lead operations. This is less of a challenge for investigations which are centred on activities of a network where the risk is more easily defined and the interconnectedness of the SOIs means investigative progress can be more readily tracked.[221]

189. MI5 has identified this as a 'lesson learned':

We will… develop best practice for managing multiple lead work, with particular reference to formally monitoring progress and tracking/ reflecting levels of risk.[222]

S. The eight months it took for MI5 to start investigating Adebowale (three months to identify him followed by five months of inaction) is unacceptable. In retrospect, we can see that the time taken did not affect the outcome in this case. However, this does not excuse the delay. There is a problem with the time taken to investigate low priority cases and MI5 must seek to address this by introducing deadlines.

[221] *Written Evidence – MI5, 7 February 2014.*
[222] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

OPERATION FIR: INVESTIGATING ADEBOWALE

190. When, in April 2012, the investigative team started investigating Adebowale, they created a Corporate Investigative Record[223] on him. The team then conducted routine investigative enquiries into Adebowale, including analysis of his communications data, checks with the police, ***, assessments of his financial situation, and open source analysis.

(i) Telephone analysis

191. MI5 used their databases of historical Subject of Interest (SoI) contacts to identify who Adebowale's telephone number had been in contact with during the period April 2009 to October 2011.[224] The analysis of this data revealed that Adebowale had been in contact with a number of (***) Subjects of Interest to MI5,[225] most of whom were based around South East London (***).[226]

192. One of these SoIs was Adebolajo,[227] who at that point was being investigated under Operation DOGWOOD (see previous section, from paragraph 100 onwards). The data also showed that Adebowale had been in contact with an individual named *** (SoI CHARLIE) on two occasions in 2009.[228] While SoI CHARLIE was, by 2012, a high priority SoI, he had not been under investigation by MI5 in 2009. (Further attempted contact between Adebowale and SoI CHARLIE in April 2012, which was not seen by MI5, is discussed later at paragraph 351.)

193. MI5 also carried out retrospective billing data analysis relating to Adebowale's telephone number for the period between February and April 2012.[229] During this period, Adebowale had had contact with only a few Subjects of Interest. ***.[230] This suggested to the investigative team that his contact with extremist Subjects of Interest had by then decreased.

194. While MI5's investigative team carried out analysis of Adebowale's communications data,[231] it did not conduct any more intrusive investigation (***).

195. The Committee questioned why further intrusive measures were not carried out at this stage, and was told:

> *He was not at, or near to, the threshold that we apply for the most intrusive monitoring into people's private lives.*[232]

---

223 *A Corporate Investigative Record is a centrally retrievable summary of all the intelligence held on an individual. It justifies why enquiries into that individual are both necessary and proportionate.*

224 *This was authorised under internal RIPA authorisation.*

225 *Written Evidence – MI5, 31 October 2013.*

226 ****. (Written Evidence – MI5, 17 February 2014.)*

227 *Analysis of Adebowale's communications data revealed that his telephone had been in contact with Adebolajo's number in August 2010.*

228 *These calls were in October and November 2009 ***. (Written Evidence – MI5, 10 March 2014.) MI5's investigation into SoI CHARLIE did not begin until February 2011.*

229 *Telephone billing data analysis continued throughout the period Adebowale was investigated under Operation FIR.*

230 ****.*

231 *Communications data refers to the fact of a communication, but does not include the content of that communication. For example, communications data might reveal that a telephone call had been made, but not what had been said during that call.*

232 *Oral Evidence – MI5, 10 October 2013.*

The Director General explained that such intrusion as a result of what they knew about him at that stage would not have been proportionate:

> *** *the* [FIR] *information… falls some way short of the threshold* ***.[233]

(ii) SO15 assessment

196. The investigative team asked the Metropolitan Police Service for any traces and records held on Adebowale. SO15 responded to MI5's request with details of Adebowale's criminal history, but confirmed they held no counter-terrorism records:

> ***.[234]

197. However, the Committee was told during its Inquiry that SO15 had previously been aware of an uncorroborated (and unreliable) allegation that Adebowale had been part of Al Qaeda. ***. This intelligence had been flagged for the attention of SO15 at the time. However, there is now no record of SO15's assessment of the intelligence, nor of any action taken by them.[235]

198. These circumstances, and the allegation that Adebowale was part of Al Qaeda, were not mentioned to the MI5 team investigating Adebowale in 2012. The Committee was surprised at this omission, given that it related to allegations of involvement in extremism. However, Assistant Commissioner Cressida Dick told the Committee:

> *I would not have expected MI5 to be informed of that information.*[236]

She explained that, while the allegation was serious, neither the source nor the content were at all credible:

> ***. *When you look at the content of it, it does not look tremendously sort of credible in many respects. ***. It was assessed as the sort of thing people sometimes say.* *** [it was] *a rather ridiculous excuse. ***.*[237]

199. The Committee asked MI5 whether they would have expected to have seen this intelligence in 2012, and whether it might have made a difference to their investigation. MI5's Director General responded that, while he did not know why the police did not pass on the information to MI5, he did not believe that it would have been material. Now that they had seen the intelligence, MI5 assessed that it would not have made any difference:

> *… we absolutely agree with the police that it was a completely rubbish accusation. We would attach no weight to it at all.*[238]

T. We accept that a historical allegation – that Adebowale was part of Al Qaeda – lacked credibility. We therefore do not believe the failure by the police to share this information with MI5 made any difference to MI5's actions in investigating

---

233 *Oral Evidence – MI5, 12 December 2013. ***.*

234 *Primary material (Adebowale), Metropolitan Police Service, 19 April 2012.*

235 *It is possible that this information was recorded at the time, but then lost during a later upgrade of the police's records system, known as Crimint (Written Evidence – Metropolitan Police Service, 30 August 2013).*

236 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*

237 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*

238 *Oral Evidence – MI5, 10 October 2013.*

Adebowale. Nevertheless, when MI5 requests information from the police, the police should ensure that all information held – whatever their assessment of it at the time – is shared with MI5.

(iii) WECTU assessment

200. MI5's investigative team discovered that Adebowale was at that point (April 2012) studying Arabic at the European Institute of Human Sciences in Wales. The investigative team therefore made enquiries with the counter-terrorist police in Wales (a unit known as WECTU – the Welsh Extremist and Counter Terrorism Unit).[239]

EUROPEAN INSTITUTE OF HUMAN SCIENCES

The European Institute of Human Sciences (EIHS) is a residential Islamic college located near Ceredigion in Wales, founded in 1998 by a group of Iraqi Islamic clerics as a registered charity. Its principal aim is to provide Islamic teaching to underprivileged Muslims. This teaching concentrates on Qur'an studies, Arabic, Sharia and Islamic jurisprudence.

The police have told the Committee that the college has followed a moderate ethos, aiming to integrate students with the local community. ***.

However, the college lost its academic accreditation in 2005 (apparently due to concerns over the level of academic rigour) and is believed to have mounting debts. Although the current principal is believed to be trying to raise funds to pay off debts and resurrect the college, it is currently unable to offer any courses, and largely stands empty.

201. The Committee considered whether Adebowale's choice of college might have been significant, particularly in light of the fact that it had lost its academic accreditation in 2005, and questioned what assessment MI5 or the police made of the institution. MI5 told the Committee:

> *… we do… try to keep an assessment of where extremist meeting places are, whether religious or academic or whatever. And the college in Wales where he was* [studying was] *looked at and considered to be moderate, it was not an extremist place.*[240]

202. Officers in WECTU made enquiries about Adebowale. They found no suggestion that Adebowale had been involved in any trouble while a student at the EIHS: he was thought to be a good student who had never caused any problems. Adebowale was believed to have converted to Islam in order to move away from the crime gangs and drugs scene he was involved with in London.[241]

203. The Committee noted that this assessment of Adebowale's conversion to Islam differs from that given by SO15 Counter-Terrorism Command in London. SO15 had suggested to MI5 that:

---

[239] *WECTU is a collaboration of the four Welsh police forces. It is a Counter-Terrorism Intelligence Unit which responds to the threat posed by international terrorism and domestic extremism in Wales. It is part of SO15's regional network.*

[240] *Oral Evidence – MI5, 10 October 2013.*

[241] *Primary Material (Adebowale), WECTU, 2 May 2012.*

… it is probable that his conversion was in some part due to his association with likely Somali gangs in Woolwich and not, as often is the case, due to pressure from associates in the prison system.[242]

204. Given the differing accounts provided by the two sections of the police, the Committee questioned the Assistant Commissioner on how these assessments had been reached. She explained that the officer in WECTU:

*… actually went further than the request ***. I think actually, she may also at some stage have spoken to Mr Adebowale himself… I think she did more than she was asked and she* [WECTU] *made a reasonable assessment.*[243]

205. The Assistant Commissioner considered that the assessments were not necessarily contradictory, because:

… different [individuals] *have different information and put slightly different slants on perhaps the same information.*[244]

206. The Committee asked MI5 how much weight they had attached to the assessments made by the police, and particularly that from WECTU, which seemed to indicate that Adebowale was moving away from extremist activity. MI5 put the information into context, saying:

The WECTU report was, you know, one piece of [the overall assessment] *and him moving away from crime was a fragment of a larger picture.*[245]

(iv) Closing the investigation

207. By June 2012, MI5 had conducted a number of enquiries and checks. They explained to the Committee that:

The investigation had revealed a reduction in contact with SOIs and an absence of police counter-terrorism traces which led us to assess he had disengaged from extremist and criminal activity perhaps as a result of him being located away from the influence of his criminal and extremist associates in London. We assessed at this point that Adebowale did not pose a threat to national security.[246]

208. MI5 therefore closed their investigation into Adebowale in June 2012. The Committee tested whether, in the light of subsequent events, MI5 still believed this had been the right decision. The Director General confirmed that they stood by the decision, which had been based on what they knew at the time:

I am absolutely confident, having gone back over it, that we made the right decisions, based on the circumstances. So this is a man who goes to a moderate college to learn Arabic, who has converted to Islam, and who has some degree, but diminishing, range of contact with people that we are concerned about; and who we get the

---

242 *Primary Material (Adebowale), Metropolitan Police Service, 19 April 2012.*
243 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*
244 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*
245 *Oral Evidence – MI5, 10 October 2013.*
246 *Written Evidence – MI5, 30 August 2013.*

*police report from… we do financial enquiries. *** The overall picture, based on all of that, rightly, was that this is not somebody at the time who is involved actively in violent extremism that we need to investigate further. So we did not, and so we closed it, and that was the right decision.*[247]

U. The Committee considers that, in the circumstances, the decision to close the investigation into Adebowale in June 2012 was reasonable. It was based on the intelligence available to MI5 at the time, which suggested that Adebowale was moving away from his extremist associates.

[247] *Oral Evidence – MI5, 10 October 2013.*

OPERATION FIR: FOLLOW-UP

209. At the point at which an investigation is closed, there are various options available to discourage a Subject of Interest from re-engaging with extremist activity. These options depend on the individual concerned: certain options may not be appropriate for some individuals. Options might include referral to the police for a non-terrorist criminal investigation, if appropriate, or referral to the Government's *Prevent* programme.[248] In many cases, however, no further action is taken. In May 2012, shortly before ceasing the investigation into Adebowale under Operation FIR, discussions were held as to whether to refer Adebowale to the police's *Prevent* case management process.

PREVENT AND THE CHANNEL PROJECT

Prevent is one of the four elements of the Government's counter-terrorism strategy, CONTEST (the others being *Pursue, Protect* and *Prepare*). The *Prevent* strategy:

- responds to the ideological challenge the UK faces from terrorism and aspects of extremism, and the threat we face from those who promote these views;
- provides practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support; and
- works with a wide range of sectors (including education, criminal justice, faith, charities and health) where there are risks of radicalisation.

The Channel project, which operates under *Prevent,* is a multi-agency project to identify and support people who are at risk of radicalisation across England and Wales. 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 are one of a number of bodies who assist in identifying suitable individuals for referral to *Prevent*. [249]

210. The internal discussions concluded that referring Adebowale to *Prevent* was not an option to be progressed. ***:

> ***.[250]

211. ***.[251] (***.)

Co-ordination with the police

212. When making the decision whether to refer Adebowale to a *Prevent* programme, the police were not consulted. In evidence from the Metropolitan Police Service, the Assistant Commissioner said that she would not necessarily have expected the police to

248 ***.
249 *Written Evidence – Metropolitan Police Service, 30 August 2013.*
250 ***.
251 ***.

have been involved in this discussion, given that the investigation was in the early stages. The police explained:

> *His name was referenced in a Channel meeting, but one of a large number of Channel referrals considered at that point. But given ***, the absence of police involvement in him as an individual, it would be quite normal for the Channel unit to accept the *** view that* [there were alternative options] *for that individual.*[252]

213. We are concerned that this approach did not provide the police (who play a key role in facilitating referrals to the Channel project) with the opportunity to offer their opinion. The Committee has been told that this has been addressed and, in future, where a Senior Investigating Officer (SIO)[253] has been appointed in a case, there will be *"a Prevent tactical adviser sitting next to them, to think through what are the Prevent options"*.[254] Whilst this is reassuring, it will still only happen in cases where an SIO has already been appointed. This leaves a number of cases where a *Prevent* tactical adviser may not be involved.

V. The police should always be consulted when considering whether an individual might be referred to a *Prevent* programme: this should include low level cases where the *Prevent* programme could potentially have the greatest impact.

Prevent referral?

214. The Committee questioned whether the right decision was made in not referring Adebowale to *Prevent*. ***:

> ***.[255]

215. ***. Where vulnerable young people are trying to move away from extremism, the *Prevent* programme can offer a successful outcome long term. For those on the periphery of extremism, their ability to move away from extremist associates towards a more constructive and fulfilling lifestyle might not only be the best outcome for them, but might also serve as a useful example to others.

216. Given this, there ought to be a more complex assessment of individuals, to determine in each case what might be the best approach.[256] When making an assessment of the best approach to take, the involvement of experts in the police and other agencies is important, as they bring different skills which can be combined to enable a more holistic approach tailored to suit each individual case. It is essential that *Prevent* options are given proper consideration. The evidence we have seen suggests that *Prevent* was not given sufficient priority, ***.

217. ***:

> ***.[257]

---

252 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*

253 *An SIO is a police officer appointed to help manage an investigation, leading the police interaction and developing a joint tactical strategy with the MI5 lead. More detail on this role is provided in paragraph 300.*

254 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*

255 ***.

256 ***.

257 ***.

218. ***.

219. It is difficult to assess whether a referral to a *Prevent* programme such as Channel might have been successful. The police have provided the following information on the Channel project:

- The Channel project has assessed over 3,000 referrals from various sources on the basis of radicalisation. [258]
- Of these, 600 (20%) have been deemed to be vulnerable to radicalisation, and have received a "*multi-agency support package*".[259]

These statistics do not measure the success of a referral, and therefore it is difficult to assess how well the scheme works. Nevertheless, it might have offered an opportunity to persuade Adebowale to turn away from extremism.

220. The Committee has also already noted that there was no consideration given to the possibility of Adebolajo being referred to the *Prevent* programme (see paragraph 44). While the Channel programme did not exist when Adebolajo was first investigated, by 2009 it had been set up in the area where Adebolajo was thought to be living, and it had been introduced nationally by April 2012. By this point Adebolajo was still under investigation ***; consideration should therefore have been given as to whether a referral to the Channel programme might have provided an opportunity to encourage Adebolajo to turn away from extremism.

W. Neither Adebolajo nor Adebowale was referred to *Prevent* programmes. A referral to the *Prevent* programme may in many cases be the best outcome for a vulnerable and impressionable individual. A more holistic approach should therefore be taken when deciding whether to refer Subjects of Interest to *Prevent* or whether to take a different route, to ensure the views of all stakeholders are considered.

[258] *This figure includes the original Channel programme pilot phase.*
[259] *Written Evidence – Metropolitan Police Service, 10 December 2013. (***.)*

221. MI5's investigation into Adebowale had included analysis of his communications data, enquiries with the police, ***. MI5 had found no intelligence to indicate involvement in violent extremism, and therefore closed its investigation into Adebowale in June 2012.

222. However, very shortly afterwards, Adebowale again came to the attention of the intelligence and security Agencies. An unknown individual (not at this stage identified as Adebowale) had been espousing extremist views online. ***.[260]

223. GCHQ reported that these views included references to operating as a lone wolf (or lone actor), and other general extremist remarks. (***.)[261]

224. ***.

225. ***:

***.[262]

***.[263]

226. ***.

227. In terms of a 'counter-narrative' to views such as those espoused by Adebowale, the Home Office said that the cross-government Research, Information and Communications Unit (RICU) has targeted material produced by extremist groups and has challenged material that encourages people to travel to Syria. The effectiveness of this work is currently being assessed. There may be scope to expand it if it proves successful.[264]

260 ***.

261 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013* ***.

262 *Oral Evidence – MI5, 10 October 2013.*

263 ***.

264 *Written Evidence – Home Office, 24 February 2014.*

THE RESEARCH, INFORMATION AND COMMUNICATIONS UNIT

Established in 2007 as part of the Office for Security and Counter Terrorism in the Home Office, RICU aims to co-ordinate government-wide communications activities to counter the appeal of violent extremism. It does this by:

- advising partners on their communications related to counter-terrorism;
- exposing the weaknesses of violent extremist ideologies and brands; and
- seeking to influence audiences overseas and domestically away from extremist ideologies and promote stronger grassroots inter-community relations.

RICU is composed of research and communications specialists. It is staffed and directed by the Foreign and Commonwealth Office and the Home Office.

228. ***.[265]

229. In terms of law enforcement, the police (through the specialist MPS Counter-Terrorism Internet Referral Unit) have the power under the Terrorism Act 2000 to enforce the removal of illegal content where it is hosted in the UK. However, most extremist content is hosted overseas, and the police have no power to remove material overseas: they are reliant on industry doing so voluntarily.

230. The Home Office has told the Committee that, as a result of the Extremism Task Force, they are working on options for restricting access to unlawful terrorist-related content which is hosted overseas but which may give rise to offences under UK law. ***.[266]

X. Whilst the Home Office's Research, Information and Communications Unit has done some work around a counter-narrative, this does not seem to have been prioritised. More work should be done to deter people from accessing extremist material online.

Assessment of the extremist views

231. The views expressed by the then unknown individual, in particular the reference to a lone wolf, are at first sight striking. The Committee questioned MI5 as to the significance they attached to them. MI5 advised that these sorts of views are in fact relatively common, and are not necessarily a precursor to carrying out a violent act. The Director General explained:

> *… those sorts of things said, and worse, on these sorts of* [sites] *are very common; and the challenge that we have is to try to discern rhetoric from intent in these things… The vast majority of it, *** translates into no action at all. No action at all.*[267]

---

[265] *Written Evidence – Home Office, 11 December 2013.*

[266] ****. (Written Evidence – Home Office, 11 December 2013.)*

[267] *Oral Evidence – MI5, 10 October 2013.*

Y. Despite appearing significant, the Committee notes MI5's assessment that the extremist remarks made online by Adebowale in 2012, including reference to lone wolf attacks, are common extremist rhetoric. Nevertheless, such comments – as on this occasion – may turn out to display more serious intent, and must be investigated on a case-by-case basis, taking into account all the intelligence known about the individual.

LONE ACTORS

232. The idea of a 'lone actor', an individual acting entirely independently, as so often portrayed in the media, is misleading. Roshonara Choudhry (who was jailed for life for attempting to murder Stephen Timms MP) was a very rare example of a lone actor: she was radicalised after having watched Anwar Al Awlaki's[268] sermons online, but had had no contact with other extremists.

233. By contrast, those involved in extremism and terrorism are usually in contact with other extremists to some extent. While there may have been a move away from attacks that are directly organised by Al Qaeda leadership (such as the failed printer cartridge bomb plot orchestrated by AQAP in 2010), those who MI5 now see planning terrorist attacks have usually nevertheless been in contact with other extremists and received inspiration or encouragement from others.

234. MI5 has told the Committee that they believe that, while Adebowale and Adebolajo were in contact with other extremists, they planned the murder of Fusilier Lee Rigby without external support, tasking or direction.[269] In relation to how far this fitted their concept of a 'lone actor' attack, they provided the following assessment:

> *Neither Adebolajo nor Adebowale fit neatly into the definition of a lone actor.*[270] *In both cases, MI5 had become aware of their extremist mindset through contact with more prominent Islamist extremists prior to the murder of Lee Rigby. However… we consider that the actions of Adebolajo and Adebowale in relation to the murder of Lee Rigby were broadly typical of the lone actor threat.*[271]

235. There appears to be a distinction between true 'lone actors' such as Roshonara Choudhry and individuals such as Adebowale and Adebolajo, who had both been in contact with other extremists (albeit they were not directly controlled or tasked by them). Rather than 'lone actors', these individuals might more accurately be described as 'self-starting terrorists': extremists who seek encouragement or inspiration from extremists such as Al Qaeda leadership, but who then plan and conduct their own attacks without external direction.

Z. The concept of 'lone actors' when applied to individuals such as Adebowale and Adebolajo is misleading. Such individuals – who are in contact with other extremists and seek inspiration and encouragement from them but who plan their own attack – are more accurately seen as 'self-starting terrorists' rather than 'lone actors'.

Identifying such individuals

236. The Committee questioned the Home Secretary on her views of 'self-starting terrorist' style attacks, and the threat they were likely to pose in future. She considered that the type of attack seen in Woolwich was likely to become more prevalent:

---

268 *Al Awlaki was AQAP's external operations commander – ***.*

269 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

270 *MI5 defines a Lone Actor as: "… an individual inspired by an ideology to conduct an attack but operating independently, having had no significant interaction with a terrorist group". (Written Evidence – MI5, GCHQ and SIS, 30 August 2013.)*

271 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

> *… in the past, the assumption was that groups were operating to, if you like, an al-Qaeda franchise, they had that sort of instruction, that… linkage back to* [the formal leadership structure]. *Increasingly you'll see groups that will operate without that linkage, but based on the same ideology, and then others who will come together which are… much more disparate… but just people who will come together in a variety of forms, and harder therefore to identify…*[272]

237. MI5 has in the past had considerable success in foiling centrally orchestrated Al Qaeda plots. Whilst these plots were complex, the fact that they involved more people and therefore more communications offered more opportunities to discover them. By contrast, this new threat involves simpler plots involving very few people: the fact that these individuals are often operating independently means that there is less likelihood of detecting them.

238. The threat from extremists who are outside Al Qaeda's command structure or franchises therefore presents MI5 with a significant challenge. MI5 has explained to the Committee:

> *In order to maximise our chances of detecting* [such individuals]*, we use a set of factors identified as being common – but not unique – to many lone actors: an inability to cope with stress and anxiety; a pre-existing history of violence; mental health issues; blaming others for (personal or group) grievances; an immediate need to act to rectify grievances; social isolation; and significant interest in extremist material encouraging lone actor attacks. We use the factors – drawing on psychologists in our Behavioural Science Unit (BSU)*[273] *where appropriate – in conjunction with other intelligence to inform risk assessments.*[274]

239. However, the Director General was clear that in terms of this particular threat they were heavily reliant on information received from the public:

> *… our challenge with finding lone actors is… and it is partly a police one about encouraging members of the public to come forward with things that are not right, that they see; and what we can do, in consulting with GCHQ, looking at odd things on the internet.*[275]

Prioritisation of this threat

240. The Committee asked the Director General whether MI5's current processes – which are broadly network-based – are sufficiently flexible to deal with the newer threat coming from individuals who act without external direction. He considered that:

> *I think what we have is an increase… a threat which is diversifying and is increasingly complex, because these methods are added. Nothing else falls off. We still have many different methods and many different sources of threat; and so our model that we have given the Committee a briefing about, for risk management, needs to continue to adapt, be dynamic, move on, adapt to the shape of the current threat.*

---

[272] *Oral Evidence – Home Secretary, 21 November 2013.*
[273] *The BSU is a team within MI5 of behavioural and social science specialists. For more detail, see paragraph 286.*
[274] *Written Evidence – MI5, 3 October 2013.*
[275] *Oral Evidence – MI5, 17 October 2013.*

And certainly lone actors are part of that picture, and must be; and not losing sight of the individual is central to that.[276]

241. While the Committee recognises that MI5 must have a framework to manage and prioritise its operations, it needs to ensure that this framework is flexible enough to deal with the increasing threat posed by 'self-starting terrorists'. So, for example, at present the examples used for Priority 2 investigations (large-scale fundraising, significant terrorist training, supply of false documents) are all relevant to networks rather than individuals. However, Priority 3 investigations relate to uncorroborated intelligence. The Committee was concerned that there was therefore potentially a 'gap' when it comes to individuals on whom there is corroborated intelligence but who are not part of a network.[277] MI5 has reassured the Committee that *"the current prioritisation system is a flexible process"* and that *"an individual can be investigated under a P2H/M if they are engaged in extremist activities on their own as opposed to a network"*.[278]

AA. There is an increasing threat from 'self-starting terrorists'. Whilst the plots involved are often less sophisticated than those co-ordinated by Al Qaeda, the fact that these individuals operate more independently offers fewer opportunities to detect them. MI5 must ensure that its prioritisation framework is sufficiently flexible to deal with the threat from individuals as well as networks.

---

[276] *Oral Evidence – MI5, 17 October 2013.*

[277] *Priority 2 High Risk operations are defined as investigations into individuals or networks where there is, for example, a serious intent to travel overseas to join jihad; large-scale fundraising; or significant terrorist training. Priority 2 Medium Risk operations are defined as investigations into individuals or networks where there is, for example, supply of false documents; or smaller scale fundraising. Priority 3 operations are defined as investigations into uncorroborated intelligence (or an ICT prisoner on release), where there are investigations or networks that require further action to determine whether they pose a threat. MI5's full definitions of priority levels are included at Annex A.*

[278] *Written Evidence – MI5, 23 April 2014.*

TIMESCALES FOR LOW PRIORITY OPERATIONS: LEADS PROCESSING QUEUE

242. When MI5 received the intelligence about an individual espousing extremist views in mid-2012, they created a new Lead (Lead ***, hereafter known as Lead A) to examine the intelligence and identify the individual concerned (***). It took two months – until 5 September – for the user to be identified as Adebowale.

NEW LEADS

Leads
A Lead is new intelligence not linked to an ongoing investigation that, following initial investigation, suggests activities of national security concern. Leads will be developed through intelligence channels to establish their credibility.

Triage Team
Leads received by MI5 and the police are dealt with by the Triage Team, using the Intelligence Handling Model (IHM). This provides a framework to ensure that resources are directed to the most credible new Leads.

Prioritisation
Leads are assessed through the 'RCAP' framework (Risk – Credibility – Actionability – Proportionality). Leads are allocated a risk status according to the nature of the reporting, and a grading according to the credibility of the assessment. *** (see Annex A).

Lead A

243. Lead A was not classed as an imminent threat and was of unknown credibility (***). The Lead included information from GCHQ which linked the individual concerned to a home address.[279] Under Operation FIR, MI5 had already linked that address to Adebowale; therefore, they should have been able to identify the individual as Adebowale immediately. However, the Operation FIR investigative team had failed to add the address to Adebowale's Corporate Investigative Record.

244. This meant that when, in July 2012, the Triage Team ran checks against the address it was not automatically linked to Adebowale. The Lead therefore sat in MI5's 'Leads Processing Queue' for six weeks, from 9 July to 23 August. It was only when a manual check on the address was carried out, searching in MI5's wider databases, that the Lead was connected to Adebowale.

279 ***.

THE LEADS PROCESSING QUEUE

When Leads first arrive in the Triage Team they are assessed and given a priority. Those which are urgent are dealt with straight away; those which are not urgent or time-specific are allocated to the Leads Processing Queue. Leads wait in this Queue until resources are available to look at them in greater detail.

A number of staff within the Triage Team work on the Leads Processing Queue (amongst other responsibilities). MI5 estimates that:

> *… a total of *** staff worked on the Leads Processing Queue at this time (principally at EO and HEO equivalent grade), with management oversight by *** SEO and *** Grade 7 equivalent staff (who would also have had other management duties)… *** police officers, who were based in ***, assisted MI5 work on Leads (*** Detective Sergeant and *** Detective Constables). These officers were line managed by a Detective Chief Inspector and an Inspector.*[280]

245. The Committee questioned MI5 on the failure of the Operation FIR team and the impact of the unnecessary delay while the Lead waited in the Queue. The Director General replied:

> *… even if we progressed to opening the P3 investigation much sooner than it happened, it would immediately have been one of those that was suspended during the Olympic period and following, while we were concentrating on high priority P1 and P2H cases... So that six week delay did occur due to an administrative oversight in an entry of that address onto the right system at the right time, and I think we need to acknowledge that and look at: is there anything we can do to make that less likely to happen? But I do not think it was material to the progress of the case.*[281]

Whilst this may well be true, it was nevertheless a failure of process. This was further compounded by the fact that even then the address was still not added to Adebowale's Corporate Investigative Record – it was not until February 2013 that the address was finally recorded.

BB. The failure of MI5 to add Adebowale's address to his Corporate Investigative Record caused unnecessary delay in the investigation. On the basis of the evidence we have seen, we agree with MI5's assessment that this did not have a material impact on the case. However, the fact that this failure in process happened not once but twice indicates a broader problem that must be addressed.

Lead B

246. Even after Adebowale was identified as the individual concerned, there was a further delay of ten weeks:

- On 5 September, Lead A was referred to Operation FIR (because Adebowale had previously been investigated under Operation FIR).

[280] *Written Evidence – MI5, 3 October 2013.*
[281] *Oral Evidence – MI5, 10 October 2013.*

- However, the Operation FIR team assessed the Lead but referred it back to the Triage Team, as their investigation only dealt with unidentified individuals.
- The Lead was therefore returned to the Triage Team with a recommendation to create a new investigation into Adebowale.
- The Triage Team therefore closed Lead A and created a new Lead (Lead ***, hereafter known as Lead B).
- This new Lead then waited in the Leads Processing Queue for a further ten weeks, from 5 September to 13 November.

247. The Committee questioned MI5 as to why the Triage Team created another Lead rather than creating an Operation. We also questioned why that new Lead was returned to the Leads Processing Queue (for assessment) when it had already been assessed. MI5 explained that the Triage Team does not solely assess Leads; they also have a role in approving the creation of new investigations, and in co-ordinating, prioritising and allocating resources for those investigations:

> *In this instance, Adebowale went back into the triage and co-ordination team in order to identify the appropriate investigative team and priority for the new investigation.*[282]

248. This explains why the Lead was returned to the Triage Team. However, for it to then wait there for a further ten weeks appears extraordinary. MI5 highlighted that:

> *… in the week that that intelligence came in, in July, we were pursuing* [several hundred] *leads nationally. So this is a process that is done at volume and the risk assessment needs to be industrialised in the way that we have done it, to keep track of all that.*[283]

249. Whilst we recognise the numbers involved, from our examination of the primary material we have seen that the expected timescale for the Triage Team's work was to respond to routine Leads within one to two weeks. In Adebowale's case, the response time was six weeks (Lead A) on the first occasion and ten weeks (Lead B) on the second occasion – both far in excess of the expected waiting time.

250. The Committee asked MI5 for the average length of time Leads of a similar priority spent in the Queue around this period. MI5 replied:

> *… we have compared the Adebowale Lead with broadly similar examples (***) from the time that this Lead was put into the queue. Comparable Leads spent a varied amount of time in the processing queue… This ranged from one to eleven weeks and the average being two to three weeks.*[284]

Both Adebowale Leads therefore took far longer than the expected time and the average time.

---

[282] *Written Evidence – MI5, 31 October 2013.*
[283] *Oral Evidence – MI5, 12 December 2013.*
[284] *Written Evidence – MI5, 10 January 2014.*

251. MI5 assured us that the Leads in the Queue are kept under review. Nevertheless, they have identified delays in the Leads Processing Queue as a 'lesson learned':

> *… we recognise that the delays which can occur in the 'queue' system for the processing and allocation of intelligence leads, while an inevitable consequence of the volumes involved, represent a risk for MI5…* ***.[285]

CC. Whilst we recognise the numbers and consequent pressures involved, the Committee was nevertheless seriously concerned to discover the length of time Adebowale's Leads waited in MI5's 'Leads Processing Queue' – far greater than either the expected time or the average time. Leads must be given a deadline, after which they should be escalated automatically to reflect the additional risk caused by being in the Queue for so long. Further, the length of time a Lead is judged to have been in the Queue should be based on the date of its original entry, rather than re-set if it is returned to the Queue.

[285] *Written Evidence – MI5, 30 August 2013.*

TIMESCALES FOR LOW PRIORITY OPERATIONS: RESOURCES

252. The delays did not end with the Leads Processing Queue. On 13 November, the Triage Team investigators sent the recommendation for a new investigation to managers for endorsement. However, it was not until 25 January 2013 – a further ten weeks later – that the recommendation was endorsed and Operation *** (hereafter known as Operation GUM, a Priority 3 investigation into the Islamist extremist activity of Adebowale) was created.

253. MI5 has explained that this ten-week delay was due to Olympics *"resource adjustments"*,[286] compounded by the diversion of resources onto an Intelligence Operations Centre (IOC) on a high priority investigation (Operation ***, hereafter known as IOC CARNATION).[287] MI5 has also stated that:

> *The nature of the Adebowale reporting (a proposed P3 investigation* [into uncorroborated activity]*) meant that even if it were moved into an investigation sooner it would have gone straight into immediate suspension.*[288]

254. The Committee is concerned at the length of time that intelligence can sit without being actioned by a desk officer: from start to finish it took six months to create an investigation into an individual who had espoused extremist views concerning lone wolves and who had previously had an interest in extremist media online. We have therefore considered the broader issues around how MI5 deals with low priority casework.

255. MI5's prioritisation system categorises investigations on the basis of assessed threat, and then allocates resources accordingly. Given the number of investigations that MI5 is running at any one time, this prioritisation framework is essential in order to ensure that the highest priority threats are dealt with swiftly and effectively.

256. Inevitably, lower priority casework is dealt with in a slower timescale. When there is a very high priority case which demands significant resource, the lower priority cases can often be paused or suspended for months at a time. MI5's Director General explained the scale of the problem:

> *So currently we have something like…* [a few hundred] *investigations covering* [over a thousand] *people. That is the P1 to P4 stack currently… but then there* [are also people] *that we have reason to be concerned about to some degree, and then there is… those who we've had an interest in, in the past, but now are closed… That is* [thousands of people].[289]

---

286 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

287 *IOC CARNATION ran from September 2012 to April 2013 in the IOC. It was a high priority investigation into intelligence that suggested there had been a credible terrorist plot to attack the UK: ***. (Written Evidence – MI5, 10 March 2014.)*

288 *Written Evidence – MI5, 10 March 2014.*

289 *Oral Evidence – MI5, 12 December 2013.*

NUMBER OF OPERATIONS RUN BY MI5

As context, MI5 has provided specific information on the number of operations which they were investigating as of 20 May 2013.[290] There were:

- (***) hundreds of open investigations (each one usually into a group of individuals), of which:
  - most (***) were live; and
  - around a fifth (***) were suspended.
- Of the live investigations there were:
  - a handful (***) of P1a (large scale attack planning) and P1b (small scale attack planning);
  - around a hundred (***) P2H (high risk activity);
  - over a hundred (***) P2M (medium risk activity);
  - fewer than a hundred (***) P3 (uncorroborated); and
  - fewer than 50 (***) P4 (dormant and disrupted).

MI5 has said that this volume of workload was broadly in line with the previous year, although there was a particular spike around the time of the Olympics.

Within these operations, there were over 1,000 Subjects of Interest (SoIs) who were being investigated. MI5 has told the Committee that there were *** people who were being investigated as Tier 1 and Tier 2 SoIs around the time Adebowale was being investigated.[291]

257. The Director General said:

> *We have a finite amount of resource and we need to focus it on the highest priority work. No delay is desirable, but it is the reality of what we do that we carry delays in lower priority casework…*[292]

Impact of IOCs

258. As explained previously, where MI5 has either a major covert investigation or a post-incident investigation, they open an IOC (see paragraph 77). During MI5's investigations into Adebolajo and Adebowale, both cases were affected by IOCs as follows:

- There were two IOCs opened, lasting for nearly three months in total, during the first investigation into Adebowale (August 2011 to June 2012).
- There were five IOCs opened between mid-2012 (when Adebowale came to MI5's attention for the second time) and the attack in May 2013.

[290] *MI5 Letter to the Committee, Interim Report, 28 June 2013.*
[291] *Oral Evidence – MI5, 10 October 2013.*
[292] *Written Evidence – MI5, 31 October 2013.*

- One of these (IOC CARNATION) was open from September 2012 until April 2013, during which time two further IOCs were also running concurrently.
- In Adebolajo's case, there was IOC ASTER (opened in August 2010) and IOC BLUEBELL (opened in November 2010) at the time he was arrested in Kenya in November 2010. Although both IOCs were closed in January 2011, MI5 has told the Committee that these IOCs caused the delay in not opening Operation BEECH until April 2011.

259. The degree of delay in Adebowale's case, and the three months taken to 'recover' from the IOCs in Adebolajo's case, highlight the impact that IOCs and high priority and resource-intensive investigations can have. Adebolajo's case in particular suggests that this impact is not limited to the time during which an IOC is running but can also continue for some months after it has closed. The closure of an IOC is not always an indicator that the investigation has closed: continued investigation may be necessary to contain the remaining threat. As officers are deployed back to their usual investigations, they must prioritise the highest threats. This means that it can take time for lower priority investigations, which will have been suspended or left with minimal resource, to be re-opened and get up to full speed again.

260. MI5's Director General confirmed that the effort needed to run an IOC reduces the organisation's capacity to continue work on lower priority cases:

> *When we run one of these IOC operations that we have talked about… it can take up* [a significant proportion] *of our investigative resource onto one case. The only way we can do that is by removing effort from other cases. We are not an army that has battalions waiting in barracks for deployment. We are fully deployed all the time, and so the only way to go on to high priority cases is to stop low ones.*[293]

261. The Committee asked the Home Secretary whether more resources should be made available to enable MI5 to continue lower priority casework whilst IOCs are in operation. However, she thought that any additional resources might still be allocated to the higher priority cases.

262. MI5's current funding model means that lower priority investigations are effectively paused or suspended whenever an IOC is opened. Consideration should be given to whether MI5 might operate a similar funding model to the MOD, whereby core funding enables routine work to continue and individual crises are funded from a separate reserve. In this way, IOCs could be run without sacrificing other investigations.

DD. We recognise the pressures on MI5 – in particular when they encounter significant and immediate threats to life. We are concerned that when there is a major investigation into attack planning (such that an Intelligence Operations Centre is opened) this may render them unable to continue lower priority casework. We find this unacceptable. We recommend that consideration be given to a funding model that allows for periods of high intensity work without that being at the expense of the rest of the organisation's work.

[293] *Oral Evidence – MI5, 12 December 2013. ***.*

Ability to escalate cases

263. MI5's Director General emphasised that, whilst they had to operate a prioritisation system, threat levels were continuously assessed. Therefore, if further intelligence indicating a threat was received, a low priority investigation could be escalated very quickly. He said:

> [The prioritisation framework] *is not an obstacle to agility. It is a discipline on the level of resources and pace, given that we have got a limited supply.*[294]

264. MI5 has confirmed that they could have increased the priority level of Adebowale's case instantly if, for example, further intelligence had indicated that an attack might be imminent:

> *Where there has been any indication of something that needs a time sensitive reaction, it is immediately referred.*[295]

265. The Committee asked the Home Secretary whether she was concerned about the level of risk being held at the lower priority cases. She emphasised the importance of MI5 being aware of the risk, saying:

> *I think they* [MI5] *do operate on a reasonable basis for these lower priority cases, but I think what's important is ensuring that they have the ability to escalate, which they do have, when it is clear that* [in] *a lower priority case, actually something has triggered that into being of more concern…*[296]

266. Whilst this is reassuring, there is nevertheless a question as to whether waiting for new intelligence to be received constitutes active management of a case. The Committee has been told that MI5 conducts quarterly case reviews of all its cases, in order to reassess the level of risk being held in each one. However, while these reviews might cover every operation, they do not cover every SoI within those operations. This therefore means that if no new intelligence has been received on an SoI, they are usually not reviewed. This can result in long periods of inaction. We believe all SoIs should receive regular reviews.

Impact of MI5's prioritisation of resources on Adebowale's case

267. The Committee questioned MI5 about the impact the priority levels had on investigations and on Adebowale's case, as a Priority 3 investigation, in particular. The Director General provided the following context:[297]

> *So at some point… what the state has done is to draw a line around: well, what is proportionate? And I think what we are seeing in these P3 cases, in particular, is where that limit is reached and runs out.*[298]

---

294 *Oral Evidence – MI5, 12 December 2013.*

295 *Oral Evidence – MI5, 10 October 2013.*

296 *Oral Evidence – Home Secretary, 21 November 2013.*

297 *He also gave his view that the priority level given to Adebowale's case (P3) was "correctly judged" (Written Evidence – MI5, 31 October 2013).*

298 *Oral Evidence – MI5, 12 December 2013.*

268. The Director General confirmed that Adebowale's case was a *"typical low priority investigation"*. He told the Committee:

> *I am confident that what we did, based on what we knew at the time, was reasonable and is typical of what happened at the lower end of our casework… it is perfectly normal in our business that there are pauses, there are suspensions, there are periods of inactivity and then activity again.*[299]

269. However, how far Adebowale's case was *"typical"* is debatable. The evidence the Committee has seen suggests that some of the delays in his case were unusual:

First investigation (initial intelligence – Operation FIR):

- It took eight months to identify Adebowale in 2011 and begin to investigate him, including a five-month period where MI5 has admitted no work was done and they do not know what caused the delay.

Second investigation (Operation GUM):

- After espousing extremist views online in mid-2012, it was six months until Adebowale was investigated under Operation GUM in January 2013, during which time the case spent 16 weeks waiting in the Leads Processing Queue rather than the average of two to three weeks.

Adebowale's case does therefore seem to have taken significantly longer than was typical for a low priority investigation.

270. There is a separate question as to whether the delays were formal decisions to suspend the case or were simply due to overload. MI5 operates a formal process for when cases are suspended. This does not seem to have happened in Adebowale's case. If there were conscious decisions to suspend Adebowale's case, these should have been recorded.

EE. We recognise that low priority cases will inevitably receive fewer resources and that this will impact on the length of time such cases take. However, in Adebowale's case, the delays were significantly longer than the average, without any obvious explanation. This highlights the need to reform the process through which low priority Subjects of Interest are managed.

[299] *Oral Evidence – MI5, 10 October 2013.*

TIMESCALES FOR LOW PRIORITY OPERATIONS: THE OLYMPICS

271. It is important to note that MI5 was under significant pressures during this period, due to the Olympic and Paralympic Games held in London in 2012. These pressures lasted from spring 2012 to spring 2013. In a letter to the Committee of 17 December 2012, the Agencies described the Olympic and Paralympic Games as *"the largest intelligence and security challenge in peacetime that we have yet undertaken"*.[300]

272. MI5 carried out background checks on one million accreditation applications for the Olympics. The pressure affected MI5 staff most severely from May to August 2012 (known as the 'red' period). A substantial backlog of annual leave was accumulated which had to be taken later in the year, and 'business as usual' staff moves between posts were delayed until spring 2013. The impact of these resource adjustments was primarily on low priority cases such as Adebowale's.

273. The Director General referred to the overall impact of the Olympics on lower priority cases:

> *… The delay thing, of course, we are talking about the Olympics period… but that is primarily the reason why P3 level casework, and so on, had less attention and less urgency during that period.*[301]

274. MI5 has clarified that this pressure was most acute during the 'de-surge' period after the Games had finished. The Director General said:

> ****. We suspended promotions, we suspended movements of staff between posts. And you know, we circulate people. So we had a sort of catch-up period of months after the Olympics, to get back to a sort of business-as-usual stance… So it is that third period that I was referring to when suspensions, and so on, happened…*[302]

Impact on investigations into Adebowale and Adebolajo

275. MI5 has provided the Committee with specific examples of where the Olympics had an impact during the period in which Adebowale and Adebolajo were being investigated:

- Part of the delay in opening the operation into Adebowale, while the Lead sat in the 'Leads Processing Queue', was due to the Olympics. (Even had the operation been opened earlier, MI5 has said it would have been immediately suspended, due to the resource pressures in the period after the Olympics.)
- *** was delayed until after the immediate Olympic period, as non-urgent casework was formally suspended.
- Suspension of the Programme BELAYA and Programme CONGO schemes, which were designed to monitor those not under active investigation but thought to pose some level of potential threat.

---

300 *Agency Heads' letter to the ISC, 'Lessons Learned from the London 2012 Olympic and Paralympic Games (L2012)', 17 December 2012.*

301 *Oral Evidence – MI5, 10 October 2013.*

302 *Oral Evidence – MI5, 12 December 2013.*

276. Nevertheless, it is worth noting that in evidence to the ISC in January 2013, the then Director General indicated that the pressures on MI5 during the Olympics had not been as significant as expected, saying:

> *… the actual number of cases that we had to run on the terrorism side over the Olympics was very low.*[303]

Moreover, these pressures and delays cannot solely be attributed to the Olympics. MI5 has said that delays in lower priority cases are not unusual at any time, due to their continuous prioritisation of resources.

FF. The Committee recognises that the security challenges of the Olympic and Paralympic Games placed MI5 under very significant pressure, and we commend their staff for their hard work in delivering a safe and secure Games.

[303] *Oral Evidence – MI5, 17 January 2013.*

OPERATION GUM: MISSED OPPORTUNITIES?

277. Once MI5 had decided to open an investigation into Adebowale, as a result of his extremist views, Operation GUM was created on 25 January 2013. MI5 categorised Operation GUM as a Priority 3 operation: investigating uncorroborated intelligence to determine whether Adebowale posed a threat to national security.

278. MI5 carried out a range of investigative actions under Operation GUM, including reviewing Adebowale's online activity, checking his communications data, and ***. Post-event analysis has revealed three areas where information was missed during Operation GUM:

(i) Retrospective billing data;

(ii) Handling of digital intelligence; and

(iii) An assessment by the Behavioural Science Unit (BSU).

(i) Retrospective billing data

279. The Operation GUM investigative team conducted billing enquiries on Adebowale's mobile phone. However, they did not conduct enquiries on the landline at Adebowale's home address.

RETROSPECTIVE BILLING DATA

The MI5 investigator may assess whether any of the telephone numbers associated with a Subject of Interest (SoI) should be targeted and, where they consider it necessary and proportionate, they may make a request for retrospective billing data for some of those phones. The billing data provides all telephone numbers called, and received, by the telephone in question.

280. MI5 has told the Committee that investigators do not follow a standard pattern of enquiries in all investigations. They have a number of options and requesting billing data is only one of those options. When billing data is requested, MI5 has told the Committee *"we tend to focus more upon mobile telephones as these are used most"*.[304]

281. Had MI5 requested billing data on Adebowale's landline, it would have revealed contact with a Yemeni telephone associated with an individual believed to be in contact with AQAP (***), hereafter known as SoI ECHO. Knowledge of Adebowale's telephone contact with someone associated with AQAP might have led to further investigative work, and further discoveries about Adebowale's contact with this individual. The significance of these contacts is discussed later (see paragraph 367).

(ii) Handling of digital intelligence

282. Under Operation GUM, MI5 reviewed Adebowale's online activity. ***.[305]

[304] *Written Evidence – MI5, 30 August 2013.*

[305] ***.

283. However, post-event analysis has revealed that there was further intelligence regarding Adebowale's online activity which was available at the time, but was not seen by the analyst or investigator. For example, MI5 was aware that Adebowale had contacted an SoI being investigated by MI5 under a different operation, referred to in this Report as Operation JUNIPER. (***.)[306] However, MI5 was not aware of the full extent of this contact, ***.

OPERATION JUNIPER (***)

Operation JUNIPER was an MI5 investigation into a suspected Al Qaida member ***.

284. MI5 has said that this further intelligence would have:

> *… added to our concern about the nature of their relationship and further contributed to the intelligence case* [against] *Adebowale.*[307]

285. The way investigators handle online material in investigations is one of MI5's 'lessons learned'. They have proposed new guidelines which include ensuring that investigators apply consistent thresholds for tasking formal reports based on online intelligence, recording which online intelligence has been seen in order to provide an audit trail, and the possibility of automatically notifying investigators when new intelligence is received.[308]

GG. The failure to identify the further intelligence that was available regarding Adebowale's online activity was a missed opportunity. It would have revealed additional contact between Adebowale and another Subject of Interest, contributing to the intelligence case on Adebowale.

(iii) An assessment by the Behavioural Science Unit

286. The third potential missed opportunity under Operation GUM was the lack of an assessment of Adebowale by MI5's Behavioural Science Unit (BSU).

306 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

307 ****. Post-event analysis has revealed that the content of the communication did not provide any indication of attack planning (Written Evidence – MI5, GCHQ and SIS, 30 August 2013).*

308 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

MI5'S BEHAVIOURAL SCIENCE UNIT

The BSU is a team within MI5 of behavioural and social science specialists.[309] They provide support to investigative desk officers so that they can understand their targets better, and advice to agent handling sections when they are considering a range of approaches to agent handling issues.

MI5 has provided the Committee with statistics for the number of requests the BSU receives each month:

> *For Q1 and Q2 2013/14 there were *** requests for BSU assistance over the six month period which as a crude breakdown measure would be *** per month. The 'levels' of support vary considerably; from a consultancy that might take a couple of hours to a really in-depth assessment that could take weeks to prepare.*[310]

287. Amongst the primary material, the Committee has seen the Investigation Referral Form[311] used to record the decision to create an investigation into Adebowale. On this form, under the 'Outstanding Actions' section, it says:

> [Investigative] *Team: Request BSU assessment re Adebowale's *** expressions of support for lone wolf attacks and other extremist views.*[312]

MI5 has explained that the BSU assessment was only an option suggested by the Triage Team to the investigative team, as opposed to a decision requiring action:

> *… this is advice from* [the Triage Team] *on referral to the investigative team of things that they might do…* [By the time of the attack, the investigative team] *had not decided, at that point, to progress the BSU assessment.*[313]

This suggestion was not taken forward by the investigative team, and therefore no BSU assessment was made of Adebowale before the attack.[314]

288. We further note that in the 'Assessment' section of the form, it says:

> *At the present time this justifies P3 priority. However, will need to be reviewed if Adebowale demonstrates a serious intent to engage in jihad or if BSU assessment or other intelligence indicates that he may seek to carry out a lone wolf attack.*[315]

---

309 *The BSU currently has *** staff, including an additional *** staff until the end of FY 2014/15 to support work on Terrorism Prevention and Investigation Measures (TPIMs).*

310 *Written Evidence – MI5, 10 January 2014.*

311 *An Investigation Referral Form is created by the Triage Team to record their actions in relation to new Leads, when they are referred to an investigative team for further work.*

312 *Primary Material (Adebowale) – MI5 Investigation Referral Form, undated.*

313 *Oral Evidence – MI5, 10 October 2013.*

314 *After the attack, MI5 decided to commission advice from the BSU on Adebowale, ***. The BSU's view was: "Their initial reaction (but not a considered and detailed assessment) was that the Islamist rhetoric – including the lone actor reference – was standard… and would not, in itself, mark this material out as particularly concerning" (Written Evidence – MI5, 31 October 2013). They would not therefore have expected the priority level to have increased from a P3.*

315 *Primary Material (Adebowale) – MI5 Investigation Referral Form, undated.*

This clearly indicates that the BSU assessment was considered relevant to the prioritisation of the investigation.

The Behavioural Science Unit and Adebolajo

289. BSU advice was also requested but not provided in the case of Adebolajo. Advice from the BSU was first sought in January 2012, ***. However, this was not taken forward.

290. BSU advice was again sought at a later date, when the BSU provided oral advice: ***. However, MI5 has admitted that they:

> *… do not hold any formal written evidence from the BSU on either Adebolajo or Adebowale from the time advice was sought and discussed.*[316]

291. This lack of BSU advice appears to indicate a failure of process. However, the Director General said that he was not concerned about the lack of formal records in response to such requests:

> *This is a working – a working arrangement between case officers and members of the BSU. They – you know, they phone each other, they chat multiple times a day on different cases and it is just, you know, how work happens. It is not a remote formal process.*[317]

292. Nevertheless, MI5 has told the Committee that the BSU has recently improved its system of recording its requests and the advice provided in response:

> *The BSU have very recently introduced a new system that records monthly referral statistics more accurately including detailing the type of support given and the length of time taken. In time this should provide the BSU with more information to assist in providing effective support to investigative desks and agent runners.*[318]

HH. MI5's Behavioural Science Unit would appear to provide a valuable input: MI5 should ensure that the unit's advice is integrated more thoroughly into investigations.

---

316 *Written Evidence – MI5, 14 November 2013.*
317 *Oral Evidence – MI5, 12 December 2013.*
318 *Written Evidence – MI5, 10 January 2014.*

OPERATION GUM: POSSIBLE EXECUTIVE ACTION

293. In March 2013, intelligence indicated that Adebowale had sought to disseminate extremist material. (***.) Such action could potentially have been illegal.[319]

Disseminating extremist material

294. MI5 aims to identify UK-based individuals who may have obtained or disseminated significant extremist publications. ***.[320]

295. ***.

296. Disseminating extremist material to a wider audience (***[321]) can potentially constitute an offence under the Terrorism Acts. MI5 explained that:

> *If an individual* [disseminates extremist material]*, this offers a potential opportunity for disruption of their activities.*[322]

THE TERRORISM ACTS 2000 AND 2006

The Terrorism Act 2000 reformed and extended previous counter-terrorism legislation and put it largely on a permanent basis. The Terrorism Act 2006 was introduced to reform and extend the previous counter-terrorism legislation and to ensure that the UK law enforcement agencies have the necessary powers to counter the threat posed to the United Kingdom by terrorism.

Disseminating extremist material could potentially be illegal under section 2 of the Terrorism Act 2006 (dissemination of terrorist publications) or section 57 of the Terrorism Act 2000 (possession of an article for terrorist purposes).

Difficulties bringing prosecutions

297. The Metropolitan Police Service Assistant Commissioner Cressida Dick explained to the Committee that offences under the Terrorism Acts related to possessing or disseminating terrorist material:

> *… are quite regularly brought to court. It is not tens and tens and tens every year. But certainly quite a considerable number… But the actual *** offence is quite a difficult one to prove.*[323]

The Committee asked why it was difficult to prosecute an individual for dissemination offences. The Assistant Commissioner said:

---

319 *Adebowale's actions could potentially have been illegal under section 2 of the Terrorism Act 2006 (dissemination of terrorist publications) or section 57 of the Terrorism Act 2000 (possession of an article for terrorist purposes).*

320 ***.

321 ***.

322 *Written Evidence – MI5, 31 October 2013.*

323 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*

> … *clearly,* [such] *intelligence… might lead to the potential for bringing somebody to justice. It is only intelligence and it is a very long way from getting evidence…*[324]

298. The police has provided the Committee with evidence that, during the period January 2001 to 31 October 2013, 132 people were charged with offences under sections 57 and 58 of the Terrorism Act 2000 and section 2 of the Terrorism Act 2006 (***). Of these 132 charges, there were 66 convictions (a 50% conviction rate).

Adebowale's potential dissemination of extremist material

299. After the MI5 investigative team had received this reporting, they wrote to SO15 on 5 April 2013 to provide details of their investigation into Adebowale. They requested a meeting to explore potential executive action options:[325]

> *Given that Adebowale is likely to have possessed* [and disseminated extremist material]… *we are keen to determine whether he has breached TACT* [the Terrorism Act]. *We would be grateful for your assistance in exploring executive action options and whether his activity could be captured evidentially.*[326]

300. By 16 April 2013, SO15 had appointed a Detective Chief Inspector as Senior Investigating Officer (SIO) and created a police investigative team. This team carried out checks on police systems to ensure that Adebowale was not subject to an existing Metropolitan Police Service investigation, and also conducted checks with external sources such as the DVLA.[327]

POLICE INVESTIGATIVE TEAMS AND SENIOR INVESTIGATING OFFICERS

In a 'significant' counter-terrorist operation, a Senior Investigating Officer (SIO) is appointed from the police, usually at the rank of Detective Chief Inspector. The SIO will help to manage the investigation, leading the police interaction and developing a joint tactical strategy with the MI5 lead. This process will be formalised through a Joint Operational Team (JOT). The JOT sets the tactical strategy: it ensures a common understanding of operational developments, and co-ordinates collection of intelligence and deployment of resources.[328]

301. On 19 April 2013, SO15 attended a meeting with MI5 to discuss what executive action or disruption options existed as a result of Adebowale's extremist activity. The SO15 SIO's opinion was that:

> … *if an arrest was undertaken at that stage, it was unlikely that sufficient evidence to support a charge would be obtained.*[329]

---

[324] *For example, intercept material can be useful intelligence but it is not admissible in court.*

[325] *Executive action can mean Terrorism Act searches, overt approaches and potentially (but not necessarily) an arrest.*

[326] *Primary Material (Adebowale) – MI5, 5 April 2013.*

[327] *Written Evidence – Metropolitan Police Service, 30 August 2013.*

[328] *When the police are close to taking executive action, an Executive Liaison Group (ELG) will be formed to co-ordinate action. There is no mention of any ELGs to investigate Adebowale (or Adebolajo) before the attack.*

[329] *Written Evidence – Metropolitan Police Service, 30 August 2013.*

302. The Committee questioned whether this decision was reasonable: with the benefit of hindsight, this might have offered an opportunity to arrest Adebowale before the attack occurred. The Assistant Commissioner said that, whilst:

> *There is a number of offences that* [Adebowale] *may perhaps have been involved in… as I think we have said in our report, section 58, section 57 and section 2* [of the Terrorism Acts]*… they are actually quite hard to evidence and they are quite hard to prove and the threshold is quite high.*[330]

303. The police explained the lack of evidence in Adebowale's case:

> *The opinion of the SIO was in part influenced by the intelligence case which indicated that ***. It was therefore unlikely, ***, for police to be able to directly link him to the* [dissemination] *of the material. In addition the intelligence case *** was based on information supplied by secret and sensitive sources*[331] *and therefore could not be readily converted into evidential material or relied upon exclusively as the basis of executive action.*
>
> *Concern was also expressed during this initial meeting that an early intervention would adversely impact on the likelihood of establishing Adebowale's true aspirations, any associates he was engaging with and the exact nature of the threat he posed.*[332]

***

***:

***.[333]

***:

***.[334]

***:

***.[335]

Authorisation for Agency activity relating to online extremist material

304. In order for GCHQ to attempt to identify UK-based individuals accessing or disseminating extremist material online, they would have to have a warrant from a Secretary of State under the Regulation of Investigatory Powers Act 2000 (RIPA). In October 2013, the Agencies' approach to such activity changed in two key ways:

(i) The ownership of this issue transferred from MI5 to GCHQ. This meant that responsibility for authorising any related RIPA warrant which should become necessary transferred from the Home Secretary to the Foreign Secretary.

---

330 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*

331 *The police teams would have been unaware exactly what these "secret and sensitive sources" were, but would have known that they would probably not have been admissible in court.*

332 *Written Evidence – Metropolitan Police Service, 30 August 2013.*

333 *Oral Evidence – GCHQ, 24 October 2013.*

334 *Primary Material (Adebowale) – GCHQ Report, 28 May 2013.*

335 *Written Evidence – MI5, 31 October 2013.*

(ii) The focus of their work broadened, covering more named extremist publications and encompassing historical versions. (***.)[336]

(i) Ownership

305. The Committee questioned why ownership of this issue was transferred. MI5 explained that:

> *… there may be a variety of reasons why responsibility for an issue, including authorising any associated operational activity, may transfer between Agencies – for example, it could be because the Agency that was doing the operational activity was in a better position to explain their capabilities, and describe the interference and risks to their Secretary of State.*[337]

306. Whilst this may make sense in practical terms, the impact at ministerial level is that the Home Secretary, as the Secretary of State responsible for tackling terrorism and extremism within the UK, would no longer retain the final responsibility for authorising any such applications.[338]

(ii) Broader focus

307. ***.[339] ***:

> ***.[340]

308. MI5 confirmed that any such authorisations would only permit the identification of people, and would not allow any monitoring of their other communications:

> ***.[341]

II. The recent transfer of responsibility from the Home Secretary to the Foreign Secretary for authorising any warrant under the Regulation of Investigatory Powers Act which should become necessary to identify access to extremist media online appears to reduce the Home Secretary's involvement in this area. The judgement as to whether intrusive action is necessary in counter-terrorism cases is largely a domestic issue, for which the Home Secretary should be accountable. Responsibility for any such decisions should therefore lie with the Home Secretary.

---

336 *Written Evidence – GCHQ, 18 November 2013.*

337 *Written Evidence – MI5, 28 August 2014.*

338 *The Home Secretary would be consulted on renewals of any such applications, although it would be the Foreign Secretary who would authorise them.*

339 ***.

340 *Written Evidence – GCHQ, 18 November 2013.*

341 *Oral Evidence – MI5, 12 December 2013.*

OPERATION GUM: FURTHER ACTIONS

309. Given SO15's assessment that there was insufficient evidence to prosecute Adebowale at that stage, further investigative work was taken forward by both MI5 and the police. MI5 aimed to:

> *… build further coverage of Adebowale. This will enable us to form a better assessment of how best to disrupt Adebowale's online extremist activity…*[342]

310. As part of this work, MI5 ***.[343] They planned to make further enquiries into Adebowale's recent enrolment onto an academic course, and they requested checks on Adebowale's finances. They also planned to apply to the Home Secretary for the authorisation of further intrusive techniques (***); this is covered in the next section. While carrying out these enquiries, the investigative team told SO15 that:

> *In the meantime, we are keen to determine whether it would be possible to capture Adebowale's* [extremist] *activity evidentially. This will enable us to make an informed decision on the likelihood that a prosecution of Adebowale would be successful should we decide that this would be the best disruptive option. We would be grateful for your views on this.*[344]

311. The police planned to launch a *"covert police investigation ***"* in an attempt to *"obtain effective evidence"* against him. *** plans for surveillance were also discussed.[345]

312. The MPS Assistant Commissioner told the Committee that another option considered at this point was whether there was sufficient evidence from the police to be able to execute a warrant to search Adebowale's house, although in the event this was not carried out. She confirmed that the police had a series of actions in hand, in consultation with MI5, and gave her view that:

> *I do not think there was ever any disagreement about what would be the best way to deal with this problem.*[346]

313. The police documented these options in an Investigative Strategy dated 26 April 2013. This stated that *"all intervention opportunities, including Channel/Prevent, will be considered and be in scope"*.[347] ***:

> ***.[348]

Efforts then focussed on applying for authorisation to use further intrusive techniques.

---

342 *Primary Material (Adebowale) – MI5, 25 April 2013.*
343 *Primary Material (Adebowale) – MI5, 25 April 2013.*
344 *Primary Material (Adebowale) – MI5, 25 April 2013.*
345 *Written Evidence – Metropolitan Police Service, 30 August 2013.*
346 *Oral Evidence – Metropolitan Police Service, 31 October 2013.*
347 *Primary Material (Adebowale) – Metropolitan Police Service, 26 April 2013.*
348 *Oral Evidence – MI5, 10 October 2013.*

OPERATION GUM: APPLICATION FOR FURTHER INTRUSIVE TECHNIQUES

314. A significant part of MI5's effort to build further coverage of Adebowale was their decision to submit an application to the Home Secretary to authorise the use of further intrusive techniques (***). MI5's Director General set the decision to request this coverage in context for the Committee, explaining that such intrusion is unusual for lower priority cases:

> *… it is roughly 20 per cent of our P3 casework that has use of* [such techniques] *in it. But we made that decision because we and the police were looking to develop a case around him.*[349]

***

***.

***.

***:

***.[350]

315. Applications to authorise such intrusive coverage are treated as 'Urgent', 'Priority', or 'Routine'. They are first sent to the internal team in MI5 which provides advice on such applications (hereafter known as 'the legal team'),[351] before being sent to the Home Office for approval. In this case, the application was classed as 'Routine', and was processed by MI5 as follows:

[349] *Oral Evidence – MI5, 10 October 2013.*
[350] *Oral Evidence – MI5, 10 October 2013.*
[351] ***.

Date	Action taken
26 April	Initial application drafted, and approved by investigative manager.
30 April	Draft approved by senior investigative manager, and sent to MI5's internal legal team.
3 May	Draft returned to investigative team for further work.
7 May	Revised application sent by investigator to managers.
8 May	Revised draft approved by investigative managers.
8–16 May	Discussions between the legal team and investigative team to ensure the draft met the right standard.
16 May	Revised application submitted.
21 May	Approved by manager in the legal team and the Deputy Director General. Final application signed and submitted to the Home Office.
22 May	Adebowale and Adebolajo attacked and killed Fusilier Lee Rigby. The application was subsequently brought to the Home Secretary's attention and was signed the same day.

316. MI5 has explained that the re-drafting during this process was needed firstly because *"the draft needed more clearly to articulate the threat case"*, and then to *"pre-empt questions that the* [legal] *team anticipated would likely be asked by Home Office partners"*.[352]

317. MI5 has confirmed that the average length of time for a 'Routine' application between September 2012 and September 2013 was 6.7 working days, which is within their internal Service Level Agreement of 7 working days.[353] This statistic is for the time taken from the moment the draft is received by the legal team to the point when they submit it to the Secretary of State. In Adebowale's case, this part of the process took 15 working days (from 30 April to 21 May 2013): twice as long as it should have. This meant that the application was only coincidentally submitted to the Home Office the day before the attack.

Pressures in MI5's internal legal team

318. MI5's Director General has explained to the Committee the pressures that existed in the legal team during this period, which increased the time taken in this case. In his capacity as the then Deputy Director General (DDG), Andrew Parker sent a note to MI5's Senior Management Group in February 2013, warning of pressures in the team.

[352] *Written Evidence – MI5, 31 October 2013.*
[353] *Written Evidence – MI5, 31 October 2013.*

319. These pressures were caused by both an increase in the number of applications and a shortage of staff within the team:

- MI5 has confirmed that the increase in the number of applications had been considerable. The Director General gave evidence to the Committee that *"Going back five years, it has gone up* [by]*… 120 per cent"*.[354]
- The staffing pressures were caused by a number of factors. The note from the then DDG explained: *"Like many other sections,* [the team] *is under considerable staffing pressure as a result of increasing… volumes and compliance and oversight challenges, coupled with the steady stream of experienced staff leaving* [the team]*… and a number of unfilled vacancies"*.[355]

In addition, MI5 has said these staffing pressures were exacerbated by:

> *… the wider transition from Olympic staffing arrangements within MI5 and the imperative of continuing to meet our… oversight and compliance obligations.*[356]

320. In response to these pressures, the note from the then DDG explained that the Executive Board had *"… agreed some medium term measures to rebalance the system"*. However, it cautioned that: *"action is also needed in the short term (now) if we are to avoid a breakdown in the overloaded system"*.[357] These short term measures included advising senior managers to help desk officers with drafting applications wherever possible. The note stated that the legal team would no longer have the resources to help to re-draft documents, and that all re-drafting would instead have to be done by investigative desk officers.

321. The Committee asked the Director General why he had taken this particular approach. He explained:

> *… the choice came down to assigning more intelligence staff to that… team… or onto the process. If we keep adding more staff to that team, they have to come off the frontline. And so it is a zero sum game with the intelligence officers. So we decided – you know, we reached the maximum that was sensible. What we now next did was to change the process so that more of the burden was taken in the intelligence sections… rather than cut back the number of* [applications].[358]

322. The Director General explained that one of the options considered (but not taken forward) was *"putting a ceiling on the* [application] *numbers"*. If they had done so, Adebowale's case – as a Priority 3 – would have been *"the sort of case that would not have then progressed"*.[359]

323. The Committee asked whether the Home Office had been aware of these pressures at the time. MI5's Director General has regular meetings with the Home Secretary, which include discussions on resource allocation, and the authorisation of particularly intrusive coverage. In addition, the Office for Security and Counter-Terrorism (OSCT) within the

---

354 *Oral Evidence – MI5, 10 October 2013.*
355 *Primary Material (Adebowale) – MI5, 1 February 2013.*
356 *Written Evidence – MI5, 3 October 2013.*
357 *Primary Material (Adebowale) – MI5, 1 February 2013.*
358 *Oral Evidence – MI5, 10 October 2013.*
359 *Oral Evidence – MI5, 10 October 2013.*

Home Office has an oversight unit which holds daily discussions with MI5 on a range of subjects including corporate issues. However, they were not aware of these specific pressures during spring 2013. The Home Office has said:

> *Though the Home Secretary and OSCT were not aware of the specific resource pressures facing MI5's* [legal] *team before Woolwich, we would not expect to be sighted on the specific staffing position of each team within MI5.*[360]

OFFICE FOR SECURITY AND COUNTER-TERRORISM

The Office for Security and Counter-Terrorism (OSCT) within the Home Office is responsible for, and provides strategic direction to, the UK's work to counter threats from terrorism and organised crime. Regarding terrorism, its primary objective is to protect the public from terrorism by working with others to develop and deliver the UK's counter-terrorism strategy CONTEST.

The OSCT's main responsibilities are to:

- support the Home Secretary and other Ministers in directing and implementing CONTEST and the Government strategy on organised crime;
- deliver aspects of the CONTEST and the organised crime strategy through OSCT programmes and through legislation, guidance and funding;
- set the strategic Government response to terrorism-related crises through the Cabinet Office briefing rooms (COBR);
- support the UK security industry, in particular in relation to overseas export markets; and
- manage the Home Secretary's relationship with the Security Service and National Crime Agency.

OSCT also oversees the administration of the Regulation of Investigatory Powers Act 2000, the Security Services Acts 1989 and 1996, and the Home Office-related elements of the Intelligence Services Act 1994.

It currently has 740 posts, a resource budget of £684m and a capital budget of £102m. The majority of its budget is provided to the police for work on counter-terrorism.

324. The Committee asked the Home Secretary for her view of the resourcing pressures in MI5's internal legal team, in light of the delay in the application relating to Adebowale being submitted. She said:

> *… I think it is appropriate for the Service to look at how they… put the* [applications] *together and what their internal processes are, and I believe that they are actually doing that and will be coming forward with any proposals that they have to change that… this is one of the issues on which questions have been raised with them.*[361]

---

[360] *Written Evidence – Home Office, 11 December 2013.*
[361] *Oral Evidence – Home Secretary, 21 November 2013.*

325. MI5 has summarised to the Committee the actions they have taken since to improve the position within the legal team:

> *We have had* [this] *under review for the past year or so. We have done a number of things with the Home Office, and with the visibility of the Home Secretary, to try and streamline the processes, including how much detail we put into cases, how much detail we put into renewals, how we deal with cancellations, and so on, working with the Commissioners too. We have put extra resource in… to create a new team to help us deal, not only with the level of* [applications] *which has continued to rise, but also with the impact of more activist Commissioners and other aspects on that side.*[362]

Home Secretary's oversight of MI5

326. This issue raised the broader question of the Home Secretary's awareness of the work of MI5.

OVERSIGHT OF MI5

The Home Secretary is responsible for setting the strategic direction for the Government's counter-terrorism strategy, and is the Cabinet Minister responsible for MI5 (and the police).

MI5's Director General retains operational independence for day-to-day decision making: MI5 does not seek formal approval for operations in the same way that SIS requires approval from the Foreign Secretary for its activities. However, the Home Secretary's oversight of MI5 is conducted through:

- regular meetings with MI5's Director General;
- weekly updates on operations;
- discussions on resource allocation; and
- the authorisation of warrants.

327. The Home Secretary has told the Committee that she keeps the level of her contact with MI5 under review:

> *… obviously I have to consider, from time to time, whether my interaction with the Security Service is sufficient to give me that level of oversight.*[363]

She explained that her oversight in authorising Agency activity in particular gave her detailed knowledge of their work:

> *… there will be times when I will raise questions, because of the* [applications] *that I will see.*[364]

---

362 *Oral Evidence – MI5, 12 December 2013.*
363 *Oral Evidence – Home Secretary, 13 December 2012.*
364 *Oral Evidence – Home Secretary, 21 November 2013.*

328. The Committee asked whether the Home Secretary recalled raising any questions in the case of Adebolajo, who was the subject of numerous applications for intrusive coverage (***). Although applications for Adebolajo were approved by the Home Secretary before the attack, she believed she had not been specifically briefed on him as an individual. She had been briefed on the high priority operations in which he was investigated (e.g. Operation CEDAR), but could not remember any particular focus on Adebolajo:

> *I can say that I don't recall being briefed. I obviously would have been discussing* [CEDAR] *as we discuss other operations that are taking place. I can't sit here and say that I remember a particular occasion in which we were discussing that individual, no.*[365]

329. The Home Secretary also confirmed that she had not been briefed on Adebowale before the attack. The Committee accepts that the Home Secretary will not be briefed on every operation or SoI within an operation. Nevertheless, we questioned whether she was content with her lack of visibility of low priority cases. She responded:

> *I think it is right that the briefing that I received concentrates on those people who pose the greatest risk and the greatest threat. And I think that is important… But I think what is important is that I'm not the Director General of the Security Service, I'm the Home Secretary, and therefore it is not for me to be directing in any sense the Director General on every single case and operation that they are undertaking…*[366]

JJ. It is right that the Director General has operational independence: the Home Secretary should not micro-manage MI5. However, where there are significant pressures in critical areas such as MI5's internal legal team which impact on capability – as they did in spring 2013 – such issues should be brought to the Home Secretary's attention.

Impact on Adebowale's case of the delay

330. If the application to authorise further intrusive techniques against Adebowale had met MI5's internal target of submission to the Home Office within seven days, it would have reached the Home Office on or around 9 May (nearly two weeks before the attack).

331. The Home Office has said it is *"rare for* [applications] *to be refused by the Secretary of State"*, and provided statistics showing that, in May 2013, 88% of routine applications were processed by the end of the second day of receipt[367] (the Home Office's target was for 90%). In Adebowale's case, this would have meant that the application would have been processed on or around 11 May.[368]

332. It therefore seems likely that – had the seven day target for submission been met – these further techniques would have been in place during the week before, and on the day of, the attack (***). That said, there is no indication that this would have provided advance warning of the attack: retrospective analysis of all the information now available to the Agencies has not provided any such evidence.

---

365 *Oral Evidence – Home Secretary, 21 November 2013.*

366 *Oral Evidence – Home Secretary, 21 November 2013.*

367 *We were also given the figure for urgent applications: 98% of these were processed by the end of the day of receipt (Written Evidence – Home Office, 11 December 2013).*

368 ***.

333. However, the submission of the application to the Home Office was the last action taken in Adebowale's investigation: the attack took place the next day.

KK. The delays in submitting the application to use further intrusive techniques in Adebowale's case were significant – this should not have happened and must not happen again. If the application had not taken nearly twice as long as it should have, MI5 would probably have had these techniques in place in the days before the attack. While post-event analysis has not provided any evidence that these techniques would have revealed anything that might have helped prevent the attack on 22 May 2013, there can be no certainty of this.

LL. The decision to apply for authorisation to use further intrusive techniques is taken only when there is believed to be a serious risk that the subject may be involved in terrorist activity. It is therefore unacceptable that resource issues should be allowed to result in significant delays. This is a matter for the Home Office as well as MI5 to rectify.

CONTACT BETWEEN ADEBOWALE AND ADEBOLAJO

CONTACT BETWEEN ADEBOWALE AND ADEBOLAJO

334. Whilst Adebowale and Adebolajo were investigated separately by MI5, they did have intelligence that the two were in contact with each other. MI5 first discovered this contact in April 2012, and further contact was observed during the periods when Adebolajo was the subject of intensive investigation.

Level and assessment of known contact

August 2010:	Analysis of communications data revealed Adebowale and Adebolajo to have been in contact with each other in August 2010.
• The first time MI5 was aware of any contact between the two men was in April 2012, when they analysed their databases for historical Subject of Interest (SoI) contact with a telephone number associated with Adebowale under Operation FIR. • Due to the historical nature of this data, MI5 cannot be certain that both Adebolajo and/or Adebowale were the users of the telephones at this specific time. • At the time, MI5 understandably did not attach much significance to this historical contact.	

August 2012 to October 2012:	Contact between the two men was next observed in August 2012 and became more regular in the months that followed. The pair were in contact or attempted contact approximately 30 times during this period. ***.
• ***. • ***.[369] • MI5 has told the Committee that there was no intelligence to suggest extremist activity ***.[370]	

[369] ***.

[370] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

December 2012 to April 2013:	***, Adebowale and Adebolajo were in contact or attempted contact approximately 200 times. ***.

- ***.[371] The Director General added: *"… we have not seen… anything that was indicative that they were up to some extremist plot"*.[372]
- MI5 told the Committee that they had assessed the contact and meetings between Adebowale and Adebolajo during this period to be social in nature ***.[373]
- Nevertheless, the contact between Adebowale and Adebolajo was deemed important enough that MI5 brought it to SO15's attention when briefing them on Operation GUM (MI5's investigation into Adebowale) on 4 April 2013. An Operation GUM Case Review noted: *"Adebowale continues to be in contact with Adebolajo, however, we have seen no significant contact with other… SoIs and no contact with SoIs of particular concern."*[374]

April 2013 to May 2013:	***. Communications data showed that in the weeks leading up to the attack, Adebowale and Adebolajo were in contact a further 39 times.[375]

- ***, the investigative teams still had access to communications data during this time. MI5 told the Committee:

  *We were increasing our coverage of Adebowale over this time period and consequently we had *** coverage of Adebowale's communications data from late March up to the date of the attack.*[376]

Contact between Subjects of Interest

335. We questioned MI5 on the significance they attached to contact between two or more SoIs. MI5 told the Committee that such contact does not, in and of itself, warrant further investigation. When questioned on this, MI5 responded:

> *It is not uncommon for a range of SoIs to be connected. Often SoIs live in the same area and frequent the same locations such as mosques or community centres*.[377]

336. Adebowale and Adebolajo had several (***) mutual telephone contacts who were also SoIs to MI5. (A few mutual SoI telephone contacts have also been identified since the attack.) MI5 noted that all bar one of these SoIs were based in South East London, which they saw as *"an indicator, although not definitive, that there may be an association*

---

371 *Oral Evidence – MI5, 17 October 2013.*
372 *Oral Evidence – MI5, 12 December 2013.*
373 *Written Evidence – MI5, 5 November 2013.*
374 *Primary Material (Adebowale) – MI5, Q4 2013.*
375 *This contact was made on telephone numbers known at the time to belong to Adebowale and Adebolajo. This communications data was seen by investigators at the time.*
376 *Written Evidence – MI5, 17 February 2014.*
377 *Written Evidence – MI5, 5 November 2013.*

through location rather than through particular extremist activity".[378] MI5 has told the Committee that:

> *We assess the threat posed by a particular SoI's contact with other SOIs through the nature of that contact rather than on the very fact of contact itself.*[379]

Post-event analysis

337. As previously noted, communications data available on Adebowale and Adebolajo showed that Adebolajo and Adebowale were in contact a number of times (39) between 11 April and 22 May 2013.

338. Following the attack, two further telephone numbers were found to be associated with Adebolajo. Analysis of these numbers revealed a further 87 times when Adebolajo and Adebowale were in contact during this period. Therefore, we now know from post-event analysis that between 11 April and 22 May 2013 Adebolajo and Adebowale had been in contact, whether by text or phone call, over a hundred (***) times. This consisted of over a hundred (***) texts and a number of (***) phone calls (***).[380]

339. The day before the attack (21 May) there were seven attempted calls between the two men (***) and 16 text messages. In addition, they exchanged one phone call on the morning of the attack. This was between the telephone known to be associated with Adebowale at the time, and a telephone that was later identified as belonging to Adebolajo after the attack. Post-event analysis has been able forensically to recover the content of some of the text messages between the two men in the days leading up to the attack. None of these text messages revealed any indication of attack planning, or indeed anything of significance.

340. Whilst at first sight this level of contact between Adebolajo and Adebowale might seem significant, Adebolajo in particular exchanged a very large number of text messages and phone calls with numerous individuals, and therefore the extent of his contact with Adebowale is not particularly noteworthy when put into context. For instance, the day before the attack Adebolajo also exchanged 30 phone calls and 48 text messages with 17 other associates. When giving evidence to the Committee, MI5 commented:

> *I think the scale of Adebolajo's, in particular, telephone usage is remarkable and we have looked again across our SOI community and he is right at the top end of users of communication devices for a number of events*.[381]

341. ***:

> ***.[382]

---

[378] *Written Evidence – MI5, 5 November 2013.*
[379] *Written Evidence – MI5, 5 November 2013.*
[380] ***.
[381] *Oral Evidence – MI5, 12 December 2013.*
[382] *Oral Evidence – MI5, 12 December 2013.* ***.

MM. The Committee believes that MI5 should consider attaching more significance to the fact of two Subjects of Interest being in regular contact, even when this contact appears to be merely social. However, the Committee recognises that, in this case, the contact between Adebolajo and Adebowale, so far as it is known, did not reveal extremist intent.

WHAT WAS MISSED

WHAT WAS MISSED: CONTACT WITH A KNOWN EXTREMIST

342. Immediately following the attack in Woolwich on 22 May, MI5 launched a post-incident investigation. Working with the police, GCHQ, SIS and liaison partners, MI5 investigated Adebowale and Adebolajo's activities prior to the attack, including *"whether Adebowale or Adebolajo had received tasking, support or direction from a wider network"*.[383]

343. The post-incident investigation identified a number of intelligence leads which were either not known to MI5 prior to the attack or which were not explored fully at the time. Of these, the Committee considers that four might be considered missed opportunities: these are explored in the following sections.

Adebolajo: unexplored contact with a known extremist

344. In January 2010, GCHQ had issued an intelligence report listing the historic contacts of an individual of interest who later became a high-profile and senior AQAP extremist. ***.

345. At the time the list covered (2008–2009), the AQAP extremist had not been assessed to pose a direct threat to national security. ***.

346. When MI5 received the GCHQ report in January 2010, they checked it for any matches within their corporate records – there were no matches relevant to Adebolajo. (***.) MI5 did not prioritise taking any further action beyond this, because at the time the list covered (2008–2009) the AQAP extremist had not posed a direct threat to national security. (***.[384])

347. In 2011, when investigating Adebolajo under Operation BEECH, MI5 connected Adebolajo to the contacts listed in the GCHQ intelligence report, revealing the historic contact between Adebolajo and the now senior AQAP extremist. (***.) The missed opportunity was that the BEECH investigative team did not then seek the content of this communication.

348. When we questioned MI5 about this they explained:

> *Although we would have recommended that for completeness the content should have been sought, the fact that* [it was not reported] *at the time was a strong indicator that it was not of intelligence interest*.[385]

Given the greater threat which the AQAP extremist was thought to pose by 2011, when the investigative team had made the connection to Adebolajo, it seems surprising that MI5 did not seek the contents of the message – particularly since Adebolajo was being investigated for his contact with SoI BRAVO and SoI CHARLIE, who were also believed to be extremists with connections to AQAP.

---

383 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013. ***.*

384 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

385 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

349. During the post-incident investigation, MI5 obtained the content of the communication – which included, among other things, a possible reference to martyrdom. (***.[386])

350. These references to martyrdom appeared to us to be striking, and not just with the benefit of hindsight. We questioned MI5 as to the significance they would have attached to these comments, had they seen them. MI5 said:

> *The message... is not unusual... While the message does contain a reference to martyrdom (shahada), there is no suggestion of imminence or intent, and it is a fairly standard example of rhetoric.*[387]

MI5 made clear that, if they had seen the content of the communication at the time, it would not have made a difference to the course of their investigation.

NN. It was a mistake on MI5's part not to seek the content of Adebolajo's 2008 communication with an individual of interest who later became a high profile and senior AQAP extremist during their investigation in 2011. However, the Committee accepts MI5's assessment that, if they had seen it, it would not have had an impact on the investigation as the rhetoric was not unusual.

[386] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
[387] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

WHAT WAS MISSED: FAILURE TO ISSUE REPORT ON SOI CHARLIE

351. The Director of GCHQ told the Committee that their post-incident investigation revealed that, in April 2012, GCHQ failed to report an item of intelligence which might have had a bearing on the investigation into Adebowale. ***.[388]

***

***.

352. The item of intelligence revealed contact between an unidentified individual and the AQAP extremist SoI CHARLIE. (SoI CHARLIE was the Tier 1 Subject of Interest who MI5 was at that point investigating under the Priority 1B Operation ***, hereafter known as Operation LARCH,[389] and who had previously been investigated under Operations CEDAR and DOGWOOD; see previous sections.) ***.[390]

353. GCHQ did not know who the individual was, and had not received any reporting on him.[391] They were aware of SoI CHARLIE as a Tier 1 target of Operation DOGWOOD, but noted that ***. Given this, such reporting – had it been issued – would have been graded as "C – Worthwhile (Building block intelligence)", the lowest grading of intelligence reports.

GRADES OF INTELLIGENCE REPORTS

GCHQ uses three different grades for its intelligence reports, to give its customers an indication of how credible and useful the intelligence is:

A:	High	Very valuable insight/very high impact intelligence
B:	Significant	Valuable insight/high impact intelligence
C:	Worthwhile	Building block intelligence

354. The Committee questioned GCHQ about their failure to issue this intelligence report, and was told it had been due to a *"specific, individual action that was not taken"*[392] by the individual analyst concerned. The Committee asked about the specific reasons behind this failure. GCHQ responded:

> *I would say it was high workload, primarily. So what you have got was – this was immediately post* [Operation MAHOGANY]*… So all three Agencies had been… working at very high tempo, long hours… So I think at the bottom of this, we have got something that felt very low profile and you have got an analyst who was unfamiliar*

388 *Letter from GCHQ Director, 7 June 2013.*

389 *Operation LARCH was a Priority 1B operation opened in January 2012 to investigate the threat from AQAP in Yemen and its external operations. (***.) SoI CHARLIE, as an individual based with AQAP, with links to the West, was formally incorporated into this investigation in March 2012.*

390 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

391 ***.

392 *Letter from GCHQ Director, 7 June 2013.*

with a lot of the targets and the detail of it that he was newly tasked on. And in the end, it was an error that that report was not put out...[393]

CONTEXT: OPERATION MAHOGANY

***.

355. By way of context, GCHQ's Director explained the pressure that GCHQ analysts operate under:

> *The normal daily context for CT* [counter-terrorism] *analysts requires them to keep abreast of the activities of multiple targets; to analyse these targets'… activities; to translate and report such content; and to liaise with other Agencies*.[394]

Impact of the missed opportunity

GCHQ's evidence

356. The Committee questioned the Agencies about the impact of this missed report. GCHQ had initially told the Committee that their senior management had spoken to the desk officer concerned after the attack in order to:

> *… offer reassurance that the report would not have affected the outcome for Drummer Rigby*.[395]

357. Whilst we welcome this support provided to the individual, we pressed GCHQ to expand on their view that the report would not have made a difference. GCHQ explained:

> *I genuinely believe that it would not have materially impacted… Maybe the investigation would have maintained a tempo, a slightly higher tempo. This was during the Olympics. And of course, the investigation into Adebowale then picked up again a couple of months later. So certainly as far as the analyst is concerned, I am not going to say that: "You were directly responsible for that"*.[396]

The Director of GCHQ added:

> *… I have to say that that did not feel to me as if it would have triggered, if you like, a significant increase in the priority and certainly would have changed things. I am obviously not trying to be defensive, and clearly it was an area that should have gone out… But in terms of making the connection, it looked to us like an individual* [not in the UK]*, in touch with somebody* ***.[397]

---

393 *Oral Evidence – GCHQ, 24 October 2013.*
394 *Letter from GCHQ Director, 7 June 2013.*
395 *Written Evidence – GCHQ, 3 October 2013. They also provided an offer of counselling from GCHQ's specialist 'Employee Assistance' service.*
396 *Oral Evidence – GCHQ, 24 October 2013.*
397 *Oral Evidence – GCHQ, 24 October 2013.*

MI5's evidence

358. MI5 has confirmed that, if they had seen this report at the time, they would have been able to link the intelligence to Adebowale. MI5 has told the Committee that this report would have increased the priority of their investigation into Adebowale:

> *Adebowale's attempt to contact* [SoI CHARLIE] *is the only post-incident intelligence that could have been available to investigators prior to Woolwich…* [it] *would have raised our concern about Adebowale's activities and we judge it likely that the resulting investigation into Adebowale would have increased in priority and that we would have sought to increase our coverage of activities.*[398]

359. By April 2012, SoI CHARLIE was judged to be a close contact of senior AQAP leaders.[399] MI5's Director General therefore explained that the mere fact of contact with SoI CHARLIE – one of their top Subjects of Interest (SoIs) – would have been seen as significant:[400]

> *… it would have raised the priority* [of the] *investigation… because the contact with* [SoI CHARLIE] *would be an indicator that would be a red flag with us, and so we would have done more quickly, Olympics or not, had we had that.*[401]

360. The Director General suggested that, had MI5 known of Adebowale's attempted contact with SoI CHARLIE in April 2012, they would probably have considered further intrusive action in spring 2012,[402] and would not have closed their investigation into him in June 2012.

361. However, the Director General emphasised that it was difficult to know for sure what action they might have taken:

> *I want to caution every sort of "what if" answer with: I can't reconstruct all the variables to say* [in] *any confident, reliable, definitive way what actually definitely would have happened. We probably would have gone* *** [for further intrusive action]… *But I don't* [know;] *what else was going on? ****… *We were stepping up into the full Olympics shape. I can't confidently be sure.*[403]

362. Accepting this uncertainty, there nevertheless remains a possibility that had GCHQ issued a report in spring 2012, and had the intelligence been linked to Adebowale, then this would have led to different investigative decisions.[404] We also note that, as part of MI5's investigation into SoI CHARLIE under Operation DOGWOOD, they were aware of SoI CHARLIE's links to Adebolajo. MI5 also knew at that time that Adebowale and Adebolajo had previously been in contact with each other in 2010. Had MI5 been aware of the recent contact between SoI CHARLIE and Adebowale, it is possible that this connection might have been explored further. However, we note that MI5 was already aware of the

---

398 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

399 ***.

400 *MI5 was aware that Adebowale had been in contact with SoI CHARLIE twice in 2009. However, in 2009, SoI CHARLIE was not of high interest to MI5. Therefore, the historical contact was not viewed as significant. By 2012, SoI CHARLIE was of very high interest to MI5 and therefore his contacts were of significance.*

401 *Oral Evidence – MI5, 10 October 2013.*

402 ***.

403 *Oral Evidence – MI5, 10 October 2013.*

404 *The investigation would probably have increased in priority, and MI5 would probably have sought authorisation for further intrusive coverage, which might have illuminated his extremist behaviour.*

connection through historical contact between Adebowale and SoI CHARLIE from 2009; therefore, it would not be appropriate to seek to draw any firm conclusions. (We explore contact between SoIs at paragraph 335.)

363. The Committee asked MI5's Director General whether he felt this failure was indicative of a wider problem around GCHQ support to MI5 operations. The Director General said he considered that MI5 received good support from GCHQ.

Actions put in place to prevent such mistakes in future

364. GCHQ has told the Committee that they felt the failure to issue the report was:

> *… an isolated mistake that came about because of a certain set of circumstances…*[405]

In addition to emotional support provided to the individual concerned, GCHQ confirmed that they had ensured that the individual was given specific training:

> *A programme of up-skilling was put in place for the individual both in terms of reporting skills but also to focus on being more organised with work. This is enabling the individual to respond more effectively both to intelligence questions posed and in focussing their analytic efforts, mitigating the risk of being in the same situation again.*[406]

365. GCHQ's Director told the Committee that they had looked at their procedures and agreed a number of measures to try to prevent such mistakes in future. GCHQ confirmed that there had been a tracking system in place at the time. However, this did not cover the issuing of reports. GCHQ explained that this process problem had been addressed shortly after the time the mistake occurred, although not as a result of this particular incident:

> *… we put in place a different task tracking system two months later. So you will understand that it was not because of this; it was something that, with the scale of what was going on, we wanted a better handle on who was doing what, where, when and why, partly to feed into the discussions with the Security Service; and that track*[er] *now sits in place to track each of the individual tasks.*[407]

366. As a result of their review after the Woolwich attack, GCHQ identified further measures to prevent such a mistake reoccurring. These include:

> *A new CTT* [Counter-Terrorism Team] *tool to track specific analytic tasks and their current status; a fortnightly *** VTC* [video telephone conference] *to discuss ongoing operational priorities and areas of mutual interest;* [and] *a tipping process in place to flag potentially interesting intelligence across the* [Agencies].[408]

OO. GCHQ's failure to report an item of intelligence which revealed contact between an unknown individual (later identified as Adebowale) and the AQAP extremist CHARLIE was significant. It would have led to different investigative decisions regarding Adebowale, although it is difficult to judge what impact these might have had.

---

405 *Oral Evidence – GCHQ, 24 October 2013.*
406 *Written Evidence – GCHQ, 3 October 2013.*
407 *Oral Evidence – GCHQ, 24 October 2013.*
408 *Written Evidence – GCHQ, 3 October 2013.*

WHAT WAS MISSED: CONTACT WITH SOI ECHO

367. The Committee has been told that, after the attack, the Agencies sought to establish whether Adebowale and Adebolajo had received tasking, support or direction from a wider network. ***:

> ***.[409]

368. Analysis of Adebowale's activities enabled the discovery of contact between Adebowale and a wide range of extremists, including a Yemen-based individual with suspected links to AQAP, ***, hereafter known as SoI ECHO. This discovery was made through forensic analysis of a telephone number belonging to a mobile telephone which Adebowale had left in the car after the attack.[410]

Who was SoI ECHO?

369. In early 2012, SoI ECHO was known to intelligence organisations[411] as he was originally thought to be a known AQAP extremist. However, by mid-2012, he was thought instead to be a Yemen-based individual who was believed to have only limited connections with AQAP. ***:

> ***.[412]

What did Adebowale contact SoI ECHO about?

370. ***:

> ***.[413]

371. It is now known that there were other instances of contact in 2012 between Adebowale and SoI ECHO,[414] in which Adebowale expressed admiration for, and interest in, AQAP, and discussed potential extremist activity. ***.[415]

***:

> ***.[416]

372. ***:

> ***.[417]

---

409 *Written Evidence – MI5, 30 August 2013.*
410 ***.
411 ***.
412 *Primary Material (Adebowale), GCHQ, 28 May 2013.*
413 *Primary Material (Adebowale), GCHQ, 28 May 2013.*
414 ***.
415 *Primary Material (Adebowale), GCHQ, 28 May 2013.*
416 *Primary Material (Adebowale), GCHQ, 3 July 2013.*
417 *Primary Material (Adebowale), GCHQ, 3 July 2013.*

***:

> ***.[418]

373. ***:

> ***.[419]

Could this contact have been seen before the attack?

374. The Agencies did not know that Adebowale was communicating with SoI ECHO: they only discovered this after the attack. However, MI5 could have discovered that Adebowale was in telephone contact with SoI ECHO before the attack: this is therefore a missed opportunity.

375. Under Operation GUM, in January 2013, the investigative team failed to request retrospective billing data for the landline at the address for where Adebowale was then living (see paragraph 279). Had they done so, this data would have revealed telephone contact (on one occasion, on 18 January 2013) with a number in Yemen thought to be associated with extremism (***).[420]

376. MI5 told the Committee that the telephone contact itself would not necessarily have been of high importance:

> *This would of course have been relevant to the investigation, although it would not necessarily have materially increased the urgency of Operation* [GUM] *at this time*.[421]

377. However, the significance of this is that, had MI5 found this telephone contact (from the billing data), it would probably have led them to seek further communications data, which would have revealed previous contact or attempted contact with this number on five other dates since 26 September 2012.[422] It might also have led them to seek traces with other partners who might have been able to provide further information on the communications with SoI ECHO, including discussions about potential extremist activity. ***:

> ***.[423]

PP. MI5 failed to request retrospective billing data for the landline at Adebowale's home address when they were investigating him in January 2013. Had they done so, they would have discovered the telephone contact between Adebowale and SoI ECHO. This might then have led them to be aware of further discussion between the two about potential extremist activity.

---

418 *Primary Material (Adebowale), GCHQ, 3 July 2013.*
419 *Oral Evidence – GCHQ, 24 October 2013.*
420 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
421 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
422 ***.
423 *Written Evidence – MI5, 31 October 2013. ***.*

WHAT WAS MISSED: CONTACT WITH FOXTROT

378. The most significant communication discovered after the attack was an online exchange in late 2012 between Adebowale and an individual named ***, hereafter referred to as FOXTROT. Although FOXTROT was not known to the Agencies at the time, he is now thought to be a *** extremist with links to AQAP.[424]

How this information was discovered

379. ***.[425] ***.[426]

380. The Committee wished to understand exactly how this intelligence was discovered, and questioned GCHQ on the sequence of events. GCHQ told the Committee that this information was provided to them by a third party ***:

> *** *After the death of Lee Rigby,* [the third party] *got in touch with a member of GCHQ ****… *and said: "We might have information relevant to the attack"… they produced essentially the material that was the* [FOXTROT] *report.*[427]

381. This material – received on 6 June 2013 – related to a substantial online exchange between Adebowale and FOXTROT in December 2012, in which Adebowale expressed his desire to murder a soldier – in the most graphic and emotive manner – because of UK military action in Iraq and Afghanistan. Adebowale had not, at that point (five months before the attack), developed a definite plan as to how he might carry out such an attack. FOXTROT encouraged him and suggested several potential attack methodologies, ranging from a martyrdom operation to use of a knife. Adebowale believed that security arrangements that guarded soldiers' places of work might make it difficult to carry out an attack, and that alternative, less secure locations should be considered. FOXTROT wanted to be kept informed of Adebowale's ideas. However, no evidence of further contact between them has been found.

382. The Committee has seen the full transcript of this original exchange. This is reproduced at Annex C. However, this has been redacted from the published version of this Report, since it cannot be published on national security grounds. We can assure the public that there is no relevant material in the full transcript that is not reflected in the summary given in the above paragraph.

Adebowale's online accounts

383. ***:

> ***.[428]

---

424 ***.

425 ***.

426 ***. *(Written Evidence – MI5, 10 September 2013.)*

427 *Oral Evidence – GCHQ, 28 November 2013.*

428 *Written Evidence – GCHQ, 19 November 2013.*

384. The Committee was told that, in addition to the FOXTROT exchange, the information provided after the attack revealed that the company on whose system the online exchange had taken place had closed some of Adebowale's accounts before the murder:

> *What was rather odd and somewhat intriguing was that* [there was]*… a bit more data which revealed the fact that Adebowale obviously had a number of accounts, and* [the company] *had closed down some of those accounts because they hit triggers which we believe were related to their criteria for closing things down on the basis of terrorist content…*[429]

385. The Committee asked GCHQ about the processes by which companies hosting such platforms might close accounts. GCHQ explained that different Communications Service Providers (CSPs) use different systems. However, it appears that there are:

> *… various automated techniques for identifying accounts which they believe break their terms of service. They use these techniques to identify and disable accounts which they believe may be linked to child exploitation and to illegal acts such as inciting violence...*[430]

Such accounts are then automatically suspended.

386. In terms of any further action, GCHQ believes that *"human interaction with a suspect account is normally only instigated when there is a tip off or complaint from another user or an authority"*.[431] In such cases, the company concerned may review the content to decide whether to pass any information to an appropriate authority. GCHQ understands that for accounts linked to terrorism, information is only very rarely passed to the authorities. By contrast, GCHQ believes that, for child exploitation cases, information is passed to the appropriate authorities *"regularly"*.[432] (We address this later at paragraph 456.)

387. We asked GCHQ what information was provided on Adebowale's accounts. GCHQ explained that they were given a list which showed that Adebowale held eleven accounts. Eight of these eleven accounts had been disabled, seven by the company and one by Adebowale himself. The reasons provided for the seven accounts the company disabled were:

Reason given for closure	**Number of accounts**
Disabled for reasons that do not appear to be terrorism-related	Two accounts
Disabled for reasons that do not appear to be terrorism-related; and then associated with over eight terrorism accounts	One account
Associated with pro-militant *jihad* (lone wolf) group, associated with accounts suspected of links to terrorism	One account

[429] *Oral Evidence – GCHQ, 28 November 2013.*
[430] *Written Evidence – GCHQ, 1 April 2014.*
[431] *Written Evidence – GCHQ, 1 April 2014.*
[432] *Written Evidence – GCHQ, 1 April 2014.*

Reason given for closure	Number of accounts
Associated with terrorist accounts	One account
Terrorism	One account
Part of terrorist groups	One account

Although GCHQ has subsequently asked the company concerned for more detail, the company has not provided a detailed explanation of the reasons for account closure that do not appear to relate to suspected links with terrorism.

388. The company themselves only saw this information after the murder as part of a retrospective review of all eleven of Adebowale's accounts. They had not been aware of the content of these accounts before as they did not routinely monitor content in this way. GCHQ understands that Adebowale's accounts were disabled as a result of an automated process, where activity met the above descriptors, but that the company did not then manually review the content of these accounts, nor pass any information to the authorities.[433] (We discuss how the major CSPs operate such processes in the next chapter.)

389. We note that, in some cases, the company may decide to pass information to the authorities when they close accounts because of links to terrorism. In this case, however, they did not do so. We note that, even if the company does not choose to take any action themselves to interrogate an account with suspected links to terrorism, they could nevertheless notify the authorities that they had detected such an account. This in itself would be useful information for the intelligence and security Agencies. In the case of Adebowale, had MI5 been told that there was further intelligence to suggest that he was in contact with terrorist organisations, this might have led to different investigative decisions, which might in turn have led them to Adebowale's exchange with FOXTROT in December 2012.

QQ. After the attack, information was provided to GCHQ by a third party revealing a substantial online exchange between Adebowale and FOXTROT (an extremist thought to have links with AQAP) in December 2012, in which Adebowale expressed his desire to murder a soldier in the most explicit and emotive manner. The Committee has seen this exchange and was shocked by its graphic nature.

RR. The company on whose systems this exchange took place had not been aware of the exchange prior to the attack. However, they had previously closed some of Adebowale's accounts because their automated system deemed them to be associated with terrorism – yet they neither reviewed those accounts nor passed any information to the authorities.

SS. We take the view that, when possible links to terrorism trigger accounts to be closed, the company concerned – and other Communications Service Providers – should accept their responsibility to review these accounts immediately and, if such reviews provide evidence of specific intention to commit a terrorist act, they should pass this information to the appropriate authority.

[433] *Written Evidence – GCHQ, 19 December 2013.*

390. In the months following the murder, GCHQ has been able to obtain further data on Adebowale's accounts from a partner agency (***):

- GCHQ was provided with the content of six accounts.
- Four of these were accounts that had been disabled due to their association with terrorism.
- Of the remaining two out of the six, one had been closed by Adebowale and the other remained open.
- However, the content of the remaining five accounts has not been received.
- These five include one which was suspected by the company to have been associated with terrorist accounts before the attack (***).

Adebowale's eleven accounts provided by the third party and partner agency				
	Status	**Details**	**Obtained by GCHQ from partner agency**	**Selected content provided by the third party**
1	Closed	Disabled for reasons that do not appear to be terrorism-related (***)	No	No
2	Closed	Disabled for reasons that do not appear to be terrorism-related (***)	No	No
3	Closed	Disabled for reasons that do not appear to be terrorism-related, and then associated with terrorism accounts (***)	Yes	No
4	Closed	Associated with pro-militant *jihad* (lone wolf) group, associated with accounts suspected of links to terrorism (***)	Yes	Yes
5	Closed	Associated with terrorist accounts (***)	No	Yes
6	Closed	Terrorism	Yes	No
7	Closed	Part of terrorist groups	Yes	No
8	Closed	Account on which FOXTROT exchange took place. Shortly after the exchange, Adebowale closed the account himself.	Yes	Yes
9	Open	No further details on this account.	No	No
10	Open	No further details on this account.	No	No
11	Open	No further details on this account.	Yes	No

391. GCHQ has told the Committee that it is *"not unusual"* for such responses (***) to be incomplete, and for them not to be given a reason for this.[434] They have explained that such requests require a great deal of work by the partner agency.

392. In the case of Adebowale, GCHQ has asked their partner agency why content from the remaining five accounts was not provided. GCHQ has been told that there were resource constraints within the branch dealing with such requests, and a need to prioritise effort on more immediate and active terrorist threats (***). As a result, the partner agency considered that – given that they had already provided what they believed to be the most obviously relevant content to GCHQ – any further support to the post-event investigation would be more appropriately provided via a different mechanism. However, this process has yet to be implemented (***), meaning that, over a year since the murder of Fusilier Lee Rigby, GCHQ has not received all the information requested.

***

***

***

***

***

393. Of the material they have seen, GCHQ assesses there was some indication of interest by Adebowale in subjects related to Islamist extremism but *"nothing to point to intent"*,[435] with the exception of the FOXTROT exchange. However, having not seen the content of the other five accounts, GCHQ cannot be certain that there is no evidence of attack planning in the rest of these accounts.

394. In relation to the account on which the FOXTROT exchange took place, we were surprised that it did not meet the company's criteria for closure, particularly when the accounts they did close do not appear to reveal much indication of extremist activity. GCHQ noted:

> *They left the one that said…"Let's kill a soldier". That didn't meet their criteria* [for closure].[436]

The Committee was concerned that a message including references to a desire to murder a soldier did not meet the company's criteria for closing accounts. The Committee therefore sought to understand the company's processes. It appears that the automated system does not review the content of accounts or messages (***). This indicates that they were unaware of the FOXTROT exchange.

395. In examining this issue, we note that the company has not provided a detailed explanation of its criteria or how the system operates. GCHQ has been able to gain a

---

434 *Written Evidence – GCHQ, 1 April 2014.*
435 *Written Evidence – GCHQ, 1 April 2014.*
436 *Oral Evidence – GCHQ, 28 November 2013.*

broad understanding of the company's monitoring processes, but it has been *"unable to clarify exactly how this process works"*.[437]

TT. It has been difficult to gain a clear understanding from GCHQ and the company of exactly what happened in this particular case. The monitoring process used by the company is still not sufficiently clear to the Committee or, it appears, to GCHQ. On the basis of the evidence we have received, the company does not have procedures to prevent terrorists from planning attacks using its networks.

Why didn't MI5 discover the contact with FOXTROT before the attack?

396. At the time Adebowale contacted FOXTROT (in late 2012) he was not under active investigation.[438] The Committee has seen from the primary material that when Operation GUM began a month later, MI5 planned to try to access Adebowale's online activity (***) as part of their investigation. A note from MI5 to SO15, dated 25 April 2013, agreed actions to build further coverage of Adebowale:

> *To this end, we anticipate gaining extra coverage of Adebowale shortly. We are in the process of building coverage of Adebowale's* [online activity] ***.[439]

397. ***:

> ***.[440]

398. The Committee also asked MI5 what this 'coverage' would have comprised. The Director General explained that it referred to intrusive capabilities[441] which might then have resulted in access to intelligence (***). However, this was not in place before the attack.

Could it in theory have been discovered before the attack?

399. Given how significant the FOXTROT exchange was, the Committee has investigated whether the Agencies had the technical capabilities to have accessed it – had they had reason to seek to do so. There are three main processes through which they might, theoretically, have been able to do so:

(i) Serving an interception warrant on the company concerned (via NTAC);

(ii) MI5's capabilities; and

(iii) GCHQ's capabilities.

(i) Serving an interception warrant on the company concerned (via NTAC)

400. MI5 usually gains access to the communications of SoIs by serving a warrant (via NTAC), signed by the Home Secretary under the Regulation of Investigatory Powers Act (RIPA), on the CSP concerned.

---

437 *Written Evidence – GCHQ, 1 April 2014.*

438 *A recommendation had been made to create an investigation into Adebowale after he had made extremist comments in July 2012, but Operation GUM did not begin until January 2013 (see paragraph 252).*

439 *Primary Material (Adebowale) – MI5, 25 April 2013.*

440 *Written Evidence – MI5, 7 February 2014.*

441 ***.

NATIONAL TECHNICAL ASSISTANCE CENTRE

NTAC was established in 2001. It has four main roles:

- **Interception of communications**: facilitating access to electronic communications for the purpose of UK lawful interception. NTAC is also responsible for the provision, maintenance and management of appropriately secure communications networks to protect intercepted communications in transit.
- **Enhancement of intercepted data**: processing of lawfully intercepted electronic communications so as to render the contents intelligible.
- **Decryption of seized media**: recovering protected, hidden or encrypted data from lawfully acquired computers or computer media.
- **Advice to the Government and industry:** providing specialist technical advice in support of the development of government policy or operational solutions relating to interception and data recovery. Working with domestic and international partners to share best practice and develop standards in the areas of interception and data recovery.

In 2006, NTAC was transferred from the Home Office to GCHQ. It serves the UK intelligence and security Agencies and police forces, as well as HM Revenue and Customs and the National Crime Agency. NTAC is located in Thames House and staffed mainly by GCHQ personnel, with secondees from other agencies (it has *** staff in total).

401. However, some overseas CSPs do not comply with UK RIPA warrants,[442] as they do not consider themselves bound by UK legislation. Therefore, MI5 cannot use its usual process in such circumstances. The Committee is very concerned by this situation, which is covered in more detail in the next section.

402. In some circumstances, overseas CSPs may choose to comply with a request from NTAC, even though they do not consider themselves bound by UK legislation. For example, if NTAC requested information from US CSPs because they were aware of an immediate threat to life, the CSP might choose to provide this information. The US Electronic Communications Privacy Act (ECPA) permits US CSPs to disclose user information if they believe in good faith *"that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay"*.[443] However, in the case of the exchange between Adebowale and FOXTROT, whilst this could be considered a threat to life situation, the Agencies were not aware of the exchange before the attack and therefore were not in a position to request it.

403. ***:

***.[444]

---

442 ***.

443 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001.*

444 *Oral Evidence – GCHQ, 24 October 2013.*

404. ***.

(ii) MI5's capabilities

405. MI5's access might therefore have been limited ***. They can obtain this access either via their own capability to intercept a specific UK broadband or through a technical operation. In relation to the first of these approaches, MI5 told the Committee:

> ***.[445]

406. However, MI5's Director General explained that they were still unsighted on the circumstances of how Adebowale communicated with FOXTROT, ***:

> ***.[446]

407. The second way in which MI5 might have been able to access this material was through a technical operation. MI5 said they might have gained information in this way if:

> ***. [However, technical operations] *do not always provide full coverage of all activities* ***.[447]

MI5 explained that the difficulty with this approach was:

> ***.[448]

408. However, in either case, even had MI5 been able to access the communications, they might not have been able to read them. ***. MI5 added that *"availability of such analytical resource would have been dependent on other priorities at the time"*.[449]

409. Access to this exchange via MI5's capabilities would therefore have been theoretically possible, as indicated by the investigative note which referred to *"building coverage of Adebowale's* [online activity]*"*. However, it would have depended on MI5 having the appropriate authorisations for intrusive coverage in place (***), on those intrusive capabilities delivering the required levels of access (***), and on the requisite analytical resources being available. From this evidence, it appears that it would have been theoretically possible to access the exchange, but unlikely given the variables involved.

(iii) GCHQ's capabilities

410. GCHQ is able to collect communications on the internet through a variety of direct collection techniques: as they are transported across *** internal networks; as they are sent from a Subject of Interest's (SoI's) computer or device; or as they traverse the internet. However, GCHQ has told the Committee that their capabilities are limited:

- ***.

---

445 *Written Evidence – MI5, 31 October 2013.*
446 *Oral Evidence – MI5, 10 October 2013.*
447 *Written Evidence – MI5, 31 October 2013.*
448 *Oral Evidence – MI5, 12 December 2013.*
449 *Written Evidence – MI5, 31 October 2013.*

- In some circumstances, GCHQ can also conduct technical operations to access communications sent from an SoI's computer or device ***. This technique is used only when targeting the communications of the highest priority SoIs. Neither Adebowale nor FOXTROT were under active investigation at this time, and therefore this technique would not have been used against them.[450] ***.

- GCHQ also has access to communications as they move over the internet via the major internet cables. This provides the capability to intercept a small proportion of internet traffic: in theory, GCHQ can access around ***% of global internet traffic[451] and approximately ***% of internet traffic entering or leaving the UK. However, the resources required to process the vast quantity of data involved mean that, at any one time, GCHQ can only process approximately *** of what they can access. This means that the odds of collecting the content of the communications of an individual who is not specifically being targeted are *** – even if their communications have met other selection criteria they are ***. If GCHQ had unknowingly 'picked up' the exchange between Adebowale and FOXTROT using this collection capability, the fact that neither Adebowale nor FOXTROT were under active investigation at the time means that the communication would not have been selected for further analysis. ***.[452]

411. Overall, GCHQ explained that the likelihood of them being able to access the FOXTROT exchange via their own capabilities was minimal:

> *… we think that there would be a very low likelihood of us being able to do that… we were unaware of* [FOXTROT]*, so we had no active collection against him… Even if we had been able to intercept it through our foreign-facing accesses, we have got a very limited ability to process* [this company's] *communications. So our judgement is: we might have seen potentially some kind of Communications Data relating to it, but it is highly unlikely that we would have been able to access the content.*[453]

412. GCHQ has told the Committee that the only realistic route for them to have accessed the content of the exchange would have been *** via the US courts. However, experience has shown that the US courts will only grant such warrants in high priority cases, where there is a demonstrable threat to life. The Agencies would therefore have needed to have already had evidence of attack planning by Adebowale in order to approach the US courts. This was not the case.

What difference would it have made?

413. In oral evidence MI5's Director General suggested that, had MI5 been aware of Adebowale's exchange with FOXTROT in December 2012, then this:

> *… hypothetically would have been a good example of a priority 1 operation.*[454]

---

[450] *In relation to Adebowale, even if he had been under active investigation, as he was UK-based it would have been unusual for GCHQ to conduct a technical operation against him. As noted elsewhere in this Report, MI5 has similar capabilities and would have been expected to have primacy.*

[451] *Written Evidence – GCHQ, 28 February 2014.*

[452] ***.

[453] *Oral Evidence – GCHQ, 24 October 2013.*

[454] *Oral Evidence – MI5, 17 October 2013.*

414. However, MI5's Director General has cautioned against predicting any alternative chain of events:

> *It is genuinely difficult to – and I think in the end just not possible to – make reliable predictions about alternative realities… there are limits we get* [to] *pretty quickly about how far we can get by speculative construction of alternative realities. And that is because of the whole CT ecosystem that we have talked to you about, the* [hundreds of] *investigations at any time, the fluid movement of resource, events. It is genuinely difficult to create, from that many variables, an alternative universe of, you know, if you came to that bit, what would happen?*[455]

UU. We have explored whether it would have been possible, theoretically, for the Agencies to have accessed Adebowale's exchange with FOXTROT before the attack, had they sought to do so. Given the number of variables concerned, we consider that access would have been possible but unlikely without the co-operation of the company concerned.

VV. Adebowale's expressed intention to murder a soldier was highly significant. If Adebowale's exchange with FOXTROT had been seen by MI5 at the time, then we believe that the investigation would have increased to Priority 1, unlocking all the extra resources this would have entailed. This is the single issue which – had it been known at the time – might have enabled MI5 to prevent the attack.

[455] *Oral Evidence – MI5, 10 October 2013.*

SIGNIFICANT ADDITIONAL ISSUES

DIFFICULTIES ACCESSING COMMUNICATIONS CONTENT

415. One of the additional issues the Committee has considered as a result of our Inquiry is the Agencies' difficulties in accessing communications content. The Agencies have good access to the communications data associated with UK mobile and fixed line telephones. Such data is obtained directly from the relevant Communications Service Providers (CSPs) in the UK. It includes details about a communication (e.g. telephone numbers or email addresses, time, location), but not the content of what is said or written.

CSPs, ISPs AND ASPs

Communications Service Providers (CSPs) provide services that transport information electronically. Examples of CSPs include companies such as BT, Skype and Talk Talk, as well as Facebook and Twitter. They may be based anywhere in the world, and offer communications services and/or internet access.

Those companies providing only internet access are sometimes referred to as Internet Service Providers (ISPs).

Applications Service Providers (ASPs) is a term sometimes used to describe companies which provide applications or services over physical networks provided by others. Examples of ASPs include Google, Facebook, Yahoo, Skype and Apple.

Given that many companies today provide a mixture of communications services, internet access or networks, applications and internet services, we have, for ease, referred to them all as CSPs in this Report.

416. During MI5's investigations into both Adebolajo and Adebowale, communications data was sought routinely. We have seen that, on several occasions, it determined MI5's subsequent investigative decisions.

417. The Metropolitan Police Service has been keen to emphasise the importance of communications data to their counter-terrorism work:

> *The continued erosion of our capability in this area, without the necessary legislative changes, severely impinges upon our ability to conduct terrorist investigations, with potentially grave consequences. More specifically, the ability to obtain and exploit communications data is vital in ensuring we are able to protect the public and keep people safe from harm…*[456]

418. This is consistent with the evidence the Committee received in its earlier Inquiry into *Access to communications data by the intelligence and security Agencies* (published in February 2013).[457] The Committee reiterates its conclusion from the Report: it is essential that the Agencies maintain the broad capability to access communications data.[458]

---

[456] *Written Evidence – Metropolitan Police Service, 11 October 2013.*

[457] *Cm 8514.*

[458] *The Committee is considering further what form that access should take in its Inquiry into the balance between privacy and security.*

419. In addition to communications data, the Agencies can also access the content of communications.[459] As a result of our enquiries into how it might have been possible for the Agencies to have seen the online exchange between Adebowale and FOXTROT before the attack, we have discovered that there is now a worrying capability gap in the Agencies' ability to access the content of communications from CSPs based overseas.

Access to communications content via UK Communications Service Providers

420. Most interception of the content of private communications within the UK is done under a warrant through a process called Lawful Intercept (referred to previously in relation to Adebowale's communications with FOXTROT). This process – which is governed by the Regulation of Investigatory Powers Act 2000 (RIPA) – is targeted against specific individuals who the Agencies or law enforcement believe are involved in serious crime or pose a threat to national security.

INTERCEPTING COMMUNICATIONS IN THE UK THROUGH LAWFUL INTERCEPT

An example of the process by which the Agencies gain access to the content of a Subject of Interest's (SoI's) communications through Lawful Intercept is as follows:

(a) MI5 believes an SoI is communicating with other extremists over the internet (for example, using their home broadband).

(b) MI5 submits an application for a warrant to the Home Secretary for approval to intercept these communications under RIPA. This must specify the named SoI, the justification for the intrusion (which must be both necessary and proportionate) and the 'selectors' (i.e. internet address, phone number etc.) which will be targeted.

(c) Once the RIPA warrant is approved, the Home Office serves it to the telecommunications company which supplies the specified communications.

(d) The telecommunications company must legally comply with the warrant under UK law, and do so by providing the 'raw' intercept to the National Technical Assistance Centre (NTAC).

(e) NTAC is then able to re-format the 'raw' intercept, before sending it to MI5. On receipt, MI5 processes that intercept so that the DIGINT team or an investigative desk officer can view it and analyse it.

(f) The RIPA warrant authorising the interception is only valid for a limited, specified time period, after which it must be renewed (if MI5 can still justify that it is necessary and proportionate) or the telecommunications company will stop providing the interception.

421. Under this system, CSPs based in the UK are legally obliged to provide the intelligence and law enforcement agencies with access to the content of an individual's

[459] *Access to both communications data and the content of communications is governed by RIPA.*

communications which they hold on their systems and networks. The information obtained through Lawful Intercept is usually handled by NTAC, which acts as a processing hub sitting between the CSPs and the Agencies/law enforcement community.

422. Lawful Intercept previously provided the Agencies with near 100% coverage of the communications of Subjects of Interest who were based in the UK. The companies which provided these telecommunications services were based in the UK and therefore had to comply with UK legislation.

Overseas Communications Service Providers

423. Over the last 20 years, methods of communication have changed dramatically. Individuals now use mobile telephones, instead of fixed landlines, for communication. The internet, initially accessed by relatively few over their normal telephone lines, is now accessed by the majority of the population via fast broadband connections and mobile networks. In addition, most people in the UK now use many different methods of communication. There are fixed line voice calls, mobile voice calls, SMS messages, voice/video/email messages over internet services such as Skype, Gmail and Facebook, and conversations using huge numbers of smartphone applications (for example, Whatsapp, BlackBerry Messenger and Instagram). The majority of these communications services and applications are owned by companies based overseas, primarily in the US.

424. The UK Government has always asserted that RIPA has implicit extra-territorial jurisdiction. The problem is that, whereas UK CSPs accept that they are legally obliged to provide access to the communications of individuals (through Lawful Intercept), most CSPs based outside the UK do not accept that the UK legislation applies to them.[460] The Home Office has explained the argument the US CSPs have made:

> *RIPA lacks explicit extraterritorial jurisdiction and cannot be argued to place any obligations onto CSPs based outside of the UK.*[461]

The Committee asked whether the Government had any means of forcing overseas CSPs to co-operate under UK legislation. The Home Office told us:

> *RIPA… contains no lever to compel assistance from overseas CSPs, beyond the power to seek an injunction from a civil court that would require them to do so. Such a power has not yet been tested.*[462]

The Home Office explained the particular issue US CSPs have raised, that: *"complying with RIPA would leave US companies in breach of US legislation (including the Wiretap Act in relation to lawful interception)"*.[463]

---

460 *Refusal to co-operate with UK authorities can also occur for technical legalistic reasons, for example when overseas companies refuse to accept that they constitute a CSP under the definition used in RIPA.*

461 *Written Evidence – Home Office, 8 January 2014.*

462 *Written Evidence – Home Office, 8 January 2014. This problem is not unique to RIPA. The Home Office said that other possibly relevant legislation (such as the Anti-terrorism, Crime and Security Act 2001) does not have extra-territorial effect. We address the Data Retention and Investigatory Powers Act 2014 in paragraph 458.*

463 *Written Evidence – Home Office, 8 January 2014.*

Evidence from overseas Communications Service Providers

425. The Committee was extremely concerned by this situation. We wrote to seven of the major overseas CSPs – Facebook, Google Inc., BlackBerry, Microsoft, Yahoo, Apple and Twitter – to request clarification on their policies for providing information to the UK authorities. Apart from BlackBerry, which is based in Canada, all the companies are based in the US.[464]

426. From the responses we received, it is clear that there are a number of circumstances in which overseas CSPs might consider handing over content to UK authorities. This can be in response to:

(i) Requests under UK interception legislation;

(ii) Requests relating to a known emergency;

(iii) Diplomatic and legal routes such as requests under the Mutual Legal Assistance Treaty (MLAT) process; and

(iv) The companies becoming aware of potentially illegal activity on their networks (either through their own monitoring or from others reporting concerns).

(i) Requests under UK interception legislation

427. As explained in the previous section, overseas CSPs do not always accept that requests under UK legislation such as RIPA apply to them. ***:

***.[465]

428. None of the US companies we contacted accept the UK's jurisdiction on requests for Lawful Intercept (i.e. content) for intelligence investigations. For example, Twitter's 'Guidelines for Law Enforcement' clearly state that *"requests for the content of communications… require a valid US search warrant"*.[466] The companies will therefore only provide private information on users under US – and not UK – legal processes.

429. The fact that the US CSPs do recognise the jurisdiction of the US courts means that the UK Agencies or law enforcement can, in certain limited circumstances, ask their US partners to apply to the US courts for authorisation to obtain and share the relevant material with the UK. However, in practice this is limited by the US courts to high priority investigations where there is a known threat to life. It is therefore of no assistance in investigations where there is no imminent threat to life or intelligence suggesting attack planning. MI5 cannot use this tool in lower priority investigations or in seeking to identify the threat an individual or network may pose to UK national security.

(ii) Requests relating to a known emergency

430. The companies we contacted all confirmed that, if the UK authorities requested information in an emergency situation, they would provide that information. For the

---

464 *Some of the services the companies offer are based elsewhere, and therefore come under different legal jurisdictions. For example, some Microsoft email accounts are based in Ireland and so Irish law and European Union directives apply; Skype – also owned by Microsoft – is based in Luxembourg and so operates under Luxembourg law (www.microsoft.com/lerr).*

465 ***.

466 *Twitter's 'Guidelines for Law Enforcement': https://t.co/le*

companies based in the US, the US Electronic Communications Privacy Act (ECPA) permits them to disclose user information to UK authorities where they have *"a good faith belief that an emergency involving death or serious physical injury to any person requires disclosure without delay"*.[467] This enables the US companies legally to disclose information to UK authorities in such circumstances without fear of prosecution under US law. The companies have established procedures in place to deal with such requests (usually through online disclosure request forms). Google Inc., for example, stated that *"UK law enforcement have utilized this process many times"*.[468]

431. The UK Agencies can therefore obtain information from overseas CSPs where they already have clear evidence of an emergency, such as an imminent terrorist attack. However, in most cases, MI5 is seeking to establish the risk posed, which would not meet this criterion. They cannot therefore use this as an investigative tool as they are unlikely to receive a response from the CSPs.

(iii) Diplomatic and legal routes such as requests under the Mutual Legal Assistance Treaty

432. The CSPs consider that there are a number of legal routes through which the UK authorities can make requests for information from overseas CSPs. The most frequently used in the law enforcement context is the US and the UK Mutual Legal Assistance Treaty (MLAT). This provides a mechanism for sharing information between the US and UK for *"the investigation, prosecution, and combating of crime through cooperation and mutual legal assistance in criminal matters"*.[469] The existence of MLAT provides companies with the legal authority to share information with the UK, which they otherwise might not be able to do. All the US CSPs we contacted are able to provide information to the UK authorities where they receive a valid request from US authorities under the MLAT process. (Companies may also preserve data requested by the UK authorities while such legal processes are being pursued.)

433. The MLAT process can be very useful in criminal prosecutions where there is already evidence of wrongdoing, a suspect may already have been arrested, or evidence is being gathered for a court case. However, the Treaty as it stands is not available for use in intelligence investigations where the aim is to determine the threat posed by individuals and there is as yet insufficient evidence for criminal prosecution. (We discuss the MLAT process, and whether it might be extended or improved, in more detail at paragraph 451.)

(iv) The companies' monitoring arrangements

434. In addition to responses to requests, we asked whether the companies were proactive in monitoring communications on their networks, and alerting the authorities where appropriate. The companies provided the following information:

- **Apple**:
  - Apple did not refer to any automated systems. It confirmed to the Committee that it *"does not actively monitor communications on its systems"*.[470]

---

467 *Letter from Google Inc., 25 March 2014.*
468 *Letter from Google Inc., 25 March 2014.*
469 *Mutual Legal Assistance Treaty between the United States of America and the United Kingdom of Great Britain and Northern Ireland, signed on 6 January 1994.*
470 *Letter from Apple, 4 April 2014.*

– Where Apple is *"made aware of matters that violate the terms for the service at issue"* it will *"notify the applicable law enforcement authorities"*.[471] They therefore rely on either users or authorities reporting any content of concern.

- **BlackBerry**:

  – BlackBerry did not refer to any automated systems, and has confirmed that *"BlackBerry does not monitor communications content on its networks or the services offered to BlackBerry end users"*.[472]

  – An exception is their social media platform 'BBM Channels',[473] which does have a *"monitoring policy in order to ensure posted content meets published guidelines"*. It is not clear whether they review this.

  – BlackBerry has stated that, should they be made aware of an impending terrorist attack, they would respond and *"immediately notify the law enforcement agency with jurisdiction"*.[474]

  – ***.

- **Facebook**:

  – Facebook did not refer to an automated monitoring system in their response to the Committee, ***.

  – ***.

  – Facebook told the Committee that they enable users to report *"offensive or threatening content"* and they prioritise the *"most serious reports"*,[475] which may then be escalated to law enforcement as appropriate. They therefore rely on users proactively notifying Facebook of their concerns for any content to be reviewed.

- **Google Inc.**:

  – Google Inc. has an automated monitoring system: *"as permitted by US law, we use automated techniques to monitor our networks in several ways to keep our networks and our users safe and secure."*[476] These include technology looking for dangerous websites, security measures to detect suspicious logins and measures to detect and prevent spam.[477]

  – However, they do not review all the material selected by this system: *"with so much content on our sites, it would be impossible for Google to manually review even a small percentage of it. For example, users upload over 100 hours of video to our YouTube services every minute."*[478]

  – Instead, Google Inc. allows users to flag inappropriate content. For example, in relation to YouTube, the company said: "*We rely on YouTube community*

---

471 *Letter from Apple, 4 April 2014.*
472 *Letter from BlackBerry, 21 March 2014.*
473 *This service did not exist at the time of the attack on Fusilier Lee Rigby.*
474 *Letter from BlackBerry, 21 March 2014.*
475 *Letter from Facebook, 25 March 2014.*
476 *Letter from Google Inc., 25 March 2014.*
477 *Letter from Google Inc., 25 March 2014.*
478 *Letter from Google Inc., 25 March 2014.*

members to flag content that they find inappropriate. YouTube staff review flagged videos 24 hours a day, seven days a week, and videos that violate our community guidelines are removed from YouTube."[479]

– It appears that it is only where others (e.g. members of the public or law enforcement) report offensive or dangerous content that Google will review it and consider whether to take action or, if appropriate, report it to the authorities.

- **Microsoft**:

  – Microsoft did not refer to any automated systems, and told the Committee that *"we do not monitor our customers' communications in the way* [you] *contemplate…".*[480]

  – They confirmed that they will *"disclose customer data to governments in response to valid legal process"* which include *"ways for UK law enforcement agents to obtain information from Microsoft about specific accounts".*[481] These processes rely on the authorities already having concerns about an account.

- **Twitter**:

  – Twitter did not refer to any automated systems, and has confirmed it *"does not monitor its users' communications".*[482]

  – This is both because the volume of tweets makes monitoring *"unfeasible"* and because any monitoring would *"burden the free exchange of information".*[483]

  – Twitter will respond to illegal content when notified of it: *"where law enforcement brings illegal content to our attention, Twitter acts expeditiously in accordance with its policies to review such content."*[484] They will also review any content reported by users which violates their Terms of Service. These processes rely on others proactively reporting content of concern.

- **Yahoo**:

  – Yahoo did not refer to any automated systems. It stated that: *"Yahoo does not proactively monitor communications on Yahoo Mail or Yahoo Messenger. That would breach our users' privacy".*[485]

  – Yahoo confirmed that, when they are made aware of circumstances in which they are legally required (in their view) to provide information to the authorities, they will comply with that obligation.

  – This includes being made aware of circumstances which constitute an emergency: "*if we became aware of facts or circumstances indicating an*

---

479 *Letter from Google Inc., 25 March 2014.*
480 *Letter from Microsoft, 1 April 2014.*
481 *Letter from Microsoft, 1 April 2014.*
482 *Letter from Twitter, 25 March 2014.*
483 *Letter from Twitter, 25 March 2014.*
484 *Letter from Twitter, 25 March 2014.*
485 *Letter from Yahoo, 4 April 2014.*

imminent risk of serious bodily injury or death to a person, we would report this to appropriate authorities."[486]

– These processes therefore rely on others proactively reporting content of concern.

435. It is clear from the responses we received that the CSPs take different approaches to monitoring their networks. However, for the most part, action is only triggered when they are notified of offensive content (or content which breaches their guidelines) by others.[487] In the case of communications between terrorists, user reporting is unlikely to happen, and therefore such content is unlikely to be discovered. This approach to reviewing content does not therefore help the intelligence and security Agencies to discover terrorist networks or plots.

WW. We note that several of the companies ascribed their failure to review suspicious content to the volume of material on their systems. Whilst there may be practical difficulties involved, the companies should accept they have a responsibility to notify the relevant authorities when an automatic trigger indicating terrorism is activated and allow the authorities, whether US or UK, to take the next step. We further note that several of the companies attributed the lack of monitoring to the need to protect their users' privacy. However, where there is a possibility that a terrorist atrocity is being planned, that argument should not be allowed to prevail.

Attempts to solve the problem: the Agencies' own capabilities

436. Given that the Agencies cannot use their usual Lawful Intercept capability in respect of US CSPs, we have explored whether they are able to obtain the communications of SoIs in other ways. The Agencies can attempt to: access the communications as they travel over UK networks (which are covered by RIPA); conduct a technical operation against the SoI; or obtain the communications using GCHQ's SIGINT (Signals Intelligence) capabilities.

(i) Access via Lawful Intercept of the UK infrastructure

437. This technique can provide access where a Subject of Interest is using services from an overseas CSP, but is accessing them through infrastructure provided by a British company. Access to UK networks would be covered by the Lawful Intercept arrangements set out earlier. However, communications obtained in this way will not necessarily be recovered in an easily readable format.

438. ***.[488] ***.

439. Encryption is increasingly being used by CSPs in order to prevent criminality (for example, to prevent cyber criminals from stealing their customers' data) and to protect their customers' information. ***.

---

[486] *Letter from Yahoo, 4 April 2014.*

[487] *This could be by users or by the authorities (for example, where there is an immediate threat to life).*

[488] ***.

WHAT IS ENCRYPTION?

Encryption, in its simplest sense, involves making a message unreadable by anyone other than the intended recipient. This is achieved by 'scrambling' the message according to a particular set of rules, which includes applying an encryption 'key'. Each unique encryption key 'scrambles' the message in a different way.

Without the encryption key the scrambled message cannot easily be turned back into its original form. Therefore, if the sender of a message and the recipient keep the encryption key secret, anyone intercepting the message in transit will be unable to make sense of it.

There are mathematical techniques that can be used to 'crack' encryption – by discovering either the secret key, or a flaw in the encryption process which was used to scramble the message. However, these become more difficult as the complexity and length of the encryption key increases (e.g. if the key is a number between one and ten it can easily be guessed; if it is a number between one and a billion it becomes less straightforward to guess it). ***.

440. Encryption is also becoming a market differentiator, particularly after the NSA leaks, as individuals have become more concerned about the privacy of their communications.[489] ***. MI5 said:

> *… one of the effects of the Snowden disclosures has been to accelerate the use of default encryption by the internet companies… which was coming anyway, but I think that's why I'm underlining the word "accelerate"…* ***.[490]

441. ***:

> ***.[491]

***:

> ***.[492]

442. The growing use of increasingly sophisticated encryption is challenging. ***.

(ii) Technical operations

443. MI5 can gather intelligence directly using targeted attacks against specific SoIs. For example, they might deploy a technical operation against a target to gather intelligence.[493] ***:

> ***.[494]

---

489 ***.

490 *Oral Evidence – MI5, 12 December 2013.*

491 *Oral Evidence – GCHQ, 28 November 2013.*

492 *Written Evidence – GCHQ, 19 November 2013.*

493 ***.

494 *Oral Evidence – GCHQ, 12 December 2013.*

444. As explained previously, capability provided by such operations is limited.[495] ***. It is therefore not always successful. Further, these operations do not provide comprehensive coverage, and this technique cannot provide large-scale access to communications.

(iii) GCHQ access

445. GCHQ can potentially access external internet communications (i.e. one or both ends outside the UK) via their intelligence capabilities. This includes their ability to access the material travelling through the fibre-optic cables carrying information to and from the UK. However, this capability is not the widespread and complete access that some commentators make it out to be, particularly in terms of accessing specific communications content.

GCHQ'S ACCESS TO COMMUNICATIONS

***.

***.

446. Access to communications using these techniques can be dependent on encryption, their location and the volume of information:

1. **Encryption:** We have already described the problems posed by the growing use of increasingly sophisticated encryption. ***.

2. **Location:** ***.[496]

3. **Volume:** The internet is vast – there are 204 million email messages sent every minute, 100,000 tweets and a million Facebook posts. GCHQ only has the capability to access a tiny fraction of this information, and resource constraints mean that only a very small fraction of that can ever be stored or processed. (***.)

*Attempts to solve the problem: ****

447. ***.

448. ***.[497,498]

449. ***.[499]

450. ***:

***.[500]

---

[495] *For example, a technical operation against Adebolajo was first authorised in August 2011 but an opportunity did not occur until December 2011. The operation did not continue after May 2012, as it had not yielded any further intelligence dividend.*

[496] *Oral Evidence – GCHQ, 24 October 2013.*

[497] ***.

[498] ***.

[499] ***.

[500] *Oral Evidence – Home Secretary, 21 November 2013.*

Attempts to solve the problem: the Mutual Legal Assistance Treaty and legislation

451. As previously explained, the Home Office has told the Committee that the main reason why US CSPs do not provide information to the UK authorities in response to a request under RIPA (***) is because the CSPs maintain that this would leave them in breach of US legislation, such as the Wiretap Act. As a result, we have been told that the companies maintain that they need a valid legal process in place to compel them to provide information to the UK authorities. Given the companies' position, this problem can therefore only satisfactorily be resolved either through legislation, with the US amending its domestic legislation, or by a treaty with the UK which places an obligation on US companies to provide this information.

452. In terms of US law, the Committee has been assured that the difficulty in accessing communications from US service providers has been raised with the US authorities. The US Government is aware that changes to US law might help to resolve the situation. While discussions with the US are important, and may in time provide a solution, any changes to US legislation are unlikely in the short term, particularly in the climate created by the NSA leaks.

453. The Committee has therefore explored whether there is a solution through an international treaty. The Home Office told the Committee that some US CSPs have suggested that the MLAT process should be used to improve the sharing of information between governments, suggesting that it should be broadened and improved to provide better access to both communications data and Lawful Intercept requests: *"these CSPs… maintain that the Mutual Legal Assistance Treaty (MLAT) process offers an accepted mechanism of sharing information between governments."*[501] However, when the Committee asked the Home Office whether this might offer a solution, they said that they *"do not believe… that the MLAT process is capable of meeting all of our requirements",*[502] on the basis that the process is too slow and does not provide for co-operation on intelligence investigations.

454. The Committee subsequently received evidence from a number of CSPs which indicated their strong support for the use and improvement of the MLAT process. Google Inc. said:

> *Google supports use of international diplomatic legal processes, such as the MLAT, whenever non-U.S. parties seek information about users of Google services.*[503]

Similarly, Facebook said:

> *We… promptly respond to requests submitted by the UK authorities through the Mutual Legal Assistance Treaty (MLAT) process, and broadly support efforts to enhance and improve this formal channel for international cooperation.*[504]

---

501 *Written Evidence – Home Office, 8 January 2014.*
502 *Written Evidence – Home Office, 8 January 2014.*
503 *Letter from Google Inc., 25 March 2014.*
504 *Letter from Facebook, 25 March 2014.*

455. The Committee therefore questioned the Home Office as to what the barriers were that would need to be overcome for the MLAT process to work. The Home Office reiterated that:

> *We do not consider that the use of MLAT will ever provide a viable alternative to direct cooperation from Communications Service Providers on interception requests made under RIPA.*[505]

They considered that there were three key problems which could not be easily resolved:

(i) First, whilst the Treaty with the US could be amended to provide for co-operation on interception, *"any treaty change may need to be ratified by the Senate and, depending on its terms, may require primary legislation in order to permit for the change in legal practice"*.[506]

(ii) Second, whilst the Home Office is working with the US Department of Justice to improve the speed with which requests are dealt with, the Home Office does not think it will ever meet the needs of intelligence investigations. For instance, requests currently made to the US for provision of communications data (let alone content) *"take on average 286 days (over nine months) to conclude"*.[507]

(iii) Third, the MLAT process would require the release of sensitive data to the US authorities, since *"the intelligence case underpinning the warrant application* [would have] *to be considered by US authorities"*.[508] In addition, the US legal process would mean that the Secretary of State's decision (i.e. the warrant) would be exposed to scrutiny by a US court. This would be at odds with RIPA which prohibits the disclosure of the existence of an interception warrant.

456. There are clearly problems with extending the MLAT process to intelligence investigations. However, the Committee believes there is merit in exploring this option further. We note that the US CSPs have an agreed process for tackling child sexual abuse images: this should be examined to see whether a similar model could be adopted for terrorism cases. In the case of child abuse, there is a mandatory obligation under US law to report such images to the US National Center for Missing and Exploited Children (NCMEC). NCMEC then *"makes that information available to non-US law enforcement by providing access to country-specific information in NCMEC's database via a virtual private network"*.[509] This demonstrates that it is possible to find a system of sharing information that is acceptable to the CSPs and the US courts. Work should therefore be done to consider how this could be achieved in relation to terrorism.

---

505 *Written Evidence – Home Office, 1 April 2014.*
506 *Written Evidence – Home Office, 1 April 2014.*
507 *Written Evidence – Home Office, 1 April 2014.*
508 *Written Evidence – Home Office, 1 April 2014.*
509 *Letter from Google Inc., 25 March 2014.*

Accessing communications from US Communications Service Providers: summary

457. The number of different forms of communication now available presents the Agencies with significant challenges in terms of their ability to detect and prevent terrorist threats to the UK. However, the real problem arises from the fact that most of these services and applications are hosted overseas. The Government told us during our Inquiry that CSPs based in the US have, for the most part, refused to recognise UK legislation requiring them to provide the content of communications on their networks: they do not consider themselves to be bound by the legal obligations set out in RIPA, as UK CSPs do, and may find themselves subject to legal or civil action if they share information with the UK authorities.

458. The Committee reached its conclusions regarding this issue in April 2014, and at that point shared a draft of its Report with the Agencies and departments. Subsequently, in July 2014, the Government introduced emergency legislation in the form of the Data Retention and Investigatory Powers Act. The Act established a new legal regime to ensure that CSPs retain communications data (following a European Court of Justice ruling that found the European Data Retention Directive to be invalid). However, of more relevance to our Inquiry is the fact that it also sought to clarify the extra-territorial nature of the interception regime set out in RIPA. Whilst this clear statement is a useful first step, it is not yet clear whether it will make any difference: the real test will be whether there is any improvement in the co-operation from overseas CSPs that are served with an interception warrant.

459. In the meantime, the Agencies have sought alternative routes to obtain communications content from these CSPs based in the US, but none offers a workable solution, particularly given the increasing use of sophisticated encryption by the major companies such as Facebook and Google.

460. From the evidence we have heard we consider this to be the single most important challenge that the Agencies face. It has very serious ramifications for the security of the UK: if the Agencies cannot access the content of communications of individuals whom they assess to be of national security concern they will be unable to detect and prevent terrorist attacks. MI5 told the Committee that they are at the limits of their technical expertise and the Director General warned: *"the Government will need to come to a consideration of how to manage this… Or else we will have no intercept in the future."*[510] The Director of GCHQ said, *"our national security targets will be able to select ways of storing and communicating information that are near-impervious to exploitation"*, concluding simply *"it is a bad news story"*.[511]

XX. The capability of the Agencies to access the communications of their targets is essential to their ability to detect and prevent terrorist threats to the UK and our allies. The considerable difficulty that the Agencies face in accessing the content of online communications, both in the UK and overseas, from providers which are based in the US – such as Apple, Facebook, Google, Microsoft, Twitter and Yahoo – is therefore of great concern.

---

[510] *Oral Evidence – MI5, 12 December 2013.*

[511] *Oral Evidence – GCHQ, 28 November 2013.*

YY. Whilst we note that progress has started to be made on this issue, with the Data Retention and Investigatory Powers Act 2014 and the appointment of the Special Envoy on intelligence and law enforcement data sharing, the problem is acute. The Prime Minister, with the National Security Council, should prioritise this issue. The exceptional and long-standing co-operation between the UK and the US on intelligence issues must be utilised to explore an agreed procedure for access to online communications from providers based in the US. UK citizens are unnecessarily exposed to greater risk while the current situation continues.

ALLEGATIONS OF MISTREATMENT

461. In paragraph 68, we reported that, on Adebolajo's return to the UK on 25 November 2010, after his arrest in Kenya, he alleged that he had been mistreated by the Kenyan authorities. We have a number of serious concerns about the way these allegations were dealt with, which we address in this section.

The allegations

462. Prior to his departure from Kenya, Adebolajo was contacted by telephone at Nairobi airport by a consular officer from the British High Commission, who checked on his welfare. We have been told that, after this conversation:

> [A consular officer from the British High Commission] *commented that he* [Adebolajo] *was being treated well and was returning to the UK on his own ticket, but that Adebolajo had said that officials in Mombasa were 'cowboys'.*[512]

463. During the 'Port Stop' interview on his return to the UK, the SO15 officer recorded that Adebolajo made specific allegations of mistreatment:

> *Adebolajo claims that he was beaten, and threatened with electrocution and rape on more than one occasion during his detention.*[513]

464. The record of this interview also notes that Adebolajo claims he was refused access to officials from the British High Commission whilst he was detained. SO15's record of the Port Stop interview, which included these allegations of mistreatment, was sent to MI5, the Foreign and Commonwealth Office and SIS.

Application of the Consolidated Guidance

465. The Government's 'Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas' sets out the Agencies' obligations in relation to the involvement of UK personnel with detainees overseas who are in the custody of an overseas security and intelligence service.[514] In order to establish whether the Consolidated Guidance applies in Adebolajo's case, the question is whether SIS could conceivably be considered:

(i) to have solicited or encouraged Adebolajo's detention;

(ii) to have interviewed Adebolajo; or

(iii) to have been involved in the passage or receipt of intelligence relating to Adebolajo which could have affected his treatment.

---

512 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

513 *Primary Material (Adebolajo), Metropolitan Police Service, 25 November 2010.*

514 *The Consolidated Guidance was published in July 2010. It sets out the principles (consistent with UK domestic law and international legal obligations) which govern the interviewing of detainees overseas, the passing and receipt of intelligence relating to detainees, seeking intelligence from a detainee and soliciting, co-operating or participating in a detention. The guidance must be adhered to by officers of the UK's intelligence and security Agencies, members of the UK's Armed Forces and employees of the Ministry of Defence.*

466. The Agencies told the Committee that there is no reference within the Consolidated Guidance to the *"particular scenario"*[515] of Adebolajo's arrest and detention. SIS has repeatedly stated that *"there is no doubt in our mind that the Consolidated Guidance was not engaged in this case"*.[516] They state that:

> *SIS had no prior knowledge of plans to detain Adebolajo, or that the detention was about to take place, nor had SIS ever previously discussed this individual with the Kenyans… once SIS learned of his arrest and the immediate plans to deport him SIS did not seek to interview Adebolajo, feed in questions or seek intelligence information. They only engaged to check the progress of his deportation to the UK.*[517]

They said:

> *… it cannot apply because we did not know – the consolidated guidance applies when we make something happen. By definition, we did not know it was going on. We could not have made it happen.*[518]

On the latter point we note that SIS had been told that a British citizen was being held in detention: therefore, they did know that *"it was going on"*. That said, the Consolidated Guidance is tightly drawn and arguably it does not apply to the specific situation of Adebolajo's detention.

467. There nevertheless remains a question as to the extent to which SIS could be regarded as having had any involvement in Adebolajo's interview. The Committee originally believed that Adebolajo was interviewed by the Kenyan police, since it was the Kenyan police who held him in detention. However, during the course of our Inquiry it became clear that Adebolajo had been interviewed twice on 22 November 2010: first by the Kenyan police (***) and then, during the evening, by a counter-terrorism unit known as *** (hereafter referred to as ARCTIC). This unit has a close working relationship with HM Government (HMG), specifically ***, who is responsible for *** and ***.

ARCTIC

ARCTIC is a counter-terrorism unit which has a close working relationship with HMG. ***.

***[519,520]

468. When Adebolajo reported his mistreatment, it was not clear whether he was referring to his treatment by the Kenyan police, by ARCTIC, or by both. The Committee notes that SIS did not try to establish which unit Adebolajo's allegations of mistreatment referred to, despite the fact that one of the two organisations in question was a unit which ***. This is surprising: if Adebolajo's allegations of mistreatment did refer to his interview by ARCTIC then HMG could be said to have had some involvement – whether or not UK personnel were present in the room.

---

515 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
516 *Written Evidence – SIS, 23 April 2014.*
517 *Written Evidence – SIS, 23 April 2014.*
518 ***.
519 *Written Evidence – SIS, 14 January 2013.*
520 *Oral Evidence – SIS, 24 October 2013.*

469. In previous high profile cases of allegations of mistreatment, SIS in particular has been accused of 'complicity' in mistreatment, even where there was no direct involvement. 'Complicity' has been taken to mean knowledge, awareness, a reasonable expectation of awareness etc. Given that *** has a close relationship with ARCTIC, ***, this certainly could be enough to raise questions of complicity.[521]

470. SIS themselves acknowledge that for HMG to avoid accusations of complicity they must *"… recognise the point at which we bear responsibility *** which is fundamentally the issue in question"*.[522] In this case, no such effort was made to bear any responsibility. However, ***.

ZZ. Where HM Government (HMG) has a close working relationship with counter-terrorist units, they will share responsibility for those units' actions. HMG must therefore seek to ensure that the same legal and moral obligations to which HMG adheres, and guidance which they follow, also apply to such units. Where there is a possibility that an allegation of mistreatment might refer to a unit where HMG has such responsibility, then HMG must investigate as a matter of priority to establish whether the unit is involved.

Responsibility to investigate

471. Leaving aside the extent to which some might consider HMG to be involved ***, there remains the question of SIS's general obligations in response to allegations of mistreatment. We were originally told that SIS East Africa representatives[523] were:

> *… informed by SIS Head Office of the need to investigate Adebolajo's allegations with a particular focus on establishing whether there had been Consular access and the extent of UK involvement.*[524]

472. When the Committee questioned the Chief of SIS about their responsibility to investigate any allegations of mistreatment, he focussed on the issue of consular access and support for the individual, rather than responsibility to investigate the actual allegations:

> *So the policy framework is very clearly there: that where there are credible allegations being made about the mistreatment of detainees, in this case with UK citizenship, that that information should be passed to the consul and that they will then pursue that. But we don't take on the consulate responsibility for bad guys overseas. For good guys and bad guys, the consulate responsibility for that rests with the Foreign Office.*[525]

Leaving aside the consular aspects, we questioned SIS further on their own responsibilities and sought the relevant primary material.

---

[521] *Since the terrorist attacks of 11 September 2001 a number of allegations have been made against the UK security and intelligence Agencies relating to their involvement in the treatment of detainees held by other countries, including allegations of mistreatment by those countries. In addition, allegations have been made about the UK's involvement in the rendition of detainees. The interim Report of the Detainee Inquiry (published in December 2013) noted that the Agencies continued working with liaison partners even where allegations of mistreatment have been raised: documents provided to the Inquiry show that in some instances there was a reluctance to raise treatment issues for fear of damaging liaison relationships, or that when those issues were raised, only limited details were provided. (Interim Report of the Detainee Inquiry, page 24.)*

[522] *Oral Evidence – SIS, 24 October 2013.*

[523] ***.

[524] *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

[525] *Oral Evidence – SIS, 24 October 2013.*

473. In the material subsequently provided by SIS, we saw an email from an SIS officer to SIS East Africa representatives, which had been sent on receipt of the write-up of the Port Stop interview in which Adebolajo claimed he had been mistreated. The email states:

> *We obviously need to investigate these allegations, which underline the need for continuing assurances from Kenyans on the issue of detainee treatment. We would be grateful if you could provide a summary of* [HMG] *and* [ARCTIC] *involvement in the investigation into Adebolajo… We know that he was questioned by* [ARCTIC] *but was this the extent of ***?*

The email goes on to say:

> *… we would be grateful if you would consider this as a matter of urgency. *** we need to maintain clarity on the assurances given to us by the Kenyan authorities and any potential breaches of these.*[526]

474. This email clearly indicates that SIS officers believed that they had a responsibility to investigate the allegations made by Adebolajo, particularly in light of ***. We support this view. However, SIS has no record of any response to this email and it is not consistent with the evidence provided to the Committee by the Chief of SIS, who said:

> [The Committee is] *suggesting that somehow we should have treated this as an SIS responsibility, when it is simply not the case; it is not an SIS responsibility.*[527]

475. Separately we note our concern that this email was not provided as part of the primary material initially offered in support of this Inquiry as it should have been. It was clearly relevant to the issues under consideration.

---

[526] *Primary Material (Adebolajo), SIS, 1 December 2010.*

[527] *Oral Evidence – SIS, 5 December 2013.*

LACK OF RECORD KEEPING: EPHEMERAL MESSAGES

Despite the fact that the primary material clearly indicates that SIS Head Office had asked SIS representatives to follow up on Adebolajo's allegations of mistreatment, there is no record of the actions undertaken in response, or even a reply to this email. The Committee has been told that:

> *Nothing further can be found in SIS records which relates to action taken to assess the credibility or otherwise of Adebolajo's claim or to SIS discussions with the British High Commission (BHC) or the Kenyan authorities on this matter.*[528]

We questioned SIS on why there was no record of this, and whether this had been in line with their policy at the time. SIS said:

> *Contact between SIS and FCO overseas is routinely conducted by telephone or face to face. It is possible that information from any meetings or discussions held between SIS and FCO staff was reported by ephemeral message.*[529]

SIS provided a definition of 'ephemeral messages':

> *SIS use the term ephemeral when referring to electronic documents or e-mail messages (passed within SIS or outside) which contain information which is of a short-term interest and is assessed to not require filing. Ephemeral messages are held on SIS databases for a period of 3 months.*[530]

We were concerned to see that, in this case, an allegation of mistreatment was not formally recorded. This is particularly worrying given that SIS told the Committee:

> *I think more often than not, when we are engaged in operations to disrupt the activities of British citizens, some form of allegation comes out of it.*[531]

We asked SIS for further information on the number of allegations of mistreatment involving SIS. At the time of asking, SIS was aware of 13 cases involving allegations that they had been complicit in an individual's alleged mistreatment by another country.[532] ***. However, we were surprised to be told that:

> *SIS does not hold a historic record of the total number of cases handled by SIS legal and disclosure teams.*[533]

AAA. There is clearly some uncertainty in SIS as to their obligations in relation to allegations of mistreatment. This lack of clarity must be resolved.

---

528 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
529 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*
530 *Written Evidence – MI5,GCHQ and SIS, 30 August 2013.*
531 *Oral Evidence – SIS, 5 December 2013.*
532 *These figures do not include civil claims for damages which are at the pre-action stage, or judicial reviews where complicity in mistreatment allegations have been made but where permission has not yet been given to proceed by the court.*
533 *Written Evidence – SIS, 14 January 2014.*

SIS's assessment of the allegations

476. The Committee asked SIS what actions they took in order to assess the credibility of Adebolajo's allegations. SIS responded that SIS East Africa representatives were told by a senior Kenyan police officer on 23 November 2010 (before Adebolajo had made any specific allegations of mistreatment):

> *… that his* [Adebolajo's] *treatment would be consistent with Kenyan and International law obligations. This assurance was given by the* [Kenyan police] *which* [SIS] *judged to be credible.*[534]

***.

477. SIS said that, once they were aware of Adebolajo's specific allegations of mistreatment, these allegations were subsequently:

> *… considered against the assurances given by the* [senior Kenyan police officer] *on this and other… operations and judged to be fabricated.*[535]

478. However, SIS told the Committee that they did not raise the allegations with the Kenyan authorities or pursue them any further. The Committee was concerned to learn that SIS had therefore judged these allegations to be *"fabricated"* without having asked the Kenyan authorities about them. We asked the Chief of SIS to explain how this conclusion was reached, to which he responded: *"I am not sure we ever quite got so far as a determination that they were fabricated".*[536] When re-called to give evidence and expand on this opinion, he then said: *"I don't have enough information to come to a view on it."*[537]

479. It therefore appears that SIS made their evaluation of Adebolajo's allegations informally, in light of their trust in the senior Kenyan police officer and the general assurance the Kenyan police had given them before the specific allegations had been made. This trust in the Kenyan police must be viewed against the backdrop that SIS has told the Committee that SIS *"does not have direct contact with the* [Kenyan police]*",*[538] as the relationship is managed by the police (through the Counter-Terrorism and Extremism Liaison Officer – CTELO), and not SIS. It is difficult to see how SIS could adequately have evaluated assurances given by an organisation that they did not know well.

BBB. SIS did not adequately assess Adebolajo's allegations of mistreatment. They viewed them in the context of assurances given before the allegations were made and by an organisation whose credibility they were not in a position to evaluate.

Factors SIS should have taken into account

480. Any allegation of mistreatment should be formally assessed, taking into account previous experience HMG had had of dealing with the authorities in question, any evidence of previous mistreatment and the country's broader human rights record. In Adebolajo's case, we believe there were relevant factors that should have been considered by SIS.

---

534 *Written Evidence – SIS, 3 October 2013.*
535 *Written Evidence – SIS, 3 October 2013.*
536 *Oral Evidence – SIS, 24 October 2013.*
537 *Oral Evidence – SIS, 5 December 2013.*
538 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

481. ***:

> ***.[539]

482. ***.[540] When we raised this issue with SIS, they responded that this was very specific to the circumstances and was not relevant to the circumstances of Adebolajo's detention:

> ***.[541]

483. However, whilst this related to *** and was not related to detentions, it was nevertheless relevant background at that time.

CCC. When considering Adebolajo's allegations of mistreatment there was relevant background that SIS failed to take into account. The Committee does not agree with SIS's assessment that this evidence was irrelevant.

484. In terms of Kenya's broader human rights record, the Committee was told that this had begun to decline towards the end of 2010 and that this had had consequences for security co-operation (this is supported by the issues described in paragraphs 481–482): ***.[542]

485. Such concerns should have been formally recorded in a Country Assessment on Kenya. These Assessments – first commissioned in 2009 – were started with the aim of getting a better and broader understanding of the human rights standards applied. They would also form an important component against which officers of the UK's intelligence and security Agencies, members of the UK's Armed Forces and employees of the Ministry of Defence could assess the risks of working with foreign partners. They formed a key part of the previous Government's proposed policy under which the Agencies would assess the risks of dealing with detainees held overseas.

486. However, during this Inquiry the Committee eventually established, after persistent questioning, that at the time of Adebolajo's allegations there was no Country Assessment of Kenya in place. Although Kenya was one of a number of countries where assessments had been commissioned, this work did not produce a finalised assessment and in fact the whole programme of Country Assessments had been abandoned.[543]

487. SIS told the Committee:

> *… it was an FCO-led exercise…* [but] *foundered upon the issues of practicality, because we discovered reasonably quickly that the particular circumstances of a detention and the particular political conditions prevailing at the time were decisive in making the decisions relevant to a particular detention. So… using a system of more generic assessments proved, in practice, not to be worth the very considerable input.*[544]

---

539 *Written Evidence – SIS, 19 November 2013.*

540 ***.

541 *Oral Evidence – SIS, 5 December 2013.*

542 ***.

543 *The project was announced in August 2009 and the first phase was limited to the *** priority countries, including ***. The FCO selected *** for the pilot project. Following completion of the pilot, the project was brought to an end. However, the Government cannot confirm when the project was cancelled.*

544 *Oral Evidence – SIS, 5 December 2013.*

DDD. The Committee was concerned to discover that the entire programme of Country Assessments – against which the Agencies were due to assess the risks of working with overseas liaison partners – has been abandoned. The Committee recommends that the Government reconsiders this decision: it is essential that SIS have an evidence base against which to consider their work with liaison partners.

Overall response by SIS

488. The Committee has been concerned about the way SIS dealt with Adebolajo's allegations of mistreatment. SIS does not seem to have taken them seriously, even in the wake of previous allegations. The Chief of SIS described the way they approach and assess such matters:

> *There was a climate amongst extremist groups that if you are arrested, you make these allegations. And we have to aim off for that. Just because someone had made an allegation, it doesn't mean that that puts… cooperation with* [those] *against whom the allegation is made into baulk.*[545]

EEE. The Committee is concerned by SIS's approach on this occasion to allegations of mistreatment, which appears dismissive. Pre-judging allegations in this way is completely inappropriate.

Allegations of mistreatment: other organisations

489. The Committee recognises that several organisations were involved in responding to Adebolajo's allegations of mistreatment. Whilst our criticism has focussed on SIS, we do not regard any organisation as having performed well in this case. The responses of the relevant departments and Agencies are summarised below.

Other government departments and the Metropolitan Police Service

490. Adebolajo's allegations of mistreatment were made to SO15 during his interview at Heathrow. The police have advised that *"the ports officers complied with the policy in place at the time and completed the relevant paperwork designed to record the allegation"*.[546] However, this policy was an interim process which only recorded and retained the allegations; there was no immediate action to assess them. At the time, the Home Office, the FCO and the Crown Prosecution Service (CPS) – with police assistance – had been developing a new policy on handling allegations of cruel, inhumane or degrading treatment (CIDT).

491. It took over a year to reach agreement, given the legal complexities involved. It was only at this point, in December 2011, that Adebolajo's allegations were placed on the MPS crime reporting system and flagged to the war crimes team for assessment. This team then reviewed Adebolajo's allegations and decided that they did not meet the threshold for formal investigation.

492. The Committee questioned whether the police passed a copy of the Ports Examination to the FCO for them to take forward Adebolajo's allegations in the meantime. However, the police responded that *"the interim policy in place at the time of receipt of the allegation*

---

[545] *Oral Evidence – SIS, 24 October 2013.*

[546] *Written Evidence – Metropolitan Police Service, 30 August 2013.*

included a provision to inform the FCO. A record of whether the FCO were informed in this particular case is not available".[547]

MI5

493. MI5 seems to have been aware of the potential severity of Adebolajo's allegations. They sought internal legal advice, and received the following response:

> *While these allegations of mistreatment may not be true, the threshold for informing Ministers is low.*[548]

494. Whilst the threshold was low, MI5 nevertheless decided Adebolajo's case did not meet it, and they therefore did not raise the allegations with Ministers. Instead:

> *… the decision was taken (but not formally recorded) that this information should be passed to FCO via SIS.*[549]

495. MI5 therefore also assumed that the FCO would take forward the allegations as a consular matter. They did not check whether this had been carried out, ***.[550] They also failed to keep proper records of their actions.[551]

FCO

496. The FCO has the lead in supporting British nationals overseas through the provision of consular services. After his arrest, Adebolajo's sister contacted the FCO on 24 November 2010 (whilst Adebolajo was still in detention) to inform them of Adebolajo's case and to raise concerns about legal representation and medical assistance. The FCO was subsequently in contact with Adebolajo's sister several times, including about Adebolajo's allegations of mistreatment.

497. On 21 December 2010, following a telephone conversation with his sister on 17 December, the FCO Consular Directorate sent a letter to Adebolajo, offering their assistance in pursuing the matter with the Kenyan authorities. We are concerned that it might only have been in response to contact from Adebolajo's sister that the FCO took any action, nearly a month after the allegations were first made.

498. Furthermore, having received no response from Adebolajo to this letter, the FCO did not take any follow-up action. We queried why this was and were told, *"the FCO only raise allegations with the permission of the individual concerned".*[552] However, it is not clear whether Adebolajo ever received this letter: the attempt seems insufficient, particularly when set against the firm commitments made by the Foreign Secretary regarding the mistreatment of detainees by partners overseas.

---

547 *Written Evidence – Metropolitan Police Service, 10 December 2013.*

548 *Primary Material (Adebolajo) – MI5, 1 December 2010.*

549 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

550 *** .

551 *The Agencies have said that they are "discussing the implementation of a new process to ensure greater clarity… the process provides guidance on which Agency should take the lead in deciding whether action is necessary, as well as how that decision should be recorded and shared" (Written Evidence – MI5, GCHQ and SIS, 30 August 2013).*

552 *Written Evidence – MI5, GCHQ and SIS, 30 August 2013.*

Ministerial involvement

499. None of the organisations that were aware of Adebolajo's allegations of mistreatment proactively assessed or investigated them. Further, we note that at no stage were Ministers or senior officials informed of his allegations of mistreatment. The fact that Adebolajo was a UK citizen means that we would have expected Ministers or senior officials to be informed. However, what makes it inexcusable that Ministers or senior officials were not informed was the possible involvement of a unit for which HMG bears some responsibility, given the specific nature of the relationship ***.

FFF. Given the recent focus on the treatment of detainees, and the allegations against the UK Agencies of complicity in mistreatment, we would have expected that all allegations of mistreatment would now be treated with the seriousness they merit. We have therefore been deeply concerned at the informal manner in which Adebolajo's allegations were handled: whatever we now know about him as an individual does not detract from the fact that his allegations were not dealt with appropriately.

GGG. Adebolajo's allegations of mistreatment potentially related to a *. It is essential that Ministers are informed immediately of any allegations made against an overseas organisation for which any part of HMG bears responsibility and which is ***.**

RECOMMENDATIONS AND CONCLUSIONS

LIST OF RECOMMENDATIONS AND CONCLUSIONS

A. Adebolajo first came to MI5's attention through his association with other Subjects of Interest and his attendance at an event assessed to have an extremist agenda. We accept MI5's assessment that attendance at such events is relatively common. We would therefore not have expected MI5 to place an individual under intrusive surveillance purely on the basis of attendance at such an event.

B. Nevertheless, MI5 must take some action to assess individuals who attend such events in order to ascertain whether they pose a threat to national security, in which case more intrusive investigation would be justified. In the case of Adebolajo there were three recommended actions which were not carried out. The Committee, following the Director General's assessment, accepts that this may not have made any substantial difference in Adebolajo's case. However, the Committee considers that, where actions were recommended, they should have been carried out. If the investigative team had good reason not to carry out a recommended action, then this should have been formally recorded, together with the basis for that decision. We expect MI5 to rectify their procedures in this respect.

C. Extremist groups operate within a complex ideological landscape and therefore identifying the threat posed by such groups, and by their individual members, can be difficult. However, the Committee considers that, if there are reasonable grounds to suspect that individuals are members of a proscribed organisation, this should be sufficient to make them a Subject of Interest to MI5 or the police.

D. We are told that it is difficult to prosecute individuals for membership of proscribed organisations. Nevertheless, given the deterrent effect and the value in drawing attention to individuals who hold extremist views, the Committee considers that there is benefit in continuing to proscribe organisations.

E. We welcome the Home Secretary's attempt to find a solution 'below proscription'. This should take into account the differences between the various extremist groups that exist in the UK. However, the Government should first consider, as a matter of urgency, whether the existing legislation could be amended to enable effective prosecutions.

F. Clearly, MI5 must focus primarily on the highest priority individuals. However, that leaves a large group of individuals who may also pose a risk to national security, but who are not under active investigation. Previous attempts by MI5 and the police to manage this group have failed: we have not yet seen any evidence that the new programme, established in late 2013, will be any better. This is an important issue and the Committee will continue to take a close interest in it in order to ensure that the necessary improvements are made.

G. The Committee is concerned that SIS and the police provided conflicting accounts with regards to information that might have been available to them prior to Adebolajo's arrest. The problem is compounded by the fact that neither SIS nor the police kept adequate records. In any case concerning a British national suspected

of involvement in terrorism (whether in the UK or overseas) it is essential that all information – whether corroborated or not – should be properly recorded. That failed to happen on this occasion.

H. SIS has told the Committee that they often take the operational lead when a British national is detained in a country such as Kenya on a terrorism-related matter. They have also told the Committee that they have responsibility for disrupting the link between UK extremists and terrorist organisations overseas, and that in Kenya this is at the centre of their operational preoccupations. The Committee therefore finds SIS's apparent lack of interest in Adebolajo's arrest deeply unsatisfactory: on this occasion, SIS's role in countering 'jihadi tourism' does not appear to have extended to any practical action being taken. SIS must ensure that their procedures are improved so that this does not happen again. This is particularly important given the current challenges faced by the Agencies in countering 'jihadi tourism' in Syria and Iraq.

I. We note our concern at the four-month delay in opening an investigation into Adebolajo following his return from Kenya. Where an individual is believed to have been seeking to join a terrorist organisation overseas, there should be no such delays. This must be addressed as a matter of urgency.

J. The Committee accepts that during 2011 MI5 put significant effort into investigating Adebolajo and employed a broad range of intrusive techniques. In the event, none of these revealed any evidence of attack planning.

K. MI5 rarely have complete coverage of their targets, even those who are under intensive investigation. In some circumstances they may not have sufficient intelligence indicating extremist intent to justify continued investigation. Where they are aware that their coverage is incomplete, we recognise that the decision to stop investigating such an individual will always be difficult.

L. To publish any information in response to allegations that MI5 harassed Adebolajo or tried to recruit him as an agent would damage national security – irrespective of the substance of such allegations. Despite the considerable public interest in this case, it is nevertheless essential that we do not comment on the allegation that MI5 had been trying to recruit Adebolajo as an agent. In relation to allegations of harassment, we can confirm that we have investigated all aspects of MI5's actions thoroughly, and have not seen any evidence of wrongdoing by MI5 in this area.

M. The Committee considers that there is insufficient co-ordination between MI5 and police investigations. Disruption based on criminal activities offers a potential opportunity to reduce the threat posed by extremists. MI5 and the police must improve both the process and the level of communication.

N. Intrusive coverage of Adebolajo from December 2012 to April 2013 showed that he was involved in drug dealing. However, it did not provide any intelligence of national security concern: on this basis, MI5 had to cancel their coverage in April 2013. MI5 cannot continue intrusive coverage against an individual unless it

is necessary and proportionate to do so. On this occasion, based on the intelligence they had, it was not.

O. MI5 does not currently have a strategy for dealing with Subjects of Interest who occur on the periphery of several investigations. This is a key issue which has arisen during the course of our Inquiry which must be addressed by MI5. The Committee recommends that where individuals repeatedly come to MI5's attention, through their connections with a wide range of Subjects of Interest, MI5 must take this 'cumulative effect' into account. They should ensure that interactions between Subjects of Interest are highlighted when making investigative decisions.

P. Engagement with extremist media should be taken extremely seriously. For example, *Inspire* magazine provides advice and guidance to individuals on how to commit terrorist attacks in the UK. In most cases, engaging with extremist media such as *Inspire* should be sufficient grounds to justify intrusive action.

Q. In low priority cases, it takes MI5's DIGINT team an average of 69 days to complete identification tasks, such as identifying an individual who has sought to engage with extremist material online. Whilst we accept that these are low priority cases, two months is nevertheless too long. This process must be improved as a matter of urgency.

R. We recognise the pressures that investigative teams are under. Nevertheless, MI5 must maintain comprehensive records and ensure that there is a complete audit trail.

S. The eight months it took for MI5 to start investigating Adebowale (three months to identify him followed by five months of inaction) is unacceptable. In retrospect, we can see that the time taken did not affect the outcome in this case. However, this does not excuse the delay. There is a problem with the time taken to investigate low priority cases and MI5 must seek to address this by introducing deadlines.

T. We accept that a historical allegation – that Adebowale was part of Al Qaeda – lacked credibility. We therefore do not believe the failure by the police to share this information with MI5 made any difference to MI5's actions in investigating Adebowale. Nevertheless, when MI5 requests information from the police, the police should ensure that all information held – whatever their assessment of it at the time – is shared with MI5.

U. The Committee considers that, in the circumstances, the decision to close the investigation into Adebowale in June 2012 was reasonable. It was based on the intelligence available to MI5 at the time, which suggested that Adebowale was moving away from his extremist associates.

V. The police should always be consulted when considering whether an individual might be referred to a *Prevent* programme: this should include low level cases where the *Prevent* programme could potentially have the greatest impact.

W. Neither Adebolajo nor Adebowale was referred to *Prevent* programmes. A referral to the *Prevent* programme may in many cases be the best outcome for

a vulnerable and impressionable individual. A more holistic approach should therefore be taken when deciding whether to refer Subjects of Interest to *Prevent* or whether to take a different route, to ensure the views of all stakeholders are considered.

X. Whilst the Home Office's Research, Information and Communications Unit has done some work around a counter-narrative, this does not seem to have been prioritised. More work should be done to deter people from accessing extremist material online.

Y. Despite appearing significant, the Committee notes MI5's assessment that the extremist remarks made online by Adebowale in 2012, including reference to lone wolf attacks, are common extremist rhetoric. Nevertheless, such comments – as on this occasion – may turn out to display more serious intent, and must be investigated on a case-by-case basis, taking into account all the intelligence known about the individual.

Z. The concept of 'lone actors' when applied to individuals such as Adebowale and Adebolajo is misleading. Such individuals – who are in contact with other extremists and seek inspiration and encouragement from them but who plan their own attack – are more accurately seen as 'self-starting terrorists' rather than 'lone actors'.

AA. There is an increasing threat from 'self-starting terrorists'. Whilst the plots involved are often less sophisticated than those co-ordinated by Al Qaeda, the fact that these individuals operate more independently offers fewer opportunities to detect them. MI5 must ensure that its prioritisation framework is sufficiently flexible to deal with the threat from individuals as well as networks.

BB. The failure of MI5 to add Adebowale's address to his Corporate Investigative Record caused unnecessary delay in the investigation. On the basis of the evidence we have seen, we agree with MI5's assessment that this did not have a material impact on the case. However, the fact that this failure in process happened not once but twice indicates a broader problem that must be addressed.

CC. Whilst we recognise the numbers and consequent pressures involved, the Committee was nevertheless seriously concerned to discover the length of time Adebowale's Leads waited in MI5's 'Leads Processing Queue' – far greater than either the expected time or the average time. Leads must be given a deadline, after which they should be escalated automatically to reflect the additional risk caused by being in the Queue for so long. Further, the length of time a Lead is judged to have been in the Queue should be based on the date of its original entry, rather than re-set if it is returned to the Queue.

DD. We recognise the pressures on MI5 – in particular when they encounter significant and immediate threats to life. We are concerned that when there is a major investigation into attack planning (such that an Intelligence Operations Centre is opened) this may render them unable to continue lower priority casework. We find this unacceptable. We recommend that consideration be given to a funding model that allows for periods of high intensity work without that being at the expense of the rest of the organisation's work.

EE. We recognise that low priority cases will inevitably receive fewer resources and that this will impact on the length of time such cases take. However, in Adebowale's case, the delays were significantly longer than the average, without any obvious explanation. This highlights the need to reform the process through which low priority Subjects of Interest are managed.

FF. The Committee recognises that the security challenges of the Olympic and Paralympic Games placed MI5 under very significant pressure, and we commend their staff for their hard work in delivering a safe and secure Games.

GG. The failure to identify the further intelligence that was available regarding Adebowale's online activity was a missed opportunity. It would have revealed additional contact between Adebowale and another Subject of Interest, contributing to the intelligence case on Adebowale.

HH. MI5's Behavioural Science Unit would appear to provide a valuable input: MI5 should ensure that the unit's advice is integrated more thoroughly into investigations.

II. The recent transfer of responsibility from the Home Secretary to the Foreign Secretary for authorising any warrant under the Regulation of Investigatory Powers Act which should become necessary to identify access to extremist media online appears to reduce the Home Secretary's involvement in this area. The judgement as to whether intrusive action is necessary in counter-terrorism cases is largely a domestic issue, for which the Home Secretary should be accountable. Responsibility for any such decisions should therefore lie with the Home Secretary.

JJ. It is right that the Director General has operational independence: the Home Secretary should not micro-manage MI5. However, where there are significant pressures in critical areas such as MI5's internal legal team which impact on capability – as they did in spring 2013 – such issues should be brought to the Home Secretary's attention.

KK. The delays in submitting the application to use further intrusive techniques in Adebowale's case were significant – this should not have happened and must not happen again. If the application had not taken nearly twice as long as it should have, MI5 would probably have had these techniques in place in the days before the attack. While post-event analysis has not provided any evidence that these techniques would have revealed anything that might have helped prevent the attack on 22 May 2013, there can be no certainty of this.

LL. The decision to apply for authorisation to use further intrusive techniques is taken only when there is believed to be a serious risk that the subject may be involved in terrorist activity. It is therefore unacceptable that resource issues should be allowed to result in significant delays. This is a matter for the Home Office as well as MI5 to rectify.

MM. The Committee believes that MI5 should consider attaching more significance to the fact of two Subjects of Interest being in regular contact, even when this contact appears to be merely social. However, the Committee recognises that, in this case,

the contact between Adebolajo and Adebowale, so far as it is known, did not reveal extremist intent.

NN. It was a mistake on MI5's part not to seek the content of Adebolajo's 2008 communication with an individual of interest who later became a high profile and senior AQAP extremist during their investigation in 2011. However, the Committee accepts MI5's assessment that, if they had seen it, it would not have had an impact on the investigation as the rhetoric was not unusual.

OO. GCHQ's failure to report an item of intelligence which revealed contact between an unknown individual (later identified as Adebowale) and the AQAP extremist CHARLIE was significant. It would have led to different investigative decisions regarding Adebowale, although it is difficult to judge what impact these might have had.

PP. MI5 failed to request retrospective billing data for the landline at Adebowale's home address when they were investigating him in January 2013. Had they done so, they would have discovered the telephone contact between Adebowale and SoI ECHO. This might then have led them to be aware of further discussion between the two about potential extremist activity.

QQ. After the attack, information was provided to GCHQ by a third party revealing a substantial online exchange between Adebowale and FOXTROT (an extremist thought to have links with AQAP) in December 2012, in which Adebowale expressed his desire to murder a soldier in the most explicit and emotive manner. The Committee has seen this exchange and was shocked by its graphic nature.

RR. The company on whose systems this exchange took place had not been aware of the exchange prior to the attack. However, they had previously closed some of Adebowale's accounts because their automated system deemed them to be associated with terrorism – yet they neither reviewed those accounts nor passed any information to the authorities.

SS. We take the view that, when possible links to terrorism trigger accounts to be closed, the company concerned – and other Communications Service Providers – should accept their responsibility to review these accounts immediately and, if such reviews provide evidence of specific intention to commit a terrorist act, they should pass this information to the appropriate authority.

TT. It has been difficult to gain a clear understanding from GCHQ and the company of exactly what happened in this particular case. The monitoring process used by the company is still not sufficiently clear to the Committee or, it appears, to GCHQ. On the basis of the evidence we have received, the company does not have procedures to prevent terrorists from planning attacks using its networks.

UU. We have explored whether it would have been possible, theoretically, for the Agencies to have accessed Adebowale's exchange with FOXTROT before the attack, had they sought to do so. Given the number of variables concerned, we consider that access would have been possible but unlikely without the co-operation of the company concerned.

VV. Adebowale's expressed intention to murder a soldier was highly significant. If Adebowale's exchange with FOXTROT had been seen by MI5 at the time, then we believe that the investigation would have increased to Priority 1, unlocking all the extra resources this would have entailed. This is the single issue which – had it been known at the time – might have enabled MI5 to prevent the attack.

WW. We note that several of the companies ascribed their failure to review suspicious content to the volume of material on their systems. Whilst there may be practical difficulties involved, the companies should accept they have a responsibility to notify the relevant authorities when an automatic trigger indicating terrorism is activated and allow the authorities, whether US or UK, to take the next step. We further note that several of the companies attributed the lack of monitoring to the need to protect their users' privacy. However, where there is a possibility that a terrorist atrocity is being planned, that argument should not be allowed to prevail.

XX. The capability of the Agencies to access the communications of their targets is essential to their ability to detect and prevent terrorist threats to the UK and our allies. The considerable difficulty that the Agencies face in accessing the content of online communications, both in the UK and overseas, from providers which are based in the US – such as Apple, Facebook, Google, Microsoft, Twitter and Yahoo – is therefore of great concern.

YY. Whilst we note that progress has started to be made on this issue, with the Data Retention and Investigatory Powers Act 2014 and the appointment of the Special Envoy on intelligence and law enforcement data sharing, the problem is acute. The Prime Minister, with the National Security Council, should prioritise this issue. The exceptional and long-standing co-operation between the UK and the US on intelligence issues must be utilised to explore an agreed procedure for access to online communications from providers based in the US. UK citizens are unnecessarily exposed to greater risk while the current situation continues.

ZZ. Where HM Government (HMG) has a close working relationship with counter-terrorist units, they will share responsibility for those units' actions. HMG must therefore seek to ensure that the same legal and moral obligations to which HMG adheres, and guidance which they follow, also apply to such units. Where there is a possibility that an allegation of mistreatment might refer to a unit where HMG has such responsibility, then HMG must investigate as a matter of priority to establish whether the unit is involved.

AAA. There is clearly some uncertainty in SIS as to their obligations in relation to allegations of mistreatment. This lack of clarity must be resolved.

BBB. SIS did not adequately assess Adebolajo's allegations of mistreatment. They viewed them in the context of assurances given before the allegations were made and by an organisation whose credibility they were not in a position to evaluate.

CCC. When considering Adebolajo's allegations of mistreatment there was relevant background that SIS failed to take into account. The Committee does not agree with SIS's assessment that this evidence was irrelevant.

DDD. The Committee was concerned to discover that the entire programme of Country Assessments – against which the Agencies were due to assess the risks of working with overseas liaison partners – has been abandoned. The Committee recommends that the Government reconsiders this decision: it is essential that SIS have an evidence base against which to consider their work with liaison partners.

EEE. The Committee is concerned by SIS's approach on this occasion to allegations of mistreatment, which appears dismissive. Pre-judging allegations in this way is completely inappropriate.

FFF. Given the recent focus on the treatment of detainees, and the allegations against the UK Agencies of complicity in mistreatment, we would have expected that all allegations of mistreatment would now be treated with the seriousness they merit. We have therefore been deeply concerned at the informal manner in which Adebolajo's allegations were handled: whatever we now know about him as an individual does not detract from the fact that his allegations were not dealt with appropriately.

GGG. Adebolajo's allegations of mistreatment potentially related to a *. It is essential that Ministers are informed immediately of any allegations made against an overseas organisation for which any part of HMG bears responsibility and which is ***.**

ANNEXES

ANNEX A: MI5'S PRIORITISATION PROCESSES

MI5 has provided the Committee with an overview of their investigative approach and prioritisation processes. This is reproduced below:

1. The following provides a brief overview of our investigative approach, drawing particular attention to the points at which there is challenge (both internally and from Whitehall) and where there is flexibility to respond to developments. This document is not an exhaustive explanation of our prioritisation processes. We would like to provide you with more detail on this during briefing sessions.

Internal Processes

2. The rise in the Islamist extremist threat over the last 12 years has necessitated a response akin to an industrialisation of MI5's approach to investigation. We now have in place a formal **triage process for incoming threat intelligence**, a **prioritisation system** which is visited regularly for adjustments according to the waxing and waning of risk and a **higher level review process to set strategic priorities**.

- On receipt, intelligence Leads and Traces are **tested for links** to existing investigations and forwarded to the appropriate team where those links exist. Alternatively, where they do not relate to existing investigations, Leads are **tested for credibility** and a new investigation is launched if appropriate. During the week prior to the Woolwich attacks MI5 received *[hundreds of]* (***) International Counter Terrorism (ICT) leads.

A **Lead** is the term to describe all intelligence or information that is not linked to an ongoing investigation that, following initial assessment, suggests **activities** of National Security (NS) interest.
A **Trace** is a request for a check across MI5 indices to determine potential links to Islamist Extremist activity which does not immediately meet the potential for lead development.

- Investigations are given a **priority according to the risk they carry**. The broad categories are described in the table below. This table does not attempt to explain in detail our prioritisation process but is designed to provide an overview of the way we manage our investigations. ***. There are no stringent rules for what resources should be given to a particular investigation and actions are taken based on whether it is judged necessary and proportionate to do so and on the balance of risk in other investigations. The priority level is regularly tested at senior management level, and priority levels are altered as changes are noted in the activities or aspirations of the individuals or networks we are investigating. During the week prior to the Woolwich attacks, MI5 were running *[several hundred]* *** ICT investigations.

Category	Definition (for ICT)	General Resource Allocation
Priority 1 – Attack Planning (P1a and P1b)	Investigations into individuals or networks where there is credible and actionable intelligence of significant (P1a) or smaller scale (P1b) attack planning.	***.
Priority 2 – high and medium risk activity (P2H and P2M)	Investigation into individuals or networks where there is for example: • a serious intent to travel overseas to join Jihad (P2H). • large scale fundraising (P2H). • significant terrorist training (P2H). • supply of false documents (P2M). • smaller scale fundraising (P2M).	***.
P3 – Investigations into uncorroborated intelligence / ICT prisoner on release	Investigations or networks that require further action to determine whether they pose a threat.	***.
P4 – Risk of re-engagement	Those who have previously posed a serious threat to national security who we judge are not currently involved in such activities but there is a risk of re-engagement.	***.

- Within most investigations we also prioritise the subjects of interest we investigate. This is done through the allocation of 'Tiers' to SOIs. The Tier of an SOI within an investigation can change regularly depending on the importance of that individual.

Tiers reflect the position/importance of SOIs within the investigation that they are assigned to. This will help investigators manage their targets and support understanding of the investigation.

- **Tier 1**: Main targets of an investigation – targets will likely be involved in all aspects of the activities under investigation.
- **Tier 2**: Key contacts of the main targets – targets will likely be involved in a significant portion of the activities under investigation.
- **Tier 3**: Contact of Tier 1 and Tier 2 targets – targets will likely be involved in only marginal aspects of the activities under investigation.

- Sitting within our investigative structure we have a **Strategic Intelligence Group**, specifically designed to provide **assessments** which inform resource allocation decisions and **challenge** the assumptions of investigators.
- Every week, the head of investigations reviews intelligence developments in a **formal meeting**, incorporating updates from those leading individual operations, input from police and SIA colleagues and an analytical feed from JTAC. This process results in the production of the ***** highest risk investigations**, the apportionment of resources accordingly and the weekly letter we send to the PUS at the Home Office *[NB: this is now sent to the Home Secretary]*.
- Also every week, the ICT senior management team considers a **weekly dashboard of wider resourcing issues**, such as the total number of investigations, staffing levels, the processing of leads and any backlog thereof. This dashboard of management information allows for the flexible reinforcement of staff and other resources where the need arises.
- The **Director General (DG) is briefed on a weekly basis** as to the main developments and risks. The **Deputy Director General has oversight of the use of intrusive investigation measures** before they are sent to the **Home Secretary** for consideration.
- Every quarter, there is a **thorough review** of all our ICT casework. Some investigations are closed, others are selected for an injection of resource. Out of this quarterly process also comes an **internal report on trends in our casework**, which informs a more **strategic review** of our investigative footprint. At this point the ICT business also feeds into the **MI5's Quarterly Performance Report** (of which more below).
- Every week we brief ACSO on key developments in our investigations. Separately, the Executive Liaison Group (ELG) process exists to allow us to jointly agree with police the management of risk where we identify a risk to the public from our investigations. At working level a police senior investigator is appointed to major MI5 investigations and is an integral part of our management team making decisions on resourcing and priorities.
- Similarly, the **Director of ICT agrees monthly with his counterparts in SIS and GCHQ any strategic shifts** required to improve our collective response to developments in the threat. The head of JTAC also sits on this body.

- These SIA CT heads also agree a **joint annual business plan for ICT**.

External Visibility and Scrutiny

3. The processes outlined above have a number of docking points with Ministers and senior officials to facilitate scrutiny and challenge to the emphasis of our CT effort, whilst preserving our operational independence to take case-specific decisions. Not all of the portals below are specific to ICT, but naturally our single largest area of business features prominently.

- Principal among these at a strategic level are, of course, the Home Secretary's **Weekly Security Meeting** and the **National Security Council** and its subject-specific sub-committees.
- Beneath these structures, our priorities are discussed and scrutinised across government via the **CONTEST** provisions. Key among these elements are the **PURSUE Board**, the **Overseas CONTEST Group** and the bi-annual **CONTEST Performance Report**.
- Our quarterly review process forms part of the **MI5 Quarterly Performance Report**, which we share with Home Office (Office for Security and Counter Terrorism) colleagues. We also write our own quarterly report on trends in our investigations, and share that with colleagues in Whitehall. Additionally, we supply intelligence and statistical data to inform JTAC's quarterly review.
- The DG attends the **Weekly Security Meeting** at the Home Office, which is chaired by the Home Secretary and discusses the highest priority cases. The DG also has regular bilateral meetings with **the National Security Adviser, the PUS at the Home Office, and the Director General of the National Crime Agency**, and sees the **Prime Minister** on an ad hoc basis.
- At a more granular level of detail, there is the **DG's weekly CT letter** *[to the Home Secretary]* highlighting significant developments *** [in our] highest priority investigations for the week ahead.
- MI5 ICT senior managers also engage in frequent dialogue with counterparts in OSCT on matters relating to warrantry and disruptive measures, such as TPIMs and deprivation of nationality.

Leads

The management of all new CT Lead intelligence and threat reporting not linked to ongoing CT investigations received by both MI5 and the Police is conducted through the Intelligence Handling Model (IHM). This is a joint initiative between MI5 and the Police and provides a single point of entry for intelligence and ensures new leads benefit, where appropriate, from a co-ordinated MI5, GCHQ, JTAC and CT Police tracing and expertise. This co-ordination takes place by dedicated teams in MI5.

The IHM provides a robust framework to ensure that finite covert investigative resources are directed against the most credible new leads – and that leads lacking credibility are resolved in the most appropriate way, without significant covert investigative resource.

A **Lead** is the term to describe all intelligence or information that is not linked to an ongoing investigation that, following initial assessment, suggests activities of National Security (NS) concern.
An **Investigation** is a Lead that has met the threshold for significant covert resource to be deployed. Investigations will make use of the full range of covert investigative actions, as necessary.

Risk, Credibility, Actionability and Proportionality (RCAP) are the key principles for the assessment and decision-making in the IHM. The RCAP Framework is used at all stages of assessment commencing with the Single Point of Entry (SPOE) and most importantly, at the initial point of triage and assessment.[553]

Each lead passes through the four stages of lead development: Receive, Assess, Develop, Decide.

I. **Receive.** All information and intelligence entering the Security Service or Police CT Network is received via a clearly identified and recognised Single Point Of Entry (SPOE) where its receipt is recorded. Processes are in place to receive and assess intelligence 24hrs a day, 365 days a year.

II. **Assess.** Assessment of intelligence occurs at each stage of the process, beginning with the SPOE. All information and intelligence received is assessed to determine if it **fulfils the definition of a lead.** This is the 'initial assessment' referred to in the definition of a lead. Although tracing against indices will usually be sufficient in order to come to a judgement that information or intelligence meets the definition of a lead, it may be that further preliminary actions are necessary, such as a call back to the provider of the information.

    Identified leads are assessed using the RCAP Framework. They are allocated a *** [grading] according to the nature of the reporting and *** credibility assessment.[554]

III. **Develop.** Lead development is the process of identifying intelligence gaps and requirements, and the further research and actions necessary, to enable a more informed assessment of the lead. All development activities should be necessary and proportionate to the level of risk to national security. Leads should be developed where possible without the application of significant covert resource (such as surveillance or intercept). Any application of resources must be proportionate to the risk held by the lead and considered within the overall prioritisation framework. MI5 and Police endeavour to agree and deploy resources in accordance with the risk and credibility assessment. Each organisation is accountable for the deployment of its own resources.

IV. **Decide.** Decisions on what action is to be taken on a lead occur at each stage of the lead assessment process, beginning with the SPOE. The *** [grading] will be reviewed continually and amended where appropriate to ensure it accurately reflects the risk and credibility assessment.

553 *A table providing detail on the RCAP framework has been removed.*

554 *Tables providing detail on risk assessment and credibility grading have been removed.*

MI5 and police will jointly agree on the actions taken on each national security lead. The decision is informed by the credibility assessment; however, at this point consideration is also given to whether any further actions are possible and the proportionality of any further investigation.[555]

[555] *A diagram summarising the lead development process has been removed.*

ANNEX B: MI5'S LESSONS LEARNED

MI5 has told the Committee they have identified a number of areas for improvement as a result of their review of their processes after the attack in Woolwich. Their 'lessons learned' are reproduced below:

1. Leads processing system and associated risks:

- Over the last six years, we have built a clear and consistent triage process for incoming international counter-terrorism (ICT) leads, ensuring all leads are assessed, recorded and actioned appropriately. However, we recognise that the delays which occur in the 'queue' system for the processing and allocation of intelligence leads, while an inevitable consequence of the volumes involved, represent a risk for MI5. In the case of Adebowale, intelligence relating to his extremist activity was not processed for six weeks following receipt.
- Minimising delays in the leads processing system is a particular challenge given the large number of leads routinely requiring assessment by a finite number of investigative staff, and the parallel imperative of maintaining sufficient focus on identified threats already under investigation. The challenge is especially acute in respect of leads *** which are high volume in nature but often offer little supporting context on which to confidently assess credibility.

Action:

- While we are confident that the overall process of managing leads is right, we acknowledge that it may require some adjustments. We will therefore assess the level of risk associated with holding intelligence in the leads processing queue and evaluate our current arrangements for managing this process, identifying resource requirements to reduce delays and any realistic options to mitigate this risk (subject to availability of resources and the opportunity cost of relocating resource from other areas of work). In particular, we will explore the handling arrangements for leads *** in order to ensure that our approach is consistent and appropriate.

2. Tackling recurring Subjects of Interest:

- It is common for Islamist extremist networks to overlap and interlink and therefore for SoIs to feature in more than one extremist network and be investigated under multiple investigations over time, as demonstrated in the case of Adebolajo whose investigative history spanned five ICT investigations over a period of five years. Assessing and managing the associated knowledge and cumulative risk posed by individuals who repeatedly feature in disparate investigations is challenging, especially when the investigations they feature in do not fully illuminate the nature and extent of their involvement in extremist activities.

Action:

- We will seek to develop criteria for identifying when recurring SoIs meet the threshold for investigation in their own right. We will incorporate the criteria

in formal discussions at quarterly case reviews at the end of 2013 and in the closure of investigations/SoIs process.

- In parallel we are developing (since November 2012) new techniques for managing emerging and residual threats alongside our police partners. The residual threats strand of this focuses on how we reach a joint assessment on the residual risk of a SoI who we are no longer investigating, how we record that decision, how we agree what actions need to be taken against the individual, and how we monitor the level of risk that closed SOI poses over time. While this work aims to place a greater emphasis on the risk posed by an individual when an investigation is closed down, there is still scope for MI5 to improve the way in which we handle those SOIs who move repeatedly between investigations. The work will take several quarters to bed in and produce higher levels of reassurance.

3. The nature of multiple-lead operations:

- Reporting regarding Adebowale's [interest in extremist media] was initially progressed under a multiple-lead operation (Op FIR) where it featured as one of multiple strands of similar reporting regarding other individuals. Multiple-lead operations focus on an activity, ***, rather than a network of individuals. From an investigative perspective, the nature of multiple-lead operations can make it challenging to track investigative progress and levels of risk, especially as the work conducted under them tends to be of a lower priority compared to the other higher priority live P1 and P2 investigative work focussed on identified threats being progressed by the investigators that work on them.

Action:

- We will explore whether running multiple-lead operations in investigative teams is the best model for capturing and developing all leads relating to a certain type of extremist activity. We will also develop best practice for managing multiple-lead work, with particular reference to formally monitoring progress and tracking/reflecting levels of risk. We are in the early stages of thinking regarding this particular issue. Our first step will be to establish how many multiple-lead operations are currently in existence and the volume of leads being progressed under them, in addition to seeking feedback about the practicalities of managing them from relevant team leaders.

4. Handling of MI5 DIGINT:

- As a result of the increase in the online presence of ICT SoIs coupled with the rapid expansion of MI5's digital intelligence (DIGINT) capability, investigators are now required to interrogate ever increasing volumes of digital intelligence relating to their SoIs. Investigators must balance the requirement to interrogate DIGINT against the requirement to interrogate intelligence from a wide variety of non-DIGINT intelligence sources.

- In the case of Adebowale, DIGINT (***) was reviewed by the investigator, alongside a DIGINT analyst, on an ad-hoc basis and when competing investigative priorities allowed. ***, much of the intelligence viewed was not

deemed to meet the threshold to be formally reported. For some of our DIGINT databases there is currently no easy way of establishing which product has been viewed and assessed unless it has been formally reported.

Action:

- While we are confident that the overall process for handling and managing the interrogation of MI5 DIGINT databases is right, we will explore whether there are any further steps we can take to ensure that thresholds for tasking formal reports are consistent. We will also explore whether there are any improvements we can make to enhance our ability to account for which DIGINT an investigator or analyst has seen and reviewed. We will consult with MI5 DIGINT experts with a view to establishing whether we need to revise best practice guidance and training for investigators and [DIGINT] analysts regarding reporting thresholds, and will in parallel explore whether anything more can be done to automate our exploitation of new DIGINT intelligence (***).

- In addition to the high level lessons learned described above, we have identified several minor process issues where we feel that guidance or best practice could be improved in order to increase our investigative efficiency and make best use of the resources at our disposal. These can be summarised as follows:

  – Review why certain communications data is not being fed into MI5 data systems (***);

  – Review guidance for investigators in relation to SOIs suffering from mental health problems;

  – Revisit general guidance given to investigators about best practice, including making the most appropriate use of resource, searching standards on MI5 databases, and their responsibilities for compliance.

ANNEX C: TRANSCRIPT (POST-INCIDENT)

***.

ANNEX D: ADEBOLAJO – TIMELINE

2008	
May	Adebolajo first identified by MI5 following his plans to attend a social event (***) with a Subject of Interest (SoI) investigated under Op ASH (P1A). Corporate Investigative Record created.
May	Adebolajo linked to Al Ghurabaa events dating back to 2005. MI5 also conducted enquiries with the police.
September	Op ASH concluded following the disruption of the primary SoI.
October	Adebolajo listed as Category 1 on Programme AMAZON given his links to Op ASH SoIs.
2009	
Throughout 2009–2010	Occasional indirect coverage of Adebolajo obtained through his contact with another SoI to MI5.
2010	
July	Adebolajo reclassified as Category 3 on Programme AMAZON to indicate there was no further substantial reporting on his extremist activities.
21 November	Adebolajo arrested in Kenya by the Kenyan authorities with a group of other individuals, assessed to have been attempting to travel to Somalia to join Al Shabaab.
22 November	SIS and MI5 told of Adebolajo's arrest. MI5 opened a Trace.
22 November	Adebolajo interviewed by the Kenyan police and ARCTIC.
24 November	Adebolajo left Kenya voluntarily.
25 November	Adebolajo arrived back in UK. Interviewed by SO15 under Schedule 7 of the Terrorism Act 2000. Adebolajo claimed he had been mistreated during his detention in Kenya.
29 November	***.
2011	
April	Op BEECH (P3) created to focus on Adebolajo's involvement in extremist activity. Initial enquiries made to investigate Adebolajo and confirm where he was living.

14 April	MI5 linked Adebolajo to a GCHQ report from January 2010 which listed the historic contacts (between 2008 and 2009) of an individual of interest who later became a high profile and senior AQAP figure. The content of this communication was not sought.
May	Retrospective analysis of Adebolajo's call data between September and December 2010 linked him to SoIs BRAVO and CHARLIE of Op CEDAR (P1B). ***.
9 May	Urgent application made for further intrusive coverage against Adebolajo (***).
May	*** surveillance deployments conducted from May to September 2011.
June	Op BEECH closed. Investigation of Adebolajo continued under Op CEDAR.
June	MI5 made an urgent application for the use of additional techniques against Adebolajo (***).
27 June	***.
Late June	Intrusive techniques against Adebolajo resulted in some material of interest (***).
July–September	***.
4 July	***.
July	***.
21 July	Surveillance deployments indicated that Adebolajo had met ***, an SoI investigated for radicalising UK-based individuals and facilitating their travel overseas.
July	***.
August	MI5 passed intelligence to the police regarding Adebolajo's possible intention to be involved in the London riots. In the event, however, Adebolajo was not arrested.
August	MI5 contacted the National Terrorist Financial Investigative Unit, suspecting Adebolajo was engaged in fraudulent activity. No evidence of fraud was discovered.
August	MI5 carried out an intelligence gathering operation to increase their coverage of his activities.

September	MI5 commissioned an internal report to summarise what was known about Adebolajo's activities. This noted there was no indication he was currently involved in extremist activities.
September	Op CEDAR split into a number of different operations, including Op DOGWOOD, which was focussed on BRAVO and CHARLIE. Adebolajo was moved into Op DOGWOOD.
December	MI5 initiated a technical operation against Adebolajo (***).
2012	
***	***.
***	***.
***	***.
***	***.
September	***.
October	Investigation into Adebolajo found no evidence of current Islamist extremist activity. MI5 cancelled their coverage and planned to close the investigation into him.
October	New information suggested that Adebolajo might act as a contact for Al Shabaab, linked to SoI DELTA, an SoI being investigated under Op ELM.
November	Adebolajo transferred to Op ELM. Intrusive coverage (***) of Adebolajo reinstated.
November	Adebolajo came to police attention as part of a group involved in a violent confrontation. Adebolajo stopped but not arrested.
December	Intrusive coverage of Adebolajo reinstated (***).
December–May 2013	No indication of intelligence of national security concern was identified. Coverage indicated that Adebolajo was spending most of his time involved in drug dealing.
2013	
February	Adebolajo demoted to a Tier 3 SoI within Op ELM.
15 February	MI5 notified SO15 that they believed Adebolajo was involved in drug dealing.
27 March	A sanitised form of words for dissemination within the police was provided to SO15 by MI5.

10 April	SO15 channelled this information to the local police. However, the house number was accidently omitted. No further action was taken.
11 April	Intrusive coverage of Adebolajo (***) cancelled.
22 May	Fusilier Lee Rigby murdered.

ANNEX E: ADEBOWALE – TIMELINE

2011	
August	Intelligence from GCHQ indicated an unknown individual had shown interest in extremist material online (***). This was taken forward by MI5 for investigation.
5 August	MI5 passed this intelligence to Op FIR. They tasked MI5's Digital Intelligence (DIGINT) team to identify the individual concerned.
September	The DIGINT team identified the individual as Adebowale.
November	The DIGINT team finished all their enquiries.
2012	
April	The Op FIR team confirmed Adebowale as the individual concerned, and opened a Corporate Investigative Record, before conducting routine investigative enquiries.
April	Telephone analysis showed that Adebowale had been in contact with SoIs centred around ***, although he was now located in South Wales.
April	SO15 and the Welsh Extremism and Counter-Terrorism Unit conducted enquiries into Adebowale. No traces of current involvement in extremist activity were found.
June	MI5 closed their investigation into Adebowale. They assessed that he did not pose a current threat to UK national security.
***	***.
***	GCHQ reported comments online, including references to a lone wolf. MI5 created a new Lead to examine this.
5 September	Adebowale identified as the individual concerned. Case initially assigned to Op FIR, who assessed it and referred it back to the Triage Team as it did not fit with the objectives of Op FIR.
13 November	Triage Team concluded that covert resources were needed to investigate Adebowale. They sent a recommendation for a new investigation to managers for endorsement.
2013	
25 January	Decision to create operation into Adebowale was endorsed by management team. Op GUM (P3) was created.

January–February	Adebowale's online activity was reviewed. This showed considerable activity and revealed that he had been in contact with another SoI.
13 March	Intelligence indicated Adebowale had sought to disseminate extremist material (***). This was a possible offence; potential executive action was considered.
***	***.
19 April	MI5 and SO15 agreed to build further coverage of Adebowale in order to form a better assessment of how to disrupt him. Enquiries continued.
26 April	Application drafted for further intrusive techniques against Adebowale (***). Draft approved by MI5 investigative manager.
30 April	Draft approved by a senior investigative manager in MI5. Sent to MI5's legal team.
3 May	MI5's legal team returned application to investigative desk, advising that it needed to be re-drafted in order to meet the relevant statutory and policy requirements.
7 May	Revised application submitted by the investigator and approved by management.
8 May	Revised application approved by senior management.
8–16 May	Discussions continued between the legal team and investigative team to ensure the draft met the right standard. Revised application again submitted by the legal officer.
21 May	Revised application approved by a senior manager and MI5's Deputy Director General. Final draft sent to the Home Office as a routine application.
22 May	Fusilier Lee Rigby murdered.
22 May	Home Secretary signed the *** submission as an urgent application.

ANNEX F: LIST OF WITNESSES

Ministers

HOME OFFICE

The Rt. Hon. Theresa May MP – Secretary of State for the Home Department

Other officials

Officials

SECURITY SERVICE

Mr Andrew Parker – Director General, MI5

Other officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Sir Iain Lobban – Director, GCHQ (until 2 November 2014)

Other officials

SECRET INTELLIGENCE SERVICE

Sir John Sawers – Chief, SIS (until 31 October 2014)

Other officials

METROPOLITAN POLICE SERVICE

Assistant Commissioner Cressida Dick

Other officials