Government Response to the Intelligence and Security Committee of Parliament Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby

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

February 2015

Cm 9012

Government Response to the Intelligence and Security Committee of Parliament Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby

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

February 2015

Cm 9012

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

Any enquiries regarding this publication should be sent to us at
Cabinet Office
70 Whitehall
London
SW1A 2AS

Print ISBN 9781474115131
Web ISBN 9781474115148

ID 05021501 02/15 47718 19585

Printed on paper containing 75% recycled fibre content minimum

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

INTRODUCTION

The murder of Fusilier Lee Rigby was a sickening act of terrorism on our streets. The Prime Minister assured the public that his killers would be brought to justice and that we would learn lessons of what happened that day, and what the intelligence agencies knew about his killers prior to the attack. Michael Adebolajo and Michael Adebowale, the two murderers, have been sentenced to life in prison; and in November 2014 the Intelligence and Security Committee of Parliament published its Report on what the Agencies knew about the attackers. When that report was published the Prime Minister made a commitment to publish a full response to all the points raised.

The Government welcomes the Committee's overall conclusion that this attack could not have been prevented based on what was known by the agencies at the time.

The Committee found one issue that, in their words, "could have been decisive". This was an online exchange in which Michael Adebowale expressed his desire and intent to kill a soldier. The monitoring systems of the company concerned did not detect this exchange, nor did they pass on details of other accounts used by Adebowale which had been closed for terrorist associations. This was a very serious finding. The internet companies were asked to report back on the new steps that they could take – they have a social responsibility to ensure their networks do not put the communications of terrorists beyond the reach of the authorities. The company concerned has agreed to rapidly improve the identification of imminent threats and to reporting them to law enforcement and we are now engaging with a range of Communications Service Providers to press for the same approach to be adopted across all relevant platforms.

The Report highlighted a number of serious delays and potential missed opportunities. The Prime Minister has been clear that the Committee rightly identified significant areas of concern and the Government is clear there have been important and valuable lessons to learn. In response, the Security Service, and the other Agencies have introduced a number of changes to their processes and procedures. These include, additional resources and training to ensure that applications to the Home Secretary for intrusive surveillance will be handled more efficiently; a new process for managing low level subjects of interest; better record keeping processes and training; and measures to improve co-ordination. All of these, and the other changes, are set out in more detail below.

In addition, as the Prime Minister announced in November, the Government has made an extra £130 million available to strengthen our ability to combat terrorism. The Counter Terrorism and Security Act 2015 introduced new measures to address specific gaps in our powers to detect and disrupt terrorist threats, particularly from British Citizens who travel to fight with terrorist groups in Syria and Iraq. The Act also placed *Prevent* and the Channel safeguarding programme on a statutory footing, creating a new duty on all public bodies to tackle radicalisation.

THE ROLE OF COMMUNICATIONS SERVICE PROVIDERS

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 graphic 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 those 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 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.

GOVERNMENT RESPONSE

The Government strongly welcomes and agrees with the Committee's view that Communications Services Providers (CSPs) have a responsibility to ensure their networks are not used to plot terrorist attacks. It is clear that terrorists are using the internet to communicate with each other. The fact that a suspect is using a foreign, internet-based communications service as opposed to a UK-based equivalent should make no difference to our ability to access that suspect's communications, if that company supplies a service to the UK. The Committee rightly identifies a number of obstacles that make it difficult for the UK authorities to obtain the data they need to in order to investigate and prevent terrorist acts.

We have engaged with large technology platforms to identify opportunities for further collaboration to enable the early identification of threats such as those made by Adebowale. The company concerned has engaged positively with Government and the company already prohibits terrorist content on its platform. The company has committed to ongoing engagement with Government to rapidly improve the identification of imminent threats and to reporting them to law enforcement. This work will help to address the Committee's concerns about the identification and subsequent referral of terrorist threats. As the Committee has recommended, the Government is engaging with a range of Communications Service Providers to press for this approach to be adopted across all relevant platforms.

More generally we are also pushing CSPs to take stronger, faster and further action to combat the use of their services by terrorists, criminals and their supporters. They are

committed to measures that make it easier for their users and the authorities to report terrorist and extremist propaganda. We will build on this to encourage companies to work together to produce industry standards for the identification, removal and referral of terrorist activity.

The Government shares the Committee's concerns about a number of CSPs based overseas who do not consider that they are bound by UK warrants, and the considerable difficulties this creates for the Agencies in accessing the content of the online communications of individuals or groups posing a threat to the UK. The Agencies cannot tackle these challenges without greater support from the private sector, including from the largest US technology companies that dominate the web.

As the Committee acknowledges, in the summer of 2014, the Government introduced emergency legislation (The Data Retention and Investigatory Powers Act 2014) to make clear that those companies offering communications services to users in the UK have an obligation to comply with our legislation. Needless to say, we expect all communications service providers to take all reasonably practicable steps to comply with our laws, which require that requests must always be both necessary and proportionate. Companies that work across international boundaries regularly have to manage parallel legal obligations and the Government expects CSPs to do their utmost to comply with UK legislation. Where there are domestic legal provisions that hinder compliance, we are working with the governments of the countries in which those companies are domiciled to look at ways in which their legal frameworks can be utilised to allow for lawful data exchange with the UK authorities to take place.

In addition, the Prime Minister appointed Sir Nigel Sheinwald as a Special Envoy on intelligence and law enforcement data sharing. Sir Nigel's objective is to lead discussions with overseas governments, CSPs, and other key international partners on ways to improve access to data that is required for law enforcement and intelligence purposes when it is stored in different jurisdictions. He is working to identify and explore how new arrangements could improve data access and sharing in both the short and longer term, whilst preserving the real benefits the internet brings. As part of his role, Sir Nigel has had a number of meetings with the US Government, European partners and US-based CSPs. He reports to the Prime Minister and Deputy Prime Minister.

MANAGING 'FOREIGN FIGHTERS'

H. SIS has told the Committee that they usually 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.

GOVERNMENT RESPONSE

The Government acknowledges the concerns of the Committee and the delay by MI5 in opening a formal investigation into Adebolajo as a result of other higher priority investigations into attack planning against the UK. MI5 investigated Adebolajo's travel to Kenya immediately upon his return and assessed the risk he posed to national security. He was also placed on the Home Office Warnings Index to flag up further attempts to travel overseas. The Government is confident that MI5 prioritises available resources and deploys them proportionately to the level of risk represented and as necessary to satisfactorily mitigate the risk, based on the information known at the time.

SIS takes its operational responsibilities very seriously and will always respond proportionately to the threat, wherever that threat emanates from. With regards to foreign fighters, SIS always takes operational and investigative decisions on the basis of what is known at the time, the nature and scale of the threat and what constitutes a proportionate response in the circumstances. In this case, the Kenyan authorities were taking appropriate action. SIS East African representatives met the Kenyan Police, ensured MI5 and the UK police were informed of the arrest, and that all information about Adebolajo held by the UK Security and Intelligence Agencies and relevant Government departments was reviewed. Any further intervention could have led to an abuse of process and justified criticisms that the UK was intervening in a domestic situation. SIS and the other Agencies assessed that the Kenyan approach was the best way to manage the situation. It allowed for Adebolajo's quick return to the UK where he could be interviewed by UK police.

The Government recognises the threat to the UK from those who go overseas to join, or attempt to join, terrorists and then return to the UK to threaten our safety has increased significantly since 2010 when this incident took place. We share the Committee's concerns about the number of individuals travelling to Syria and Iraq to engage in terrorism. This is a significant challenge to our counter-terrorism work and is an absolute priority for the Agencies.

The police and the Agencies are actively working to detect and disrupt any terrorist threat from Syria and Iraq and individuals who travel there. This includes examining

individuals at ports and the border to determine whether they appear to be involved in the commission, preparation or instigation of acts of terrorism. Passport facilities may be refused to or withdrawn from British nationals who may seek to harm the UK or its allies by travelling on a British passport to engage in terrorism-related activity.

The Counter-Terrorism and Security Act 2015 provides important measures to address specific gaps in our powers to disrupt travellers to these regions and control their return to the UK. It enhances the ability of law enforcement and intelligence agencies to monitor and control the actions of those in the UK who pose a threat; and includes measures to combat the underlying ideology that feeds, supports and sanctions terrorism. In relation to disrupting travel, the Act:

- Provides the police with a power to seize a passport at the border temporarily, during which time they will be able to investigate the individual concerned;
- Creates a Temporary Exclusion Order that can disrupt the return to the UK of a British citizen suspected of involvement in terrorist activity abroad and ensures that when individuals do return it is done in a manner which we control;
- Includes measures on aviation, shipping and rail security relating to passenger data, 'no fly' lists, and enhanced security and screening measures. These will help us to enforce our stringent requirements effectively with carriers that provide transport to and from the UK.

MI5 PRIORITISATION PROCESSES

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.

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.

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.

GOVERNMENT RESPONSE

The Government welcomes the Committee's acknowledgement that MI5 must focus its limited resources in the way that best protects national security. As such, MI5 will always have to make difficult prioritisation decisions to manage both incoming leads and on-going operations. MI5's investigative and operational staff are constantly working directly on or supporting the full range of investigations: there is no pool of reserve staff available and waiting to be deployed. MI5 is able to move resources (whether staff or equipment) at very short notice to counter high priority threats and inevitably other investigations will therefore receive fewer resources as a consequence. It is right that the majority of resources are deployed against the most significant threats, while recognising the need to mitigate the potential for a threat to emerge from lower priority casework. MI5 employs a sophisticated and flexible prioritisation process, which enables the credibility, imminence and scale of a threat to be carefully considered, and MI5's response to be directed as appropriate. This process has been developed over a number of years, and continues to be adapted as required. MI5 keeps under review all of its processes to ensure lessons are learnt and best practice is shared.

The Government keeps budgets under review and is able to adjust resource levels for the Security and Intelligence Agencies as required. In the last spending round, the Government protected the Security and Intelligence Agencies' funding.

MI5 and the police have developed and implemented a new programme for managing the level of risk posed by low level Subjects of Interest (referred to in the Committee's report as Programme DANUBE). This is now fully operational and whenever MI5 and the police close an investigation, any remaining Subjects of Interest are referred to this programme and the residual risk they pose is assessed. The Government welcomes the Committee's interest in this area and will provide the Committee with updates on this programme.

The Agencies understand the changing nature of the terrorist threat, including the increasing number of 'self-starting terrorists' and MI5's prioritisation system is sufficiently flexible to deal with threats from individuals as well as networks. Nonetheless, since the Woolwich attack and in response to the evolving threat picture, MI5 has developed a revised methodology for managing individuals judged to present a risk of carrying out violent acts of terrorism alone or in small groups outside of the more usual network based conspiracy. This fits within MI5's existing prioritisation process and has, as a result, already contributed to the disruption of at least one individual who was in the advanced stages of planning to carry out an attack of this type. This methodology is still evolving and being refined in conjunction with the police.

The Government agrees that individuals such as Adebowale and Adebolajo could be more accurately described as 'self-starting' terrorists rather than 'lone actors'.

IDENTIFICATION AND ASSESSMENT OF SUBJECTS OF INTEREST

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.

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.

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.

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.

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.

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.

GOVERNMENT RESPONSE

The Government welcomes the Committee's understanding of the need to ensure that intrusive surveillance must, at all times be necessary and proportionate: the twin test in law for intrusive actions. As the Committee notes, attendance at such extremist events is relatively common and as was the case for Adebolajo it merited some initial inquiries and the creation of an MI5 corporate record but it would not have been proportionate to seek intrusive coverage.

The Committee recommends that communication between Subjects of Interest should be taken into account, even where this is assessed to be social in nature; that evidence of support for, or espousal of 'lone wolf' rhetoric should also be considered when assessing the threat posed by an individual and that the police should pass all information about an individual to MI5, even where the police have assessed that the information is not credible. When making assessments about individuals, MI5 considers all the information available, including the context in which the information sits. MI5 appreciates the Committee's judgment regarding the recording of the specific investigative action referred to in recommendation B. MI5 has recently implemented an additional mechanism to record investigative decisions as part of a broader programme of improvements.

The Government notes the Committee's recommendation that there is a need to improve the overall process and level of communication between the police and MI5. One of the significant successes in the development of the UK's response to the renewed terrorist threat over the past decade has been the deep integration of MI5 and the police counter-terrorism activity – both at an operational and strategic level. The interdependence of the relationship has developed to such an extent that almost every process is a shared endeavour. We do however, accept that in this particular case, where there was unspecific intelligence regarding possible drug dealing activity by Adebolajo, the co-ordination between MI5 and the police was not wholly sufficient. MI5 and the police will continue to work together to ensure co-ordination is as effective as possible.

A number of improvements in the system for sharing intelligence between the police and MI5 were developed in 2011. As described in the Committee's report, this centred on the introduction of the Intelligence Handling Model, a co-ordinated multi-agency approach to ensure new intelligence benefits, where appropriate, from co-ordinated MI5, GCHQ, JTAC (Joint Terrorism Analysis Centre) and counter-terrorism police tracing and expertise. This assessment is undertaken by dedicated joint police and MI5 teams. This ensures new intelligence which meets the relevant threshold will be jointly shared as soon as it is received and remove the risk of exclusive assessment.

MI5 recognised, prior to the attack, that whilst it was confident that the overall process for managing leads was right, improvements could be made in the management and resourcing of existing assessed leads in the processing queue. Work was already underway as a result, and adjustments to the processing queue have since been implemented including devoting more staff to managing the queue and progressing investigations into assessed leads.

The police note the Committee's conclusion that they should share all information held in response to a request from MI5. However, officers and staff have to make regular decisions on the importance, validity and relevance of large quantities of information and in doing so they must consider not only the information itself, but also the source of that information. Such assessments are valuable to MI5 and rely on the training and experience of those involved. The introduction of the Intelligence Handling Model now means that all new intelligence is viewed and assessed jointly by the police and MI5.

The Government agrees that disruption of an individual's criminal activities may offer an opportunity to reduce the extremist threat they pose. One of the regular features of the close relationship between MI5 and the police is the use of non-terrorist criminal arrests and prosecutions. However, such disruptive options can only be utilised when the relevant thresholds have been reached and when the option is consistent with the investigative strategy. There must be sufficient legal grounds before an arrest can be made.

Immediately after the attack, MI5 conducted a review of its investigations into Adebolajo and Adebowale and identified the issue of recurring Subjects of Interest as one of the areas for further consideration. This review noted that it is common for Subjects of Interest to feature in more than one extremist network. Assessing and managing the

investigation of such individuals is challenging, particularly when the investigations in which they feature do not fully illuminate the nature and extent of their involvement in extremist activities.

MI5 has since developed and implemented ways of identifying Subjects of Interest who may carry out acts of terrorism alone, outside of the more usual network conspiracy, more likely using unsophisticated methods and with limited prior planning, and has set up a dedicated team to assist with the identification and investigation of such individuals. During the course of 2015, MI5 will continue to bolster its team looking at legacy investigations.

RECORD KEEPING

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.

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.

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.

GOVERNMENT RESPONSE

The Security and Intelligence Agencies and the police agree with the Committee on the importance of maintaining comprehensive records and accepts that in the instances outlined above, this was not sufficient.

SIS and the police accept, on this occasion, their record keeping was not as complete as it could have been. Both the police and SIS are reviewing their processes and seek to continually improve their record keeping. SIS has developed and is delivering a specific presentation on the Committee's Report which it is using to strengthen training on the importance of proper record keeping to staff.

The police have developed a new process to ensure effective record keeping on proposed operational activity and to ensure that, where relevant, there is better co-ordination with the Agencies where Ministerial approval it required. The police are developing fresh guidance for its Counter-Terrorism and Extremism Liaison Officers (CTELOs) to ensure improvements in their reporting and consistency when referencing intelligence originating from other Agencies. This will be accompanied by refreshed training to ensure record keeping is consistent with the existing best practices approaches developed in other areas of policing.

The Government welcomes the Committee's acknowledgement of the pressure facing investigative teams in MI5 and MI5 recognises the importance of further refining its record management process. In April 2014, MI5 created a new Branch dedicated to enhancing its management of information and the underpinning technology, providing guidance, training and best practice.

INVESTIGATIVE DECISION MAKING

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.

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 evidence they had, it was not.

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.

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 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 judgment as to whether intrusive action is necessary in counter-terrorism cases in largely a domestic issue, for which the Home Secretary should be accountable. Responsibility for any such decisions should therefore lie with the Home Secretary.

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 have then led them to be aware of further discussion between the two about potential extremist activity.

GOVERNMENT RESPONSE

The Security and Intelligence Agencies have always recognised that Subjects of Interest try to avoid detection and that they will often utilise the latest technology to try and do so. The Agencies are constantly developing new tools and techniques to ensure they maintain the ability to detect and disrupt threats to the UK. We cannot comment on the details of these techniques because to do so would render them less effective.

The Government welcomes the Committee's conclusion that intrusive surveillance can only continue where there is intelligence to justify it and the Committee's acknowledgement of the effort MI5 put into investigating Adebolajo. We also welcome the recognition that the decision to stop investigating an individual is always difficult.

The Government thanks the Committee for its acknowledgment of the commitment and dedication of the staff of MI5, and indeed all the Security and Intelligence Agencies, in ensuring a safe and secure Olympic and Paralympic Games in 2012. The Olympic and Paralympic Games posed an unprecedented security challenge for MI5 in particular. MI5 had to respond to an increased level of risk, including a heightened threat of terrorist attack planning. MI5 is required routinely to prioritise its resources to counter threats to UK's national security, but during the Games period, this prioritisation process was particularly crucial. MI5 managed this effectively in order to mitigate the most immediate and urgent threats. Thanks in part to the considerable efforts of the police and Agencies, not one security incident marred the London 2012 Games.

The Government acknowledges the Committee's conclusions that there were four 'missed opportunities' during the two years that Adebowale and five years that Adebolajo were separately under investigation.

Firstly, the Government accepts the Committee's conclusion that it was a missed opportunity not to seek further intelligence regarding Adebowale's online activity and as referenced in the Committee's Report, it is one of the lessons identified and subsequently acted on by MI5 in its own internal review. It is important to note that the additional intelligence did not indicate Adebowale was planning an attack.

Secondly, the Government accepts that MI5 could have sought the content of a reported exchange between Adebolajo and an individual of interest who later became a high profile AQAP extremist in 2008. However, MI5 note that this exchange would not have altered the course of the investigation and the fact it was not reported at the time was a strong indicator that it was not of intelligence interest.

Thirdly, in relation to the fact that MI5 did not request retrospective billing data for a landline at Adebowale's address in January 2013, we accept that some of this information may have led to different investigative decisions. It is, however, not possible to speculate what impact those decisions might have had.

Lastly, the Government accepts the Committee's conclusion that GCHQ made a mistake in not reporting the contacts of Subject of Interest CHARLIE. Even before this error came to light, due to the ever increasing volume of terrorist threats, GCHQ had put in place additional processes to monitor progress of counter-terrorism work and to formalise communications with partners, including MI5. This includes a system to track the progress of specific analytical tasks; regular video teleconferences, and a mechanism to enable relevant teams across the UK Intelligence Agencies to be alerted to potentially relevant intelligence. The Government agrees with the Committee's acknowledgement that it is not possible to speculate what impact a different investigative decision might have had, had the report been issued.

MI5 agrees that its Behavioural Science Unit (BSU) is a valuable resource to all parts of the organisation. The BSU is regularly used by investigative and agent running teams to support assessments and decision making.

It is important that there are clear lines of operational, legal and political accountability. There is a formal protocol between the Agencies to determine which Agency should lead on seeking a warrant in circumstances where more than one Agency is working on a particular operation. In such circumstances, there is a process whereby, in addition to the Secretary of State who is formally authorising the warrant, the concurrence of the other Secretary of State is sought. The Agencies also recognise the responsibility of the Home Secretary for domestic counter-terrorism matters: that is why this formal protocol has been put in place which ensures sufficient visibility for both Secretaries of State.

DELAYS IN THE INVESTIGATIVE PROCESS

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.

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.

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 in the date of its original entry, rather than re-set if it is returned to the Queue.

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.

GOVERNMENT RESPONSE

The Government accepts that the Committee's report raises significant areas of concern in relation to delays in this case. The Government acknowledges the challenges of managing the large volume of lead intelligence of varying credibility and risk against the resources available to manage the threat and the Committee's concern with regard to the Leads Processing Queue. During its own internal review, MI5 identified that while the overall process for managing leads was correct and that this process ensured every incoming lead was assessed and recorded on receipt, some adjustments were required to manage assessed leads in the Queue. Since the Woolwich attack, these adjustments have been implemented.

MI5 is also mindful of the parallel imperative of maintaining sufficient focus on identified threats already subject to investigation. MI5 acknowledges that during the period when identification of Adebowale was progressed in August 2011, the average time taken to identify individuals through these means took around two months. This was however the time for all enquiries to be completed and it was and remains the case that certain enquiries are progressed much quicker irrespective of priority and are passed to investigators to action.

The Government agrees that the length of time it took for the application referred to in Recommendation KK to be completed was not acceptable. We note the Committee's acknowledgement that post-event analysis did not provide any evidence that, had the intrusive techniques referred to been in place, they would have revealed intelligence that might have prevented the attack.

MI5 takes seriously its obligations to provide a thorough justification based on the principles of necessity and proportionality when submitting applications to the Home Secretary for deploying the most intrusive techniques. Shortly before the attack, MI5 had begun implementing additional measures designed to manage demand for applications and to provide the opportunity to improve the process for managing such applications. This included the creation of a dedicated team to manage compliance and relations with the Interception of Communications Commissioner and the Intelligence Services Commissioner, allowing other

team members to focus solely on operational delivery. It also included the implementation of further training and guidance to investigative sections on good practice when drafting applications. This naturally took time to be completely embedded and was not fully implemented at the time the attack took place. MI5 is confident that these new processes along with regular reviews will ensure the efficiency of the process of submitting applications for deploying intrusive techniques.

The Home Secretary is regularly briefed by the Director General of MI5 on a wide-range of topics. While these updates rightly focus on the current threats facing the UK, she is also kept informed on other matters of relevance to her role as the Secretary of State with democratic accountability for MI5, and this includes MI5's resource position. While allocation of resources is an operational matter for the Director General of MI5, MI5 will consider bringing critical pressures to the Home Secretary's attention where these have the potential to impact upon operational effectiveness. The Government welcomes the Committee's recognition that the Director General of MI5 must have operational independence.

TACKLING EXTREMISM AND *PREVENT* STRATEGY

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.

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.

GOVERNMENT RESPONSE

The Government shares the Committee's view that engagement with extremist media needs to be taken extremely seriously. The Government uses a range of measures to restrict

access to extremist and terrorist content online and we are determined to continue our efforts to make such material unavailable. In many cases, engaging with extremist media online would merit further investigation, and where this involves the use of intrusive measures, and where known Subjects of Interest have accessed such material, decisions about what measures should be used will always be taken on the basis of legality, necessity and proportionality.

The Government, whilst noting the Committee's comments on the effectiveness of the *Prevent* programme, was however disappointed that the high priority which has been afforded to this important work was not acknowledged. The Government fully agrees with the Committee's assessment of the significant impact which *Prevent* can offer in diverting individuals from the radicalisation path. That is why we restructured the *Prevent* programme in 2011 and announced additional support for it in November 2014. There is no single reason or path that leads an individual to become radicalised and no single action can be taken to deter radicalisation. The point at which the opportunity to deter an individual from becoming radicalised presents itself will vary between individuals. As a result, we work to respond to the ideological challenge of terrorism, work with sectors and institutions where there are risks of radicalisation, and prevent people from being drawn into terrorism or supporting terrorism, with appropriate advice and support. Police and other partners now routinely consider preventative interventions where appropriate.

The Government has delivered over 180 community-based *Prevent* projects since 2011 and *Prevent* local projects have reached over 55,000 people since early 2012. Hundreds of people have been offered support through the Channel safeguarding programme. However, we continually look for opportunities to strengthen our response and have now placed *Prevent* and Channel on a statutory footing. This has hardwired them into the work of frontline professionals in local authorities, the education sector, prisons and many other bodies.

The Extremism Task Force was set up in July 2013 to consider what more the Government could do to reduce the threat from extremism. The Task Force continues to meet, and we are implementing a raft of practical measures to strengthen our approach across a range of sectors, including prisons, schools, universities and online. In September 2014, the Home Secretary announced that the Home Office will, for the first time, assume responsibility for a new counter-extremism strategy that goes beyond terrorism. The strategy will aim to build up the public sector and civil society to identify extremism in all of its forms, confront it, challenge it and defeat it.

The Government is disappointed that the Committee has concluded that counter-narrative work is not a priority for the Home Office. The Research Information and Communications Unit (RICU) is a government strategic communications unit which works to counter the narratives of extremists and propagandists for terrorism by training civil society activists, putting communications capabilities at their disposal, conducting research into terrorist narratives and consulting across government. The work of RICU is crucial to the

Prevent strategy, and the Government recognises the valuable role it plays in developing a counter-narrative to extremist messages.

MI5 continues to support the wider Government *Prevent* strategy, and works closely with the police to embed this within the end-to-end process for managing extremist threats in the UK. As part of this, MI5 has invested in training for its entire investigative staff to improve understanding of *Prevent* processes. In counter-terrorism operations, *Prevent* is now considered as an option where appropriate across the full range of investigations. A *Prevent* referral is now the default option (except where there are operational sensitivities) for the lowest-risk Syria related Subjects of Interest.

PROSCRIPTION

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.

GOVERNMENT RESPONSE

The Government recognises that suspected membership of a proscribed group should be an important indicator in the assessment of whether to instigate formal investigative processes. MI5 and the police agree with the Committee's conclusion regarding the complex nature of the threat and the challenges in identifying the threat posed by groups and individuals. MI5 and the police make careful decisions, on a case-by-case basis, as to the investigative response which is necessary and proportionate to the specific threat posed. This will include any information regarding an individual's affiliation to a proscribed organisation.

The Government welcomes the Committee's conclusion that there is benefit to proscribing organisations. Proscription of terrorist groups shows the Government's

condemnation of their activities and sends a strong message that terrorist organisations are not tolerated in the UK. The Government notes the ISC's recommendation to consider whether any changes could be made to existing legislation to enable more effective prosecutions for membership of a proscribed organisation.

Groups proscribed in 2014 and 2015 included the Islamic State of Iraq and the Levant (ISIL) and six other groups linked to the conflict in Syria. Proscription deters terrorist groups from operating in the UK and gives the police powers to tackle any UK based support for the group.

ALLEGATIONS OF WRONG-DOING

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 the 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.

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 ***.**

GOVERNMENT RESPONSE

The Government welcomes the Committee's conclusion that there is no evidence of wrong doing by MI5 in relation to allegations made about its actions in relation to Michael Adebolajo and their understanding of the need to protect national security by not commenting on the specifics of the allegations. The principle of 'neither confirm nor deny' is essential to the operational effectiveness of the Agencies. In order to be effective, the principle must apply even if no activity has taken place. If the Government were to deny a particular activity in one instance, the inference would be drawn that the absence of a denial in any other instance amounted to confirmation of the alleged activity.

In countries where the Government mentors foreign counter-terrorism units, these units are not controlled or managed by the UK: they remain organs of the sovereign state in which they are situated, and regularly receive national tasking on which the UK is unsighted and has no involvement. The primary role of a UK mentor to such a unit is to foster a human rights compliant approach and to improve local counter-terrorism capabilities.

Where the UK is involved in an operation, stringent safeguards are in place regarding these arrangements, including the Overseas Security and Justice Assistance Guidance and the Consolidated Guidance. If the Government assessed there was a serious risk of unacceptable treatment, or significant failures in compliance, which could not be effectively mitigated, then the UK would suspend its engagement with a particular unit and inform Ministers.

The Government and the Agencies stand firmly against torture and cruel, inhumane or degrading treatment or punishment. We do not condone it, nor do we ask others to do it on our behalf. SIS takes allegations of human rights abuses very seriously. As soon as the Government was made aware of his allegations, both the Foreign Office and SIS took actions to investigate them, including writing to Adebolajo to seek further details, to which he did not

respond. SIS asked its East Africa representatives to investigate the allegations, as evidenced by the message included in the Committee's Report. SIS accepts that it should have formally recorded the actions taken to investigate this allegation and the conclusions reached, but does not accept this means that it does not take its responsibilities seriously.

The Government agrees that SIS needs an evidence base against which to consider their work with liaison partners, but does not agree that the Country Assessment programme should be restarted. Country Assessments were a trial programme which concluded that, whilst these provided a useful mechanism for recording background information about a particular country, they soon became out of date as new information was received. The Foreign Office was concerned this could cause assessments of risk to be made on the basis of out of date information. SIS makes its decisions about how to engage with a particular liaison partner on the basis of all available information, which must be up-to-date.

A new formal tool for ensuring all our overseas security and justice assistance work meets the Government's human rights obligations and values was introduced in December 2011. This is the Overseas Security and Justice Assistance (OSJA) Guidance. The OSJA enables dynamic assessments to be made, on the basis of all available information, about how to engage with partner countries. It works at both a strategic and an operational level and provides SIS, among others, with a more effective tool for risk assessment than the Country Assessments.

It is right that there should be rigorous oversight of these issues. That is why the Prime Minister placed the oversight role of the Intelligence Services Commissioner, Sir Mark Waller, on a statutory footing in November 2014 and why he asked Sir Mark to examine the concerns raised by the Committee about the Government's responsibilities in relation to partner counter-terrorism units overseas. Sir Mark has started his examination and will report his findings in due course. SIS is co-operating fully with Sir Mark and will ensure any recommendations arising from his examination are fully addressed.

ISBN 978-1-4741-1513-1