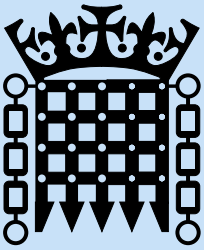


Intelligence and Security Committee of Parliament

The 2017 Attacks: What needs to change?

Westminster, Manchester Arena, London Bridge, Finsbury Park, Parsons Green

Chair:
The Rt Hon. Dominic Grieve QC MP

HC 1694

Intelligence and Security Committee of Parliament

The 2017 Attacks: What needs to change?

Westminster, Manchester Arena, London Bridge, Finsbury Park, Parsons Green

Chair:
The Rt Hon. Dominic Grieve QC 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
22 November 2018

HC 1694

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

This publication is also available on our website at: isc.independent.gov.uk

ISBN 978-1-5286-0861-9

CCS0818342688 11/18

Printed on paper containing 75% recycled fibre content minimum

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

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

The Rt Hon. Dominic Grieve QC MP (Chair)

The Rt Hon. Richard Benyon MP
The Rt Hon. Ian Blackford MP
The Rt Hon. Caroline Flint MP
The Rt Hon. David Hanson MP
The Rt Hon. the Lord Janvrin GCB GCVO QSO
The Rt Hon. Kevan Jones MP
The Most Hon. the Marquess of Lothian PC QC
The Rt Hon. Keith Simpson MP

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

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

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

The Committee makes an annual report to Parliament on the discharge of its functions. The Committee may also produce reports on specific investigations. Prior to the Committee publishing its reports, sensitive material that would damage national security is blanked out ('redacted'). This is indicated by *** in the text. The Security and Intelligence 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.

* The Committee oversees operations subject to the criteria set out in section 2 of the Justice and Security Act 2013.

CONTENTS

EXECUTIVE SUMMARY

During 2017, the United Kingdom suffered five serious terrorist attacks:

- On 22 March, Khalid MASOOD drove a car over Westminster Bridge, mounted the pavement and hit pedestrians walking on the bridge. He then entered the grounds of the Palace of Westminster and fatally stabbed a police officer. Five individuals were killed in the attack with many more seriously injured.

- On 22 May, SALMAN Abedi detonated an improvised explosive device (IED) in the foyer of Manchester Arena. Twenty-two people were killed, including a number of children and teenagers. Over 100 others were injured.

- On 3 June, Khuram BUTT, Rachid REDOUANE and Youssef ZAGHBA used a van to run over pedestrians on London Bridge, before continuing their attack on foot. Eight people were killed in the attack with many more injured.

- On 19 June, Darren OSBORNE drove a vehicle into a group of people gathered near an Islamic Centre in Finsbury Park in north London. One person was killed and ten others sustained serious injuries.

- On 15 September, Ahmed HASSAN left an IED on a District line commuter train. The device partially exploded after the train arrived at Parsons Green station. Twenty-three people sustained burn injuries as a result of the partial explosion whilst 28 people suffered crush injuries as crowds surged to exit the train.

Immediately following the attacks, MI5 and Counter Terrorism Policing (CTP) launched a number of reviews in order to identify what was known about the attackers prior to each attack, and to review their assessments, actions and decisions. They also established an Operational Improvement Review (OIR), which sought to identify and recommend improvements in counter-terrorism work. Lord Anderson of Ipswich KBE QC provided independent assurance of the robustness of the process. The Committee commends MI5 and the police for taking the initiative in conducting their own, very thorough, reviews and welcome the independent assurance provided by Lord Anderson. Nevertheless, 36 lives were lost and we therefore regarded it as essential to establish for ourselves whether mistakes were made, and to ensure that all changes and improvements required have been identified.

We have considered the actions of MI5 and CTP in relation to cross-cutting issues that can be seen as having played a part in the actions of those who perpetrated the attacks. While the detail on each is contained in the main body of the Report, we wish to highlight the following points:

(i) There has been an enormous growth in the volume of extremist material that can be found online. Studies have shown that almost all attack planners between 2012 and 2017 have downloaded, shared or consumed radical and extremist media of some kind. However, the quantity of material and the ease with which it can be uploaded, versus the difficulty and time it takes to remove it, means that the authorities will always be 'playing catch up'. This Committee was the first to identify the problem of Communications Service Providers (CSPs) failing to assist the authorities by removing extremist material from their platforms. In 2014, we urged Government to engage with the CSPs to get them to accept responsibility and take steps to prevent their systems becoming a safe haven for

extremist content and terrorist communications. While the major CSPs are beginning to engage more with this issue, there has still been little tangible progress over the last four years. We question whether this is because efforts to persuade the CSPs have sought to appeal to their sense of corporate and social responsibility, instead of concentrating on financial levers. When there was a social media backlash against companies whose adverts appeared alongside extremist videos on YouTube, those companies had little choice but temporarily to stop advertising on YouTube. More recently, Unilever announced that it is considering withdrawing its business from companies that are not doing more to provide "*responsible digital infrastructure*".[1] Action that affects the CSPs' profits clearly hits home harder than any sense of 'doing the right thing': the UK Government should now seek to lobby the business community to take action, following the Unilever example.

(ii) In relation to extremism in prisons, we support the proposal to improve the Approved Visitor Scheme in relation to Category A prisoners but note that the monitoring of visitors to extremist prisoners below Category A is haphazard. This is concerning – SALMAN Abedi, the Manchester Arena attacker, visited an extremist prisoner in a lower category.[2] Consideration should therefore be given to expanding the Approved Visitor Scheme to include all extremist prisoners. Furthermore, while we recognise the intention behind segregating extremist prisoners, we, like others, are concerned that the new Separation Centres may provide a networking opportunity for extremists.

(iii) Given the propensity for vehicles to be used as weapons – as can be seen in the Westminster, London Bridge and Finsbury Park attacks in the UK but also in a number of attacks across Europe – monitoring vehicle hire must be a significant element of counter-terrorism work in future. Currently, incompatible systems and limited capabilities are hindering progress in this area. Whilst we are encouraged that this is an area on which the Department of Transport and the Home Office are working, we note that it is still very much in the developmental stage. We also note that the *** of the proposed scheme significantly reduces the likelihood of its success.

(iv) The explosives used by terrorists are *** to produce by following *** instructions available on the internet. The key therefore lies with the ingredients required (the 'precursors'), and how access to them is regulated. The previous system for regulating and reporting purchases of the ingredients used to make explosives was out of date in dealing with the threat at the time. The Manchester Arena bombing showed this, to devastating effect. We welcome the updates to the system of regulating and reporting explosive precursor purchases, and the intent to improve co-operation and information sharing between retailers and law enforcement. Nevertheless, we note that the fact that these ingredients can be used for non-criminal purposes means that they will continue to be available commercially, making it extremely difficult to monitor all purchases.

(v) ***

(vi) Previous ISC Reports – including the Woolwich Report[3] and the original 7/7 Report[4] – have raised concerns as to how well MI5 and CTP work together. Last year's attacks revealed that there were still problems around the sharing of MI5 information with CTP, and the

[1] 'Unilever threatens to pull ads from Facebook and Google', BBC News, 12 February 2018.
[2] ***
[3] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.
[4] *Report into the London Terrorist Attacks on 7 July 2005*, Cm 6785.

involvement of CTP in MI5 decision making. We recognise that improvements have been made, but this is an area that requires continuous improvement: we would highlight the need to address cultural differences and incompatible IT systems in particular.

(vii) Previous ISC investigations have also focused on the approach towards low-priority investigations and low-level Subjects of Interest (SOIs), those who have appeared on the periphery of investigations, and SOIs who have been 'Closed'. The issue of how often Closed SOIs are subject to review arose again in the cases of the Manchester Arena attacker and the Westminster attacker. In the case of the latter, he had not been flagged as potentially posing a renewed risk by any review of Closed SOIs prior to his attack. In the case of the former, while he had been flagged for review, MI5's systems moved too slowly, and this had not happened before he launched his attack. Overall, it is clear that MI5 are now taking serious steps to improve their management of Closed SOIs: we welcome this and recognise the scale of this task given the size of the pool. It is disappointing, however, that previous recommendations of this Committee have clearly not been taken on board until now.

(viii) In relation to those seen on the peripheries of investigations – as was the case for both the Westminster attacker and the Manchester Arena attacker – we recognise that 'joining the dots' between pieces of information and identifiers is a highly complex task, but we nonetheless urge MI5 to consider what more can be done to connect those seen on the peripheries of investigations, including what processes they need to have in place to take account of the cumulative effect of an individual appearing on the periphery of numerous investigations.

(ix) The Committee questions the decision not to use travel monitoring and travel restriction capabilities in the case of the Manchester Arena attacker, allowing him to return to the UK undetected in the days immediately before he carried out his attack. We recognise that there still may not have been sufficient time to identify or act on his attack planning. It would, nevertheless, have provided more of an opportunity. We welcome the change in policy regarding the monitoring of SOIs – although in our opinion this should have been in place previously.

(x) Also in relation to travel, we consider that an eight-week delay between the receipt of a request from an international partner and onward dissemination for action – as in the case of one of the London Bridge attackers – is far too long. Delays of this nature could have a very significant impact on an operation, not just here in the UK but in other countries too.

(xi) In its 2014 Woolwich Report, the Committee noted a failure to refer individuals to Prevent. This issue – dismissed by Government at that time – has arisen again in the case of the Manchester Arena attacker. At no point was he or his family referred to Prevent.

(xii) In the case of the Parsons Green attacker, who was subject to a Prevent referral, we note that we have only been able to make an initial assessment of the case due to the Home Office failure to provide evidence. From what we have seen, it is clear to the Committee that there have been fundamental failings in the manner in which HASSAN's case was dealt with by the Home Office, the police and Surrey County Council. The litany of errors that resulted in HASSAN's attack planning passing unnoticed, despite his being an active Channel case, highlight deep-rooted issues in the administration of the Prevent

strand of CONTEST. The Committee hopes that the Home Affairs Select Committee will instigate a thorough review of the Prevent programme in relation to this case.

(xiii) Despite it not having been seen as a problem in itself in any of the attacks, MI5 and CTP have taken the opportunity of the Internal Reviews to reassess their approach to data, given the considerable increase in data both produced and accessed by the Agencies. We note the new 'multi-agency approach' proposed, whereby MI5 will allow knowledge derived from their intelligence to be shared outside of the traditional security community with a wider range of partners at national and local level. The Committee also welcomes the thought being given to working alongside industry and academia to ensure that the Agencies are able to keep pace with the increase in available data and – crucially – advances in data analytics in order to use data in a more innovative way. This partnership has the potential for significant skill and capability transfer in what will be an increasingly important area for the Agencies.

As can be seen from the points we have highlighted here, it has been striking how some of the issues which arose in relation to the 7/7 attacks and the killing of Fusilier Lee Rigby have also been seen as having been a factor in the 2017 attacks. We have previously made recommendations in these areas, yet they do not appear to have been acted on. This has been recognised by those we have spoken to during the course of this review. The National Security Adviser has committed to putting a formal mechanism in place for all recommendations made by this Committee, which we have requested be reported to us on a quarterly basis.

That is not to say that there have been no improvements made: both MI5 and CTP have been thorough in their desire to learn from past mistakes. We note that the Director General of MI5 has been clear for a number of years that they cannot foil every attack, given the scale of the threat and the methods now being employed. However, that is not used as an excuse: we have seen the determination with which this work is approached and we commend them.

SECTION 1: INTRODUCTION

1. During 2017, the United Kingdom suffered five serious terrorist attacks: at Westminster, Manchester Arena, London Bridge, Finsbury Park and Parsons Green. Thirty-six individuals were killed[5] and over 200 were injured.

2. Of the seven perpetrators and one alleged co-conspirator,[6] five were killed at the scene of the attack. The Finsbury Park attacker has been jailed for life, serving a minimum of 43 years, and the Parsons Green attacker has been handed a life jail sentence with a minimum of 34 years.[7] The alleged co-conspirator in the Manchester Arena attack has been detained in Libya by a militia group: the British Government is currently seeking to extradite him so that he can stand trial in the UK.

3. Immediately following the attacks, the Security Service (MI5)[8] and Counter Terrorism Policing (CTP)[9] launched a number of Internal Reviews in order to:

- identify what was known about the attackers and co-conspirators prior to each attack;
- review assessments, actions and decisions made prior to each attack in relation to intelligence held on the attackers and co-conspirators;
- identify and review contextual information that may have had a bearing on actions and decisions made; and
- identify learning points arising out of each case.[10]

In addition to these Internal Reviews, MI5 and CTP – supported by the wider intelligence community – established an Operational Improvement Review (OIR) which sought to identify and recommend improvements in counter-terrorism work. The then Home Secretary asked Lord Anderson of Ipswich KBE QC to oversee the Internal Reviews in order to provide independent assurance of the robustness of the process. He was provided with complete access to the Internal Review work and produced his report in December 2017. The Committee commends MI5 and CTP for taking the initiative in conducting their own, very thorough, reviews and welcome the independent assurance provided by Lord Anderson.

The Committee's Inquiry

4. The Committee received copies of the MI5 and CTP Internal Reviews in December 2017. Since then we have taken evidence from MI5, CTP and the Home Secretary. In addition to the Internal Reviews, we have also considered primary material relating to the attacks provided by

[5] Not including the perpetrators.
[6] At publication of this Report, the trial relating to HASHEM Abedi's role in the Manchester Arena attack had not concluded. Therefore he is referred to as an 'alleged' co-conspirator throughout this Report.
[7] Darren OSBORNE, perpetrator of the Finsbury Park attack, was found guilty of both murder and attempted murder and will serve two concurrent life sentences. Ahmed HASSAN, the Parsons Green attacker, was convicted of attempted murder and also handed a life sentence. The judge said he would treat the incident as a terrorist offence.
[8] For ease, this Report will refer to the Security Service as 'MI5' throughout.
[9] For ease, this Report will refer to Counter Terrorism Policing as 'CTP' throughout.
[10] MI5 and CTP, *Operational Reviews Capping Document*, October 2017.

both MI5 and CTP. This includes highly classified documents, investigation records, ***, and other intelligence reports.

5. On 4 June 2018 (after the Committee had finished holding its evidence sessions), the Home Secretary announced the publication of the Government's new 2018 CONTEST Strategy. Two days later, on 6 June, the Government announced a new Counter-Terrorism and Border Security Bill. The Committee has reflected information contained in these two publications in its Report where relevant but has not sought to undertake a review of them.

6. MI5, CTP and the Office for Security and Counter-Terrorism (OSCT) co-operated fully with our Inquiry and all requests associated with it throughout – despite it being a period during which they were under very significant operational pressure – and we recognise their clear intention to identify and learn all possible lessons from the tragic events of 2017. This Committee is aware of the exceptional effort made by the staff who work for MI5 and the police to protect the UK from attack. The threat level is currently at SEVERE and has been since September 2017 (it was briefly at CRITICAL from 23–27 May 2017 and again from 15–17 September 2017). There have been 13 attack plots foiled since the Westminster attack, alongside 445 counter-terrorism-related arrests from April 2017 to March 2018 (representing a 17% increase on the previous year), with many more plots disrupted. The Director General of MI5 has been clear for a number of years that they cannot foil every attack, given the scale of the threat and the methods now being employed. Giving evidence to this Inquiry, MI5 and CTP were clear that 2017 saw a step change, with a shift in the threat, largely due to the impact of Syria and Iraq. This – combined with the speed of the radicalisation process – meant that they were no longer able to concentrate solely on the immediate threat but were also having to consider how to manage the level of risk inherent with this volume. However, that is not used as an excuse: we have seen the determination with which this work is approached and we commend them.

7. Nevertheless, these were the first terror attacks in Britain since the murder of MP Jo Cox in 2016, with 36 lives lost. While the Committee welcomed the detailed review work that MI5 and CTP have undertaken, and the assurances provided by Lord Anderson, we regarded it as essential to establish for ourselves whether mistakes were made, and to ensure that all changes and improvements required have been identified.

Transparency

8. This Committee has always sought to place in the public domain as much information as possible about the ways in which the intelligence community work. However, in some instances, to do so would either be illegal or would severely damage the Agencies' ability to protect the UK. In our *Report on the intelligence relating to the murder of Fusilier Lee Rigby* we gave the following example: any material that 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 to act as agents if they do not trust that the intelligence they provide will be treated in confidence or if they fear that they, or their families, will end up in danger. Other examples include sensitive intelligence collection capabilities or intelligence gained from intercepted communications.

9. There are other categories of information that the Agencies might seek to protect, on the basis that disclosure 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:

- material that relates to how the Agencies conduct operations could reveal their techniques to those who seek to harm the UK. They could then change their behaviour to avoid detection;

- intelligence that has been provided by an overseas Agency is 'owned' by that Agency and it is not the UK's to disclose without their 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.

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.

10. 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; and

(ii) none of the material redacted affects the substance of this Report in any way.

SECTION 2: ABOUT THE ATTACKS

Westminster

- On 22 March 2017, Khalid MASOOD drove a hired car over Westminster Bridge, mounted the pavement and hit pedestrians walking on the bridge. MASOOD then came to a stop outside the Palace of Westminster, exited the vehicle and on entering the palace grounds fatally stabbed a police officer.
- Five individuals were killed in the attack with many more seriously injured.
- MASOOD was killed by an armed police officer.

MASOOD had an extensive criminal (non-terrorism) history dating back to 1978. His most notable offences were convictions for violent crimes in 2000–2003.

Between 2004 and 2013, MASOOD was known to MI5 due to his links to, and participation in, extremist circles. He was actively investigated by MI5 between 2010 and 2012. MASOOD was assessed to be a distributor of extremist material and possibly involved in facilitating the travel of individuals of concern to the Federally Administered Tribal Areas of Pakistan. Investigation into MASOOD was closed in 2012 and remained so until the attack in 2017. During the period 2012–2016, MI5 observed intermittent contact between MASOOD and other individuals of interest but nothing that met the threshold for re-investigation.

Manchester Arena

- On 22 May 2017, SALMAN Abedi detonated an improvised explosive device (IED) in the foyer of Manchester Arena as a concert came to a close.
- Twenty-two people were killed, including a number of children and teenagers. Over 100 others were injured. SALMAN Abedi was also killed by the device.
- Post-attack investigations identified that SALMAN's brother, HASHEM Abedi, was an alleged co-conspirator in the Manchester Arena attack.

In 2014, SALMAN Abedi was briefly investigated by MI5, as he was suspected of being an individual who had been observed acting suspiciously alongside an existing Subject of Interest (SOI).[11]

Between 2015 and 2017, the authorities received reporting in relation to SALMAN's activities. An internal MI5 process in March 2017 had raised SALMAN's name for potential further investigations; however, final decisions on this had not taken place by the time SALMAN launched his attack.

[11] Investigation into SALMAN was ceased due to his limited contact with the SOI and as he had been assessed not to have been identical with the individual mentioned in the original reporting.

London Bridge

- On 3 June 2017, Khuram BUTT, Rachid REDOUANE and Youssef ZAGHBA used a van to run over pedestrians on London Bridge. They then abandoned the van and continued the attack on foot using knives before all three attackers were killed by armed police.
- Eight people were killed in the attack with many more injured.
- This was publicly claimed by Daesh.

Khuram BUTT first came to the attention of authorities *** in relation to investigations into proscribed extremist group Al Muhajiroun. BUTT was actively investigated by MI5 between mid-2015 and 2017 following reports of aspirations to conduct an attack in the UK. The investigation into BUTT remained open at the time of the attack; however, MI5 had not detected any signs of attack planning.

ZAGHBA had not been investigated by MI5 prior to the attack, although he was known to the Italian authorities.

REDOUANE had not been investigated by either MI5 or CTP prior to the attack.

Finsbury Park

- On 19 June 2017, Darren OSBORNE drove a vehicle into a group of people gathered near an Islamic Centre in Finsbury Park in north London.
- One person was killed and ten others sustained serious injuries.
- OSBORNE attempted to flee the scene on foot but was restrained by members of the public.
- The post-attack investigation indicates that OSBORNE acted alone.
- On 2 February 2018, OSBORNE was found guilty of murder and attempted murder and sentenced to life in prison, with a minimum term of 43 years.

OSBORNE had an extensive criminal history dating back to 1984, including 33 convictions for 102 offences ranging from offences against the person to drugs and theft.

OSBORNE had not been investigated by MI5 or CTP prior to launching his attack and was not known to be a member of, or have links to, any extremist right-wing groups.

Parsons Green

- On 15 September 2017, Ahmed HASSAN left an IED on a District line commuter train. The device partially exploded after the train arrived at Parsons Green station.
- Twenty-three people sustained burn injuries as a result of the partial explosion whilst 28 people suffered crush injuries as crowds surged to exit the train.
- HASSAN had left the train one station before the bomb exploded. He was arrested the following morning in Dover.
- Forensic analysis indicated that the IED had been constructed at a property owned by HASSAN's foster parents.
- On 16 March 2018, HASSAN was found guilty of attempted murder and sentenced to life in prison, with a minimum term of 34 years.

Whilst HASSAN had revealed in an asylum interview that he had been taken by Daesh and trained to kill, he had not been investigated by MI5 prior to launching his attack.[12]

In February 2016, HASSAN was referred, by CTP, to the Channel programme. He was placed with foster parents and provided with a range of social and diversionary activities as well as health (including mental health) support.

Between June 2016 and September 2017, a Channel panel met to discuss HASSAN's case on nine separate occasions. At the time HASSAN launched his attack, the panel was in the process of considering the closure of HASSAN's case.

[12] ***

SECTION 3: INTELLIGENCE AND INVESTIGATIONS

Intelligence

11. The Committee's Report *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005* described the nature and uses of intelligence:

> *Secret intelligence is information that is lawfully gathered by the Agencies, but without the consent of the target. It can come from an individual, an organisation or a country. Intelligence, as defined by the Agencies, can include anything from a report from a recruited agent, intercepted telephone calls to covert eavesdropping of a person's home. Intelligence has to be assessed to decide how reliable it is including the reliability of the source. It also has to be analysed to decide what facts are important and what are not.*[13]

Other ISC Reports have discussed the limitations to intelligence – noting that it may be very fragmented and only give a partial picture, and it can also be misleading so there will inevitably be gaps in what MI5 and the other intelligence Agencies know at any given time.

Investigative model

12. MI5 are reliant on information collected either from their own activities or provided to them by external sources, whether that is the public, police or partner agencies. The storage and analysis of this information is vital and MI5's Key Information Store − a collection of records about people, places and objects – is therefore central to the Agency's work. When we talk of MI5 'opening a file' or 'keeping a file' on someone, it means they are a person of potential national security interest on whom MI5 have created a record in the Key Information Store. Such a record can be created before a person of interest has been fully identified (for example, if just their email address or telephone number is known, and it has not yet been linked to an individual). For ease of reference, such individuals are called 'Subjects of Interest' (SOIs). MI5 describe an SOI as someone or something who is, or has been, investigated because they are suspected of being a threat to national security.

13. MI5 and CTP jointly assess all new reporting relating to terrorism against an agreed Intelligence Handling Model. At its simplest, this model comprises the following elements (at each stage MI5 and CTP will continue to assess necessary and proportionate actions to take):

- New information or intelligence is received (e.g. from agents, GCHQ reporting, foreign liaison partners, calls to the anti-terror hotline, etc.) either by MI5 or CTP, who will conduct preliminary 'traces'. A trace is a search across MI5 and CTP databases to ascertain what is known about the subject.

↓

- If the subject of the reporting is already under investigation, the new intelligence will be directed to the appropriate MI5 and CTP team.

[13] *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, Cm 7617.

OR

- If the information is completely new, MI5 and CTP undertake a 'triage' process to assess the new information in terms of national security risk, credibility, 'actionability' and proportionality. If the intelligence or information meets these criteria it may become a 'lead'. Leads are allocated a colour based on risk (Red/ Amber/Green) and a credibility banding (1/2/3). A record of this lead investigation will be made in the Key Information Store, and a form will be completed on considerations around the intelligence and agreed actions.

↓

- Intelligence relating to a new individual of national security concern may also lead to a decision to open a new record on that person. If the individual is linked to an existing investigation, they may be referred to this investigative team.

- The purpose of a lead investigation is to develop the intelligence picture to understand the risk and determine credibility. The actions undertaken on a lead will allow MI5 and CTP to make an assessment as to how much resource to continue to dedicate. For example, lead development may involve attempting to find out who an email address or mobile telephone number belongs to.

- If the assessment determines that the lead has no national security context, lacks credibility, or is not 'actionable', it will be closed or handed to a more relevant agency, or the police, to deal with.

- A credible and actionable lead that represents the greatest risk may be converted into an investigation, and further resource will be allocated accordingly.

14. As at 1 August 2017, the number of 'live leads' was ***, almost *** the number in August 2016. These leads were categorised as follows: *** Red (representing the greatest risk), *** Amber (time sensitive) and *** Green (non-urgent). The remaining leads are Initial Assessment (IA)[14] leads.

Investigations

15. In many cases, investigations are created around 'networks' of SOIs involved in a common plot or with a shared goal. MI5 prioritise investigations according to risk and this is constantly reviewed according to new intelligence obtained or any change in the threat.

[14] MI5 and CTP use IA leads when the initial intelligence does not allow a decision as to whether there is a national security risk without further traces and enquiries being made.

Priorities (investigations)

There are four 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, funding terrorism or other extremist activity.
- 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.

SOIs involved in low-priority investigations (i.e. Priority 3 or 4) can be thought of as 'low-level SOIs'.[15]

16. In addition to the priorities attached to particular investigations, every SOI within an investigation is also prioritised.

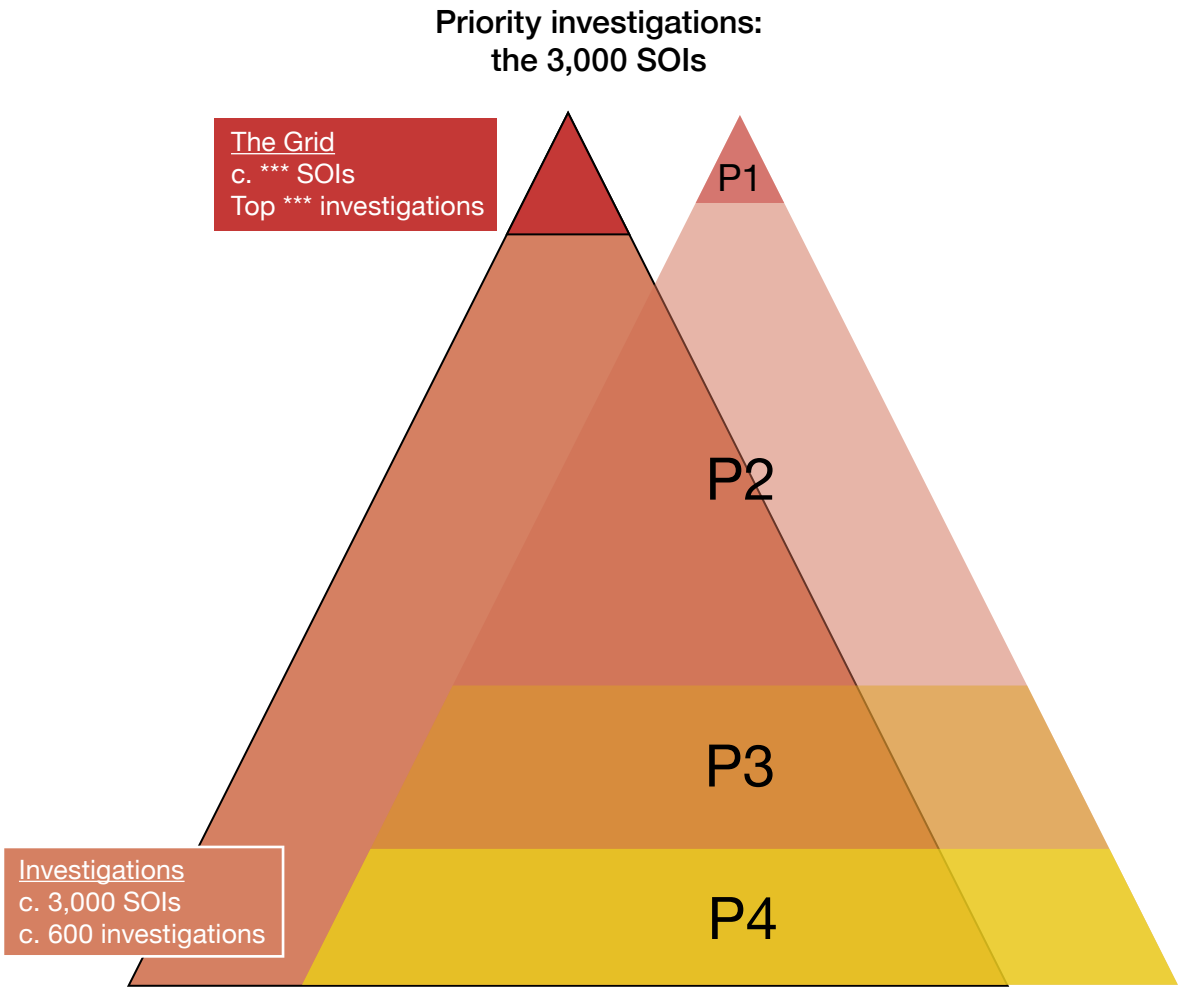
Tiers (SOIs)

- 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.

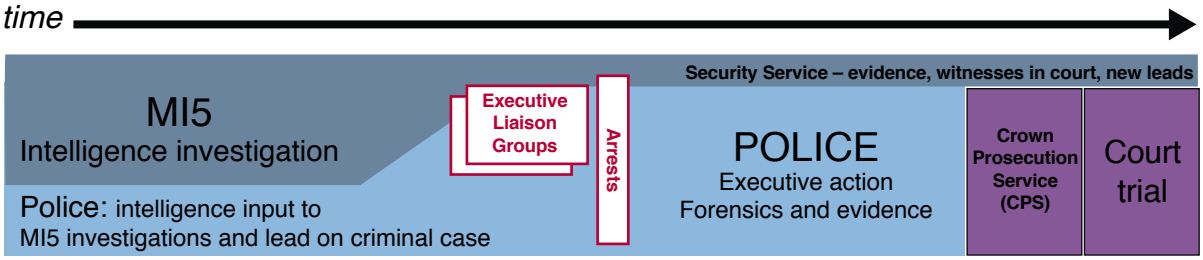
Individuals in Tier 3 are not the main SOIs in an investigation and can be thought of as 'peripheral SOIs'.[16]

17. The graphic on the following page depicts MI5's priority investigations (as of April 2018). It demonstrates how MI5's most important investigations are divided into the different prioritisation categories outlined above.[17]

[15] We note that 'low-level SOI' is not a term used by MI5, but we have used it in this Report for ease of reference.
[16] We note that 'peripheral SOI' is not a term used by MI5, but again we have used it in this Report for ease of reference.
[17] Adapted from written evidence – MI5, 5 April 2018.



18. The following diagram outlines the investigative model:



19. In order to monitor SOIs, the Agencies and CTP have a range of investigative tools available to them. These include:

- Communications Data (details about a communication, including 'who, when and where' but not the content of what was said or written);
- Bulk Personal Datasets;
- Use of agents;
- Interception of Communications;

- Interference with Wireless Telegraphy (for example TV/radio signals or mobile phone signals);
- Interference with Property (including Equipment Interference); and
- Surveillance.

Further information relating to the use of investigative powers by the Agencies can be found in the ISC's Report *Privacy and Security: A modern and transparent legal framework*.[18]

20. When an investigation concludes,[19] if any of the SOIs who have been investigated within it are still active (i.e. they have not been disrupted), and are engaging in other activities of national security concern, they may be reallocated to an existing relevant investigation or become the subject of a new separate investigation.

21. In some circumstances an SOI might be 'Closed'. This happens when they are assessed to no longer pose an active risk to national security. This could be for a variety of reasons including: arrest, prosecution, deportation, ***, or them disengaging from the activity they were involved with.[20] MI5 retain a file on every Closed SOI, even if they are no longer under active investigation by MI5 (they may continue to be investigated for other suspected criminality by the police). 'Closed SOIs', whether successfully disrupted or not in the past, may re-engage in terrorism and extremism at any time. This residual risk from Closed SOIs is considered in Section 10 of this Report.

[18] *Privacy and Security: A modern and transparent legal framework*, HC 1075.
[19] Investigations may close at any time depending on the necessity and proportionality of continuing to investigate the individual or network.
[20] At this point, MI5 will assess the residual risk that the SOI poses.

SECTION 4: EXTREMIST MATERIAL ONLINE

Access to extremist material online is reported to have played a key role in the Manchester Arena attack,[21] and may have been a factor in radicalising the London Bridge attacker and the Westminster attacker.

- Manchester Arena: *** SALMAN Abedi may have gained further expertise in Libya.
- London Bridge: Khuram BUTT is thought to have frequently accessed extremist material online, ***.
- Westminster: Khalid MASOOD is thought to have viewed general extremist material, although he had viewed some more extreme material on beheadings and executions on YouTube.

22. According to the Home Office, 'extremist material' includes:

- articles, images, speeches or videos that promote terrorism or encourage violence;
- content encouraging people to commit acts of extremism;
- websites made by terrorist or extremist organisations; and
- videos of terrorist attacks.[22]

23. Currently, there are a number of criminal offences relating to accessing extremist material online, including:

- collecting or recording information likely to be useful to a person committing or preparing for an act of terrorism, or possessing a document or record containing information of that kind;[23]
- encouragement of terrorism;[24]
- dissemination of terrorist publications;[25]
- providing or receiving instruction or training for terrorism;[26] and
- supporting a proscribed organisation.[27]

However, it is not currently an offence just to view the material.

[21] 'Manchester Bomber Salman Abedi learned how to make explosive device from YouTube videos', *Independent*, 24 June 2017.
[22] https://www.gov.uk/report-terrorism.
[23] Section 58 Terrorism Act 2000.
[24] Section 1 Terrorism Act 2006.
[25] Section 2 Terrorism Act 2006.
[26] Section 8 Terrorism Act 2006.
[27] Section 12 Terrorism Act 2000.

Scale

24. In the past, extremist material was predominantly distributed via leaflets, tape recordings or at meetings. This made it harder for individuals to access or disseminate extremist material without detection whilst the physical element also limited the scale of this activity.

25. Today, the internet allows terrorist and extremist groups to create, post, copy and distribute extremist material, which can be made accessible to over a billion people in a matter of seconds. Crucially, the speed at which material can be created and distributed, and the interactive nature of certain web services and social media platforms, means that the authors are able to interact with their audiences, and discuss current events or recent attacks, for example, in a manner that was not possible previously.

26. Consequently, the problem is vast. According to research conducted in 2013,[28] searching the internet for "*how to make a bomb*" returned almost 2 million results, and a search for "*beheading video*" returned over 250,000 results. Given the growth in the internet, these numbers will have increased considerably since that research was conducted.

27. In its 2014 Report into the murder of Fusilier Lee Rigby,[29] the Committee noted the threat posed by Al Qaida's English-language magazine *Inspire*:

- "*An internal MI5 assessment of* Inspire *in 2012 said: '*Inspire *seeks to promote home-grown 'lone actor' attacks, providing the ideological backing and practical instruction for users to commit attacks'.*"
- In evidence to the ISC a year later, the Agencies assessed: "*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.*"[30]

However, CTP explained that the problems associated with extremist material go much further than *Inspire* magazine:

> 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 twenty most commonly found files within this database.*[31]

28. During this Inquiry, MI5 updated the Committee on the changes in online extremist material:

> *since the Committee last looked at this territory in connection with a terrorist attack … five years has gone by and it has changed massively; when we examined* [intelligence relating to the murder of Fusilier Lee Rigby] *we were of course thinking about access to specific online publications, and it was* Inspire *magazine and so on, and compared to where things are now,*

[28] RAND Europe, *Radicalisation in the digital era*, 2013.
[29] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.
[30] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.
[31] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.

> *it was a relatively narrow space. The volume and pace of material and the extent to which social media in particular has just exploded … it has taken off everywhere and everybody's* [using] *it including the terrorists.*[32]

The Director General of MI5 also explained the ease with which it could be accessed:

> *the smartphone in everybody's pocket … through which we live most of our lives … also connects extremists straight with … appalling torture videos, beheadings and live video from battlefields, just at the touch of a button.*[33]

Impact

29. MI5 noted that since its establishment Daesh has expanded the concept of producing extremist material – which, in turn, has had an unprecedented radicalising effect on thousands of British citizens:

> *Daesh went some considerable way further than its Al Qaida predecessors in producing high-quality appealing material to affect thousands of predominantly young people in this country, and others.*[34]

CTP explained to the Committee that this had had a wide-ranging impact:

> *in almost every investigation and in every prosecution, this material exists in the hands of an SOI or they have been streaming it or they have been browsing it.*[35]

30. This is supported by the findings of a study conducted by the MI5 Behavioural Science Unit into the backgrounds and circumstances of *** Islamist extremist attack planners between 2012 and 2017 (those in the *** disrupted plots and the *** successful attacks). The study concluded that "*Almost all attack planners downloaded, shared or consumed radical and extremist media of some kind*".[36]

Previous examination and recommendations

31. During the Committee's investigation into the murder of Fusilier Lee Rigby, it found that one of the attackers (Michael ADEBOWALE) had engaged in significant extremist activities online. The Committee explored how the Agencies ***:

> *is aimed at* ***.[37]

***.

[32] Oral evidence – MI5, 8 March 2018.
[33] Oral evidence – MI5, 8 March 2018.
[34] Oral evidence – MI5, 8 March 2018.
[35] Oral evidence – MI5, 8 March 2018.
[36] Written evidence – MI5, 5 April 2018.
[37] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.

32. When questioned as to why more was not being done to investigate those viewing extremist material, MI5 had explained that merely viewing material did not in itself necessarily justify intrusive action. ***:

> ***. *That is not enough.*[38]

33. The Committee disagreed with this position, concluding in its 2014 Report:

> *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.*[39]

In response, the Government said it shared the Committee's view that engagement with extremist media should be taken seriously, but it considered existing arrangements to be sufficient.

34. Yet access to extremist material online is reported to have been a key factor in the Manchester Arena attack which killed 22 people. ***[40], ***.[41]

The current position

35. Giving evidence to this Inquiry in 2018 – four years after the Committee last considered the issue – both MI5 and CTP told us that it was still difficult to target those engaging with extremist material online. CTP explained that:

> *it is* [very difficult] *for law enforcement … we can arrest and prosecute* [but] *the sentences are not long enough.*[42]

Both organisations noted the importance of the Counter-Terrorism and Border Security Bill, which would update and strengthen the ability of law enforcement to respond to offences relating to extremist media.

36. CTP also raised the issue of material that is entirely lawful but which can have a radicalising effect on certain individuals. In the case of the Finsbury Park attack, the perpetrator Darren OSBORNE was heavily influenced by the BBC drama-documentary *Three Girls*, which focused on the grooming and sexual abuse of young girls in Rochdale by British-Pakistani Muslim men. The Deputy Assistant Commissioner noted:

> *It is what happens in the minds of malleable people … there is a wider society debate about some of the material out there and the effect that that … is having on people who want to commit these acts.*[43]

---

[38] Oral evidence – MI5, 12 December 2013.
[39] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.
[40] ***
[41] 'Manchester Bomber Salman Abedi learned how to make explosive device from YouTube videos', *Independent*, 24 June 2017.
[42] Oral evidence – CTP, 8 March 2018.
[43] Oral evidence – CTP, 8 March 2018.

37. Nevertheless, MI5 emphasised to the Committee the opportunities that extremist material online affords the intelligence community. They explained that they ***.[44]

38. MI5 informed the Committee that there have been a number of intelligence successes:

> *in the *** MI5 has opened over *** into intelligence from *** and a number of priority investigations have been derived or benefitted from this product.*[45]

They cited as an example the case of ***, who in *** was convicted of preparing for terrorist acts. *** first came to the intelligence community's attention through ***. He was arrested *** before he intended to carry out an attack ***. In *** he was convicted of terrorism offences.[46,47]

Removing online material: law enforcement

39. Given the difficulties in prosecuting individuals for viewing or disseminating extremist material, there has been a greater focus by law enforcement and the Agencies on identifying offensive content and referring it to the Communications Service Providers (CSPs) for removal.

40. In 2010, CTP established a national Counter-Terrorism Internet Referral Unit (CTIRU) to help tackle this issue. The CTIRU uses open source techniques to search the internet for extremist material which may radicalise or inspire terrorists. In addition to its own searches, the CTIRU also receives reports from members of the public: currently a significant proportion *** of the current activity on its case management system originates from public referrals. After a report of extremist material has been received, the CTIRU will determine whether it breaches terrorism legislation and, if so, work with industry to secure its removal.[48] Neil Basu, Assistant Commissioner, Specialist Operations, Metropolitan Police Service, informed the Committee during the course of this Inquiry that the CTIRU has successfully secured 300,000 'takedowns' in the nine years since it was established.[49]

41. However, the vast quantity of material online, and the ease with which material can be uploaded, versus the difficulty and time taken to remove it, means that the authorities will always be 'playing catch up' in seeking to address this problem in this way. ***, the Deputy Director General explained to the Committee that:

> ***.[50]

42. Neil Basu told the Committee that one of the aims was to engage international law enforcement partners to develop a similar capability to the CTIRU, to provide greater resource globally on this issue:

> *We are trying to franchise the brand … Europol have already taken that model and they have their own … we want that equivalent in all of our partners across the globe, starting with our major European partners.*[51]

---

[44] Written evidence – MI5, 5 April 2018.
[45] Written evidence – MI5, 5 April 2018.
[46] ***
[47] Oral evidence – MI5, 8 April 2018.
[48] Written evidence – CTP, 17 April 2018.
[49] Oral evidence – CTP, 8 March 2018.
[50] Oral evidence – MI5, 8 March 2018.
[51] Oral evidence – MI5, 8 March 2018.

Removing online material: internet companies

43. Given the volume of material, MI5 and CTP cannot tackle the problem alone – the key must therefore lie with the internet companies themselves: persuading the CSPs to take the lead in the identification and removal of material from their platforms. CTP highlighted the difference in speed at which CSPs can remove material – comparing their 300,000 pieces of extremist material in nine years to Twitter's ability to achieve the same amount in just six months. Furthermore, if the CSPs take responsibility for identification and removal, this would enable the CTIRU to:

> *be concentrated on prosecution, on finding the stuff we actually need to help investigations and prosecute … rather than spending all of our time effectively being an editor for someone else's publishing house.*[52]

44. In its Inquiry into the murder of Fusilier Lee Rigby, the Committee heard from technology companies such as Google, Facebook and Apple, among others, that they do not routinely monitor the content on their systems and they therefore cannot block all extremist material automatically. The companies insist that they are largely reliant on user-generated reports – from private citizens, organisations and law enforcement authorities – to trigger removal of illegal or offensive content. The Committee noted:

> *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.*[53]

45. The Committee was the first to identify the problems caused by the technology companies' actions. We concluded:

> *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.*[54]

The Government response to the Committee's recommendations welcomed the sentiment of the Committee's conclusion but offered nothing substantive in terms of a way forward:

> *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*

---

[52] Oral evidence – MI5, 8 March 2018.
[53] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.
[54] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.

> *this to encourage companies to work together to produce industry standards for the identification, removal and referral of terrorist activity.*[55]

46. This response was disappointing as it was clear to the Committee that this was a major issue, which required urgent action. However, we have observed that the Government has subsequently adopted the Committee's position and, recently, has increasingly sought to apply pressure to the major internet and communications companies to do more to prevent their systems from becoming a safe haven for extremist content and terrorist communications.

47. The Prime Minister said at the recent World Economic Forum meeting in Davos in January 2018:

> *Technology companies still need to do more in stepping up to their responsibilities for dealing with harmful and illegal online activity. Companies simply cannot stand by while their platforms are used to facilitate child abuse, modern slavery or the spreading of terrorist and extremist content.*
>
> *We have made some progress … in reducing the time it takes to remove terrorist content online, and to increase significantly* [the companies'] *efforts to stop it being uploaded in the first place.*
>
> *But we need to go further, so that ultimately this content is removed automatically.*[56]

In response, Google, YouTube and Facebook said they will hire more moderators to review material that has been flagged by users as inappropriate. They are also developing algorithms to detect harmful content automatically.

48. MI5 explained to the Committee that there has been a positive shift in engagement levels as a result:

> *companies are no longer overtly denying all responsibility for material they carry. They were doing that five years ago.*
>
> *I think to be balanced and fair to these companies, they are substantially shifted from where they were a few years ago on the particular thing of removing extremist content.*

However, MI5 conceded that there was still some way to go:

> [They are] *not yet where any one of us would wish them to be* ***.[57]

CTP supported this, explaining that whilst an automated system is positive in terms of removing extremist material, ***:

> *the automation helps,* ***.[58]

---

[55] *Government Response to the ISC Report on the intelligence relating to the murder of Fusilier Lee Rigby*, Cm 9012.
[56] www.weforum.org/agenda/2018/01/theresa-may-davos-address.
[57] Oral evidence – MI5, 8 March 2018.
[58] Oral evidence – CTP, 8 March 2018.

49. It is worth noting that many of the companies remain highly sensitive about the extent to which they are seen to co-operate with the authorities, following Edward Snowden's allegations about the intrusive capabilities of the Agencies. They are very conscious of the importance of privacy to their customers, which can trump other considerations. ***:

> ***
>
> ***
>
> ***.[59]

50. However, it does appear that the recent more positive stance is limited ***. OSCT explained that, whilst there had been some progress, a number of CSPs still refused to take down extremist material online despite requests from Government to do so. One example is *** which hosts multiple videos *** featuring violent and disturbing images. Despite multiple requests from the UK and European partners to remove the videos, *** has refused. The company has argued that the videos link back to an academic site, ***, which *** researches and analyses Islamic terrorism. *** has argued that removing the videos would compromise the quality of analysis that the site owner provides.[60]

51. *** has also refused to take down the website of *** (a UK proscribed *** group). In this case, it argued that it uses the UN proscription list when determining takedowns and *** does not feature on the UN list. In both cases, after discussions with OSCT, *** 'de-linked' the site from Google search (meaning that it would not appear when key terms were searched for). In the case of *** the content remains accessible. *** content has been removed (OSCT believes by the group itself). OSCT told the Committee that it continues to engage with *** to look at ways of removing extremist material.[61]

Removing online material: other levers for action

52. It is disappointing that – despite a great deal of engagement – little tangible progress has been made in the four years since publication of the ISC's *Report on the intelligence relating to the murder of Fusilier Lee Rigby* (the 'Woolwich Report') and the scale of the challenge remains significant. The Committee has considered whether enough is being done, and what more creative solutions should be explored.

53. It is clear that consumer action can force the companies to change. For example, in March 2017, a social media backlash against companies whose adverts appeared alongside extremist videos on YouTube gained widespread coverage in the mainstream media. Those companies had little choice but temporarily to stop advertising on YouTube, causing Google to modify its systems to reassure its advertisers. More recently, Unilever has announced that it is considering withdrawing its business from companies that are not doing more to protect children, promote diversity or provide "*responsible digital infrastructure*".[62]

54. It appears that these actions are having some impact. The companies take a commercial view – if something harms their reputation and impacts on their bottom line then that is what will prompt them to change their behaviour.

---

[59] Oral evidence – ***, 8 March 2018.
[60] Written evidence – OSCT, 8 May 2018.
[61] Written evidence – OSCT, 8 May 2018.
[62] 'Unilever threatens to pull ads from Facebook and Google', BBC News, 12 February 2018.

55. Previous efforts to persuade the CSPs to take action have appealed to their sense of corporate and social responsibility, and have achieved relatively little. Action that affects their profits hits home harder than any sense of 'doing the right thing', and it is this that the Government should focus its efforts on. Encouraging companies who advertise on the CSPs' platforms to put pressure on the CSPs to remove extremist content – with the threat of pulling their adverts if they do not – will have more impact on the CSPs.

What action is now being taken to tackle the problem?

56. Following the London Bridge attack in June 2017, the Prime Minister announced a review of counter-terrorism powers. This fed into the publication of a new CONTEST Strategy, in June 2018, and the introduction of a Counter-Terrorism and Border Security Bill in the same month. Both seek to address the current problems around extremist material online.

CONTEST[63]

57. The new counter-terrorism strategy lists halting the spread of extremist material online as a priority:

> [We will] *focus our online activity on preventing the dissemination of terrorist material and building strong counter-terrorist narratives in order to ensure there are no safe places for terrorists online.*[64]

58. With that said, there is no new approach suggested. Three current pieces of work were highlighted:

- carrying out a "*Ministerially-led global campaign*"[65] (which will form part of the overseas counter-terrorism approach), including military disruption of terrorist media operations overseas;[66]
- working with CSPs through the Global Internet Forum to Counter Terrorism[67] to press companies to develop and deploy technology that will automatically identify and remove terrorist content online; and
- using the Research, Information and Communications Unit to bring together civil society partners and industry experts to provide civil society partners with digital and communications support to allow them to deliver their own campaigns, both in communities and online (including creative advice, production capabilities, website building, media training and public relations support).[68]

---

[63] CONTEST is the Government's counter-terrorism strategy, first produced in 2003. The strategy consists of four strands: Pursue, Prevent, Protect and Prepare.
[64] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[65] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[66] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[67] The Forum was established in the wake of the Westminster attack following a roundtable (convened by the then Home Secretary) with major industry players including Facebook, Twitter, Google and Microsoft. The aim of the group is to develop technological solutions to help prevent terrorists' use of internet platforms.
[68] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.

Counter-Terrorism and Border Security Bill

59. The Bill includes amendments to existing terrorism offences to tackle the evolving methods of sharing extremist content and online radicalisation, in particular. According to the Home Office, the Bill will:

- Amend the offence of collecting information likely to be useful to a terrorist (Section 58 of the Terrorism Act 2000) to cover the repeated viewing or streaming of material online.

- Update the offence of publishing an image displaying a flag, emblem or other such symbol of a proscribed organisation (Section 13 of the Terrorism Act 2000) so that the law expressly covers displays online.

- Amend the offences of encouragement of terrorism (Section 1 of the Terrorism Act 2006) and dissemination of terrorist publications (Section 2 of the Terrorism Act 2006) so that they apply in cases where the conduct is directed at a child or vulnerable adult who may not understand what they are being encouraged to do.

- Increase the maximum sentences to 15 years for certain preparatory terrorism offences, namely: collecting terrorist information (Section 58 of the Terrorism Act 2000); eliciting, communicating or publishing information that is likely to be useful to a terrorist about a member of the armed forces, police or intelligence services (Section 58A of the Terrorism Act 2000); encouragement of terrorism (Section 1 of the Terrorism Act 2006); and dissemination of terrorist publications (Section 2 of the Terrorism Act 2006).[69]

In addition, the Bill will also:

> *extend extra-territorial jurisdiction to the offences of displaying an article associated with a proscribed organisation … dissemination of terrorist publications … where the offence is committed for terrorist purposes; and extend the existing scope of extra-territorial jurisdiction for the encouragement of terrorism offence, so that individuals who commit these offences overseas can be prosecuted in the UK if appropriate.*[70]

The Home Office notes the importance of extra-territorial jurisdiction:

> *because those who perpetrate such conduct are increasingly likely to be located abroad using online channels to promote terrorist organisations and disseminate terrorist publications in order to radicalise individuals within the United Kingdom and elsewhere, and seeking to encourage the commission of acts of terrorism.*[71]

60. At the time of publication, the Bill has reached its Committee stage in the House of Lords.

---

[69] *Counter-Terrorism and Border Security Bill 2018 – Overarching Fact Sheet*, 6 June 2018.
[70] *Counter-Terrorism and Border Security Bill 2018 – Terrorism Offences Fact Sheet*, 6 June 2018.
[71] *Counter-Terrorism and Border Security Bill 2018 – Explanatory Notes*, 5 June 2018.

A. This Committee was the first to identify – in its Report into the murder of Fusilier Lee Rigby – the problem of Communications Service Providers (CSPs) failing to remove extremist material from their platforms. In 2014, we urged Government to engage with the CSPs to get them to take action. Progress has been slow but we welcome the steps now being made by CSPs to automate the removal of extremist material.

B. Systems that the CSPs do put in place must ensure that law enforcement agencies are notified of any material that may have a national security threat element. Failure to do so will prevent early detection of potential threats.

C. In return, Government should ensure that it takes a co-ordinated approach to the CSPs: rather than confronting them with competing messages, single points of contact will ensure consistency and simplify the relationship for the CSP.

D. We particularly note the impact that recent action from advertisers such as Unilever has had in encouraging the CSPs to take action. Where reputational levers have failed to produce action, financial levers could provide the solution. We commend these companies and would encourage other major companies to follow their lead.

E. Government should now seek to lobby the business community to take action, following the Unilever example. This is a matter on which we expect a full report from the Government on what action has been taken with the business community within the next six months.

F. The ISC recommended in its 2014 Report into the murder of Fusilier Lee Rigby that more should be done to prosecute those accessing extremist material online. We are disappointed to note that the last four years have seen no progress on this issue. The Government must ensure that the Counter-Terrorism and Border Security Bill, when passed, tackles those who view extremist material online, as well as those who disseminate it.

SECTION 5: EXTREMISM IN PRISONS

Several of the attackers had previously interacted in some way with the prison system prior to their attacks:[72]

- SALMAN Abedi, the Manchester Arena attacker, had been in contact with a known extremist prisoner.
- Khalid MASOOD, the Westminster attacker, had served several prison sentences for offences unrelated to extremism. He had converted to Islam while in prison.
- Darren OSBORNE, the Finsbury Park attacker, had spent time in prison for unrelated offences.

However, these interactions were not central to the issues surrounding any of these attacks.

Management and intelligence coverage of extremism in prisons

61. Countering extremism in prisons forms part of the Prevent strand of CONTEST,[73] which is managed by OSCT. Since 2007, the Prison Service has run Prevent programmes in prisons, part-funded by OSCT. The Prison Service also leads the Operational Partnership Team, a unit which administers prisons' intelligence coverage and provides an interface between the Prison Service and the Police Service.[74] Counter Terrorism Policing (CTP) operates the National Prisons Intelligence Coordination Centre, a multi-agency organisation which co-ordinates the response to the threat from extremist, terrorist and organised crime prisoners in the UK.

62. In August 2016, the Justice Secretary announced that (where the prison estate allowed) extremists would be removed from the general prison population and held within Separation Centres.[75] In addition, a new Directorate for Security, Order and Counter-Terrorism would be created in the Prison Service; prison governors would be instructed to remove extremist literature; extremism-awareness training for officers would be improved; and vetting of prison chaplains would be increased.

63. Provision of human intelligence within prisons primarily comes from prisoners ***. ***.[76]

64. In addition to using prisoners ***[77] ***.

[72] ***

[73] The Prevent strand of CONTEST aims to stop people from becoming terrorists or supporting terrorism.

[74] More specifically, MI5 and CTP describe the Operational Partnership Team as "*responsible for the administration and quality assurance of applications for the use of covert tactics within prison*" (written evidence, MI5 and CTP, 6 July 2018).

[75] The decision to place an individual in a Separation Centre is dependent on the need to mitigate the risk that they may pose to others.

[76] Oral evidence – CTP, 8 March 2018.

[77] ***

Prisoners as Subjects of Interest

65. As at February 2018, there were *** prisoners under active investigation as Subjects of Interest (SOIs) by MI5 in relation to international counter-terrorism.[78] We were informed in August 2018 that there were approximately 300 identified extremists and 400 individuals deemed to be vulnerable to extremist messaging in prison.[79] OSCT describes the total of 700 as "*mostly Islamist (85%), with extreme right wing (13%) making up the majority of the remainder*".[80] It is clear, therefore, that ***.

Prevent in prisons

66. OSCT has informed us that a significant amount of money is being spent implementing the Prevent strand of CONTEST in the prison and probation system:

> *In the* [2017/18] *financial year, the Home Office dedicated 15% of the Prevent programme budget to fund work in prisons and probation. The Ministry of Justice complements this with additional funding of £2.3m. The indirect costs (e.g. Prison Officer resources) are borne by* [the Prison Service] *and are estimated to be* [in the] *region of £12m per annum.*[81]

67. OSCT explained how it is monitoring what is being achieved with this funding:

> *There are a number of measures in place to evaluate the capability and effectiveness of counter terrorism work in prisons. Every prison in England and Wales is subject to a six monthly* [Counter-Terrorism] *Capability Assessment …* [which] *assesses an establishment's performance in terms of its success in:*
>
> – *Identifying and understanding extremist risk – including staff extremism awareness, intelligence management and analysis, communications monitoring.*
>
> – *Prisoner management, support and intervention – including management arrangements for prisoners with extremism related risks, use of control measures and rehabilitative interventions.*
>
> *In addition, all counter terrorism assessment tools and rehabilitative programmes are regularly assessed and reviewed to evaluate impact.*[82]

68. The Committee questioned whether some extremist prisoners may be tactically engaging with de-radicalisation programmes such as Prevent, in order to dupe the authorities into believing that the risk they pose has decreased. The Joint Terrorism Analysis Centre (JTAC) assesses:

> ***
>
> ***.[83]

---

[78] ***
[79] Written evidence – OSCT, 17 August 2018.
[80] Written evidence – OSCT, 9 May 2018.
[81] Written evidence – OSCT, 9 May 2018.
[82] Written evidence – OSCT, 9 May 2018.
[83] ***

Monitoring those in contact with extremist prisoners

69. Category A prisoners[84] are subject to the Approved Visitor Scheme, whereby would-be visitors are subject to a degree of security checking (which in the case of extremist prisoners would involve ***) before being permitted to make a visit. Not all extremist prisoners are designated Category A: indeed, only *** of the prisoners under active MI5 investigation in 2016 were Category A.[85] (This is perhaps unsurprising, as the categorisation process primarily examines the likelihood of a prisoner attempting to escape and the immediate danger he would pose on doing so.) The monitoring of the visitors of prisoners at Categories B, C and D is much less systematic.

***

- ***.

70. ***

SALMAN Abedi

- The Manchester Arena bomber, SALMAN Abedi, visited prisoner *** on more than one occasion ***. *** SALMAN visited him ***.
- *** was a Category A prisoner when SALMAN first visited him ***. ***.

71. When SALMAN visited *** any visitors would have been subject to the Approved Visitor Scheme (since *** was a Category A prisoner). By ***. ***. However, it appears that no follow-up action was taken at the time in relation to SALMAN: the Internal Reviews state that ***. CTP explained:

> [SALMAN's] *association with *** was known from the previous visit *** and there was no specific intelligence suggesting that *** of concern. Therefore no further specific action was taken regarding the visit under the* [Intelligence Handling Model] *process and ***.*[86]

72. We found this explanation, and the lack of action, unsatisfactory: SALMAN was ***, but they did not have a legitimate *** link. As such, there was a clear risk that these were meetings between two extremists. MI5 admitted:

> *we wouldn't see* [SALMAN] *and *** as … legitimately connected ***. They were extremist associates … It is reasonable to suppose … that the nature of that visit was a sort of junior want-to-be extremist, in the shape of* [SALMAN]*, visiting someone to whom he looked up.*[87]

---

[84] Every adult male prisoner in England and Wales is designated as Category A, B, C or D, based on an assessment of the risk of his attempting to escape and the threat that he would pose to the public if he did so successfully; Category A is the highest. An analogous system of categorisation exists for adult female prisoners, and for adult prisoners in Scotland and Northern Ireland.
[85] ***
[86] Written evidence – CTP, 17 April 2018.
[87] Oral evidence – MI5, 8 March 2018.

73. CTP similarly recognised failings:

> *I think we can accept … that we were mea culpa about the issue of *** himself, who was seen as a key radicaliser. So he would have been somebody we should have probably been *** … we are unclear whether or not we advised the Prison Service of the risk he posed. At the time* [SALMAN] *was visiting, two things: *** was not a Category A prisoner and therefore* [the] *Approved Visitor List didn't apply to him and therefore there is less examination of who is visiting him, and I think that this* [is] *an issue about whether he was in the right categorisation or whether we were doing enough to monitor him on his conviction ...*
>
> *I think what we have absolutely accepted is that we did not alert the prison authorities sufficiently to the … radicalising risk that *** posed.*[88]

Improvements being considered by Government

74. The Internal Reviews recommended "*continuing discussions on how the Approved Visitor Scheme can be used more effectively*".[89] They do not, however, include any specific recommendations regarding visitors to extremist prisoners ***.

75. OSCT has, however, subsequently informed us that the Joint Extremism Unit and HM Prisons and Probation Service (HMPPS) are now considering extending the Approved Visitor Scheme ***:

> *The Joint Extremism Unit* [an OSCT–Prison Service team] *is currently exploring the feasibility of extending the Approved Visitor Scheme to ***.*[90]

76. Nevertheless, we note that of the 300 identified extremists currently in prison, only around 200 are Terrorism Act or Terrorism Act-related offenders. Therefore some visitors to *** prisoners will still be subject to no routine scrutiny.[91]

G. We support the intention expressed in the Internal Reviews to improve the Approved Visitor Scheme in relation to Category A prisoners – although clearly this is dependent on the detail of any measures to be implemented. We expect this detail to be provided by the Government within the next 12 months.

H. The monitoring of visitors to extremist prisoners below Category A is haphazard. This is concerning: it allows known extremist prisoners to potentially maintain links with those vulnerable to extremism. The Government should consider expanding the Approved Visitor Scheme to include all extremist prisoners.

---

[88] Oral evidence – CTP, 8 March 2018.
[89] MI5 and CTP, *Operational Improvement Review*, October 2017.
[90] Written evidence – OSCT, 9 May 2018.
[91] We note, however, that visits to such prisoners may nonetheless face some scrutiny on a case-by-case basis.

Conversion and radicalisation in prison

77. The Westminster attacker Khalid MASOOD converted to Islam while in prison in 2000 and 2001. Religious conversions in prison are not uncommon: prisoners may be motivated to convert in order to be included in a mutually supportive community within the penal environment. Anecdotally, it has also been suggested that prisoners may be keen on converting to religions that have dietary laws – such as Islam – as (whether correctly or not) special diets are viewed as offering higher-quality food than general prison catering. As such, an individual's conversion to Islam in prison should not automatically be taken as a 'flag'.

78. It does not appear that MASOOD was radicalised while in prison. There are differing views as to the link between conversion in prison and radicalisation:

> *While there is a significant body of reporting regarding conversion to Islam* [by prisoners]*, there is not necessarily always a link to radicalisation. Conversion* [to Islam by prisoners] *has often been a precursor to radicalising vulnerable individuals, whose behaviours within prison subsequently change as a result of these associations. Just as often, conversion is used as a means to coerce and exert authority on other prisoners. This remains an area of contention, as some individuals are known to completely relinquish their newly acquired faith upon release.*[92]

79. Nonetheless, it is noteworthy that converts to Islam are around four times more likely to be convicted of an Islamist-related offence than the general British Muslim population. In addition, of those converts to Islam who were convicted of Islamist-related terrorist offences between 1998 and 2015, 12% were converted in prison. Given the relatively small size of the UK's prison population, this is a high percentage, although we note it may merely reflect the propensity of those convicted of terrorist offences to have previously served prison sentences for non-terrorist-related convictions, and the numbers involved are perhaps too small for reliable conclusions to be drawn. CTP noted:

> *As a general point, it is certainly the case that we believe, and the data would tend to suggest, that people who have converted are more vulnerable to radicalisation and potentially even – I don't think there is a scientific way of saying this – but potentially not just being radicalised but becoming violent … But that is a … more general point. What I don't know is whether conversion in prison is specifically more likely.*[93]

80. There are currently around 300 identified extremist prisoners, of whom around 200 are imprisoned for offences under the Terrorism Act.[94] Of the remaining 100, some will have been radicalised by other prisoners whilst in prison. OSCT stated:

> *There is no evidence of large-scale radicalisation in prisons. However, radicalisation is a complex phenomenon and the risks are considerable in an environment that brings together significant numbers of terrorists and vulnerable people.*[95]

---

[92] ***
[93] Oral evidence – CTP, 8 March 2018.
[94] Oral evidence – CTP, 8 March 2018.
[95] Written evidence – OSCT, 9 May 2018.

81. It does appear that people who have spent time in prison are disproportionately vulnerable to radicalisation.[96] Reasons for this may include falling under the influence of an already-radicalised fellow prisoner whilst in prison, or simply that the vulnerabilities that lead an individual to general criminal behaviour can also lead that person to extremism.

82. JTAC noted this issue in 2016 in relation to Al Muhajiroun:

> ***.[97]

83. OSCT informed the Committee that, in recognition of the concern that converts to Islam could be more vulnerable to extremist rhetoric, Muslim prison chaplains provide specific support to those prisoners converting:

> *Those offenders who choose to convert to Islam in prison are supported by Muslim Chaplains, who provide guidance, challenge inappropriate behaviour and support those who are displaying potential vulnerabilities to extremism.*[98]

84. In an attempt to reduce the risk of radicalisation in prison, the first two new Separation Centres were created in HMP Frankland in 2017 and HMP Full Sutton in 2018 to separate extremist prisoners from the general prison population. They are intended "*for those offenders that pose the most significant risk of radicalisation of other prisoners*" in order to "*help safeguard the mainstream prison population*".[99]

85. We note that there could also be advantages in separating extremist prisoners from those who may have access to firearms. JTAC has expressed concerns regarding the interaction between extremist and non-extremist prisoners in relation to access to firearms:

> *In October 2016, *** prisons house both* [terrorism-related] *prisoners and criminals with firearms markers: the scale of the latter group has made routine separation difficult and these links are not routinely considered in decisions on ***.*
>
> *There is limited ***.*[100]

86. Conversely, CTP has noted the challenges that bringing terrorist prisoners together creates, and the risk that concentrating extremist prisoners in Separation Centres might lead to reinforcement of extremist views amongst prisoners:

> [Regarding] *the Separation Centres that are being trialled … you might want to have a debate about the pros and cons of Separation Centres but … bringing radicalised terrorists together, is that a good or a bad thing? It is never a good thing. All criminals who are inside have an ability to plot, so therefore you are creating an academy.*[101]

---

[96] David Anderson, *Attacks in London and Manchester March–June 2017: Independent Assessment of MI5 and CTP Internal Reviews*, December 2017.
[97] ***
[98] Written evidence – OSCT, 9 May 2018.
[99] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[100] ***
[101] Oral evidence – CTP, 8 March 2018.

87. It is worth noting that of those who began their radicalisation whilst in prison, very few are thought to have remained committed upon their release.[102] OSCT warned that the direct risk of violence posed by former terrorist prisoners on release should be kept in proportion:

> *Re-offending rates for terrorists are relatively low. Only 9% of terrorist prisoners released since 2012 have so far been re-convicted for any type of offending. By comparison, the overall re-offending rate for adults released from custody is almost 50%. Of the 183 terrorists released since 2012, only 5 have been convicted of further* [Terrorism Act] *offences (including three for the same plot).*[103]

I. It would be wholly inappropriate for prisoners who convert to Islam to be subject to routine monitoring. Nonetheless, prison officers must be trained to identify instances where someone has converted following association with extremists, to assess whether that conversion is therefore part of a positive journey or a negative one for an individual, and to be able to take action in the latter case.

J. While the Committee recognises the sound intention behind segregating extremist prisoners, we are concerned that the new Separation Centres may also provide a networking opportunity for extremists. We urge Government to keep this risk under review, and take what steps it can to minimise it. We expect to see the results of this review in 12 months' time.

Joint working

88. We have seen that there are a number of different bodies involved in managing, and gathering intelligence on, extremist prisoners – including the National Prisons Intelligence Coordination Centre (within CTP), the Operational Partnership Team (a multi-agency team in the Prison Service) and a dedicated team within MI5. In addition, the role of OSCT – already involved via its Prevent work – increased in April 2017 with its role (together with the Prison Service) in the new Joint Extremism Unit, described as "*the strategic centre for all counter terrorism work in prison and probation and* [having] *oversight of delivery across the end-to-end offender management process*".[104] Having so many different bodies involved poses risks: not only that there may be duplication of work and inefficiency, but also that the different bodies – whether due to cultural or practical obstacles – may fail to work together effectively. CTP believes that there has been significant progress:

> *I do believe the last year … maybe two years has resulted in a real step change in our joint work with prisons.*
>
> *… we haven't always been in a great place around co-ordination around our activity within prisons* [but] *it has improved dramatically. There has been a whole sea change in management capability and capacity within HMPPS that has made a substantial difference to the way we work together.*
>
> *So MoJ, Home Office, Prison Service, Probation Service on release and the Counter-Terrorism Police, alongside my National Crime Agency*

[102] ***
[103] Written evidence – OSCT, 9 May 2018.
[104] Written evidence – OSCT, 9 May 2018.

> *colleagues and organised crime colleagues, working together to properly assess the risks of individuals and pull in a proper multi-agency approach which includes prevention measures, is a real step forward and I think we are in a very positive place and this will only get stronger.*[105]

89. In this context, we note that the Internal Reviews suggest that a further team – the new National Tactical Management and Movement function – be established in relation to extremist prisoners. This additional team will sit within the Prison Service: we note that this is already a crowded space.

K. We are encouraged by witnesses' evidence that those organisations involved in managing, and gathering intelligence on, extremist prisoners are working well together. Nonetheless, we remain concerned that the number of organisations and teams working in this area makes it a crowded space. The Government should keep this matter under review and we expect a report on whether it is still working well in the next 12 months.

[105] Oral evidence – CTP, 8 March 2018.

SECTION 6: VEHICLE HIRE

Hired vehicles were used as weapons in the attacks at Westminster, London Bridge and Finsbury Park:

- In the Westminster attack, Khalid MASOOD hired his vehicle on 8 March 2017, and collected the vehicle in Birmingham on 16 March (six days before he carried out the attack on 22 March).
- The leader of the London Bridge attack, Khuram BUTT, hired the van used on the day of the attack itself (3 June 2017).
- The Finsbury Park attacker, Darren OSBORNE, hired his vehicle in Cardiff on 17 June 2017, just over a day before the attack (which happened at approximately 00:30 on 19 June).

90. The use of vehicles in terrorist attacks has long been promoted by Al Qaida, Daesh and other terrorist groups. In 2010, Al Qaida called for vehicles to be used and guided followers to go for the most crowded locations in order to strike as many people as possible.

91. In May 2013, Michael ADEBOLAJO and Michael ADEBOWALE used their car to strike and disable Fusilier Lee Rigby, before leaving the vehicle to attack him with knives. By September 2014, Daesh was calling on its followers to attack citizens of America and Europe using a variety of low-sophistication methods, including vehicles. The first use of a vehicle against a group of pedestrians in Europe occurred in France in December 2014. There have since been a number of such attacks across Europe, as the Committee mentioned in its recent Annual Report:

- 14 July 2016: a 19-tonne lorry was driven into crowds celebrating Bastille Day in Nice, resulting in the deaths of 86 people.
- 19 December 2016: a truck was driven into a Berlin Christmas market, killing 12 people.
- 7 April 2017: an attacker drove a lorry into pedestrians in Stockholm, killing five people.
- 17 August 2017: a van was driven into pedestrians in Barcelona, killing 14 people. A further person was stabbed to death.

MI5 noted that these vehicle attacks demonstrated the efficacy of the methodology and "*raised its profile amongst Islamist extremists in the UK*".[106]

[106] Written evidence – MI5, 5 April 2018.

MI5 and CTP current accesses

92. MI5 and CTP have access to *** information. *** are predominantly used by MI5 and CTP to ***:

> ***.[107]

Checks

93. When individuals hire or buy vehicles, their licence details may be checked with the Driver and Vehicle Licensing Agency (DVLA) to ensure that the individual is entitled to drive the vehicle in question.[108] This check may result in the vehicle company being warned, for example, of a driving ban – enabling it then to block the transaction and refuse to hire or sell the vehicle.

94. Currently, the DVLA system operates what are called ***.

95. In theory, these ***.

Operation AGAPANTHUS

96. The Metropolitan Police has, since November 2015, been running a pilot (Operation AGAPANTHUS) with vehicle hire firms.[109] While it does provide a route for these vehicle hire companies to report any concerns about suspicious transactions to the police, in practice the system is primarily used by the police as an investigative tool in serious crime enquiries, enabling them to obtain information from the relevant company on a case-by-case basis.[110]

Post-attack changes and improvements

97. The Internal Reviews note the use of hired vehicles in the attacks and raise a number of possibilities around greater use of ***, more use of *** and an expansion of Operation AGAPANTHUS; however, these are still ideas as opposed to concrete proposals.

Greater use of data

98. Given that MI5 and CTP already have access to ***, we questioned whether the *** could be used to *** hire – perhaps by the provision of real-time access to the ***. MI5 and CTP recognised that there were benefits to be gained and noted the possibilities offered by ***:

> *For example, ***, however this would require significant investment in technology, and timely and effective processes* ***.[111]

---

[107] Oral evidence – MI5, 8 March 2018.
[108] DVLA checks are not undertaken in the case of all vehicle hires. This is one of the key challenges in this area.
[109] ***
[110] Written evidence – MI5 and CTP, 7 June 2018.
[111] MI5 and CTP, *Operational Improvement Review*, October 2017.

99. CTP noted that real-time access to the *** was not currently possible for technical reasons, but this is something on which the Home Office and Department for Transport are considering alternatives.

Increased checks

100. A further possibility appeared to be offered by the ability to place *** against individuals on the *** and we questioned whether this might be ***.

101. However, both CTP and MI5 noted that there were a number of difficulties involved ***. The primary concern is that it might alert a Subject of Interest (SOI) to the fact that they were under investigation. For example, ***:

> *Where we are ***, the last thing we would want would be for the *** …*
>
> *… there is a real sort of careful decision about whether *** is used or not and that is part of the awareness piece. Then you have to encourage people … ***, and I think that is a problem …*[112]

102. The Internal Reviews recognise this problem and state that the Government is exploring the possibility of investment in future systems to put in place a *** capability. However, that would still leave the problem of *** – as MI5 explained:

> ***.[113]

103. Finally, CTP noted that ***. CTP explained:

> *** *I think it was discussed as to whether that needed to be in the CT bill or not but it is going forward as part of a *** with rental companies.*[114]

L. Whilst there may be some merit in increasing *, the Committee is conscious of the limitations of this capability. We query whether resources may be better served in seeking alternative solutions.**

Obtaining information from vehicle hire companies

104. While Operation AGAPANTHUS is currently used by CTP to request information from vehicle hire companies, in theory it could be used as a mechanism for vehicle hire companies to report to the police. According to the Internal Reviews, the pilot has demonstrated that the system – *** – does work and can generate valuable intelligence.

105. The Internal Reviews note that there would be resourcing implications in expanding the scheme:

> ***.[115]

However, of more concern is how practical it would be to roll out the pilot ***.

---

[112] Oral evidence – MI5 and CTP, 8 March 2018.
[113] Oral evidence – MI5, 8 March 2018.
[114] Oral evidence – CTP, 8 March 2018.
[115] MI5 and CTP, *Operational Improvement Review*, October 2017.

106. These issues are informing work being led by the Department for Transport which, with the support of the Home Office, has responsibility for improving information provided by vehicle hire companies:

> *The Transport Secretary agreed in December of last year that we would ***, which we hope to launch this autumn, which will ask those who join the scheme to ***.*[116]

In theory, this could provide useful intelligence, but again it is *** and therefore its utility will inevitably be limited.[117]

M. Given the propensity for vehicles to be used as weapons, monitoring vehicle hire must be a significant element of counter-terrorism work. The Committee is encouraged that the Department for Transport and the Home Office are working on a new system to improve the information provided by vehicle hire companies. However, we are concerned that the * of the proposed scheme significantly reduces the likelihood of its success.**

Greater use of financial data

107. The Internal Reviews note that greater use of financial data may be effective in preventing the future use of vehicles as weapons. MI5 and CTP are currently in discussion with *** regarding the possibility of ***. Furthermore, they are exploring the utility of ***.[118] This will present a significant change in MI5's current approach to sharing information and risk with external partners – this is discussed in more detail in Section 15 (Data and information).

CONTEST and the Counter-Terrorism and Border Security Bill

108. Neither CONTEST nor the Counter-Terrorism and Border Security Bill address the issues around vehicle hire – an indication that this work is still very much at the developmental stage. Instead, both note the Government's commitment to improving protective security measures in order to reduce vulnerability to, or mitigate the potential impact of, attacks on or near roads. This will be discussed later in this Report in Section 14 (Protective security).

[116] Oral evidence – OSCT, 1 May 2018.
[117] At the time of printing this Report, the scheme had not yet been launched.
[118] MI5 and CTP, *Operational Improvement Review*, October 2017.

SECTION 7: CHEMICALS AND EXPLOSIVES

- The explosive used in the Manchester Arena bombing and the device used in the Parsons Green attack were both constructed using the homemade explosive TATP (triacetone triperoxide).
- The Manchester Arena bomber, SALMAN Abedi, is thought to have obtained some of the ingredients used to make the explosives ***.
- The Parsons Green attacker, Ahmed HASSAN, allegedly bought the key ingredients for the device from the online retailer Amazon.

109. There are two explosives used by terrorists which are *** to produce by following *** instructions available on the internet:

(i) PETN (pentaerythritol tetranitrate) is from the same chemical family as nitroglycerin and, in addition to being a powerful explosive in its own right, is a key ingredient in Semtex plastic explosive. It has been used by terrorists for many years, including by Carlos the Jackal in the 1980s, the 'shoe bomber' Richard Reid in 2001, the 'underpants bomber' Umar Farouk Abdulmutallab in 2009, and the printer cartridge bomb plot in 2010. It is produced from the reaction between ***.

(ii) TATP (triacetone triperoxide) was used in the London bombings of 7/7, and in both the Manchester Arena and Parsons Green attacks. It is produced using *** – all of which are available in the UK.

110. MI5 told the Committee that TATP is *** from its component parts:

> ****. What is difficult with TATP is to manufacture it in such a way that you don't run a risk of a premature detonation. So a whole range of homemade explosives exist and obviously TATP happens to be the one most commonly attempted *** at present and … people, including the Manchester bomber and nearly the Parsons Green bomber, *** but it is often the case that people attempting to make TATP will* [blow themselves up].[119]

111. The Manchester Arena bombing showed that, once SALMAN Abedi had acquired the materials, the process of manufacturing TATP itself was ***:

- ***, online videos demonstrating how to build TATP improvised explosive devices (IEDs).
- *** SALMAN acquired the materials for the device (***[120]). It is thought that the explosive was produced ***.
- Between mid-April and 18 May, HASHEM and SALMAN Abedi were taken to Libya by their parents and during this time the explosives ***.

[119] Oral evidence – MI5, 8 March 2018.
[120] ***

- After his return to Manchester ***, SALMAN purchased additional non-explosive components and manufactured the IED before detonating it at Manchester Arena on the evening of 22 May.

Access to the chemicals

112. If the manufacture of TATP is *** with the ingredients required (the 'precursors'), and how access to them is regulated. In the UK, the regulation of access to chemicals is determined by the type, concentration and volume. The Poisons Act 1972 regulates the sale of explosives precursors and poisons. Under the Act certain explosive precursors (including TATP ingredients over a certain concentration and/or volume) require members of the public to hold a valid Home Office licence in order to import, acquire, possess and use them.[121]

Table A: Explosives precursors regulated by the Poisons Act 1972

Substance	Concentration above which a licence is required
Hydrogen peroxide	12% weight by weight
Nitric acid	3% weight by weight
Nitromethane	30% weight by weight
Sodium chlorate	40% weight by weight
Sodium perchlorate	40% weight by weight
Potassium chlorate	40% weight by weight
Potassium perchlorate	40% weight by weight
Sulfuric acid	15% weight by weight

113. The Home Office is responsible for liaising with industry and retailers and for issuing licences. Licences can be applied for online and are granted by the Home Office after certain checks have been made (including criminal record and health checks). Since 2014, the Home Office has issued 345 licences and rejected 20 applications.[122]

114. In addition, businesses and licence holders are legally required to report any suspicious transactions, losses or thefts of any regulated explosives precursors. These include the eight chemicals listed in Table A, below the concentrations that require a licence, and a further ten, as listed below in Table B.

[121] Written evidence – OSCT, 8 May 2018.
[122] Oral evidence – OSCT, 1 May 2018.

Table B: Additional explosives precursors subject to reporting requirements

Substance	Concentration at which suspicious activity reporting applies
Hexamine	Any
Acetone	Any
Potassium nitrate	Any
Sodium nitrate	Any
Calcium nitrate	Any
Calcium ammonium nitrate	Any
Ammonium nitrate	16% by weight of nitrogen
Aluminium powders	With a particle size of less than 200 μm
Magnesium powders	With a particle size of less than 200μm, as a substance or in mixtures containing 70% or more, by weight of aluminium/magnesium
Magnesium nitrate hexahydrate	Any

115. This reporting system relies on the vendor's identification of purchases as being suspicious (i.e. if purchased in unusual quantities). Retailers are required to report suspicious purchases via a Suspicious Activity Report (SAR), which they can submit via an online Home Office form that is routed to specialist assessors within CTP. Alternatively, they can report their suspicions via the anti-terror or Crimestoppers hotlines, where they will be assessed alongside other incoming intelligence and new 'leads' (as described in Section 1, Introduction).

116. In 2017, the Home Office received *** SARs. The vast majority of these cases related to non-terrorist criminal use. They did, however, lead to a small number of explosives-related arrests.[123] None of these were clearly terrorism related; however, some did involve lone actors with undetermined motivations. In addition, one Terrorism Act arrest was made as a result of SAR reporting, which led to the conviction of Warren SNEDDEN for explosives, firearms, drugs and terrorism offences.[124]

Problems with the regulation system

117. CTP noted that until November 2017 (when it was redesigned as part of the post-attack review process) the design of the reporting system no longer reflected the current threat:

> *The sole SARs reporting regime was designed in the* [Provisional Irish Republican Army] *era for fertilizer bombs … it was low-volume/high-risk stuff. We are now at high-volume transaction, electronics, and the whole system is not set up for that.*[125]

[123] ***
[124] Written evidence – MI5 and CTP, 19 April 2018.
[125] Oral evidence – CTP, 8 March 2018.

118. One problem is that vendors are responsible for deciding when a transaction of 'middle-tier' chemicals (those in Table B above) is suspicious. This means that purchases of chemicals can go unreported − ***. CTP explained to the Committee that this is something extremists have taken advantage of:

> ***.[126]

MI5 agreed:

> *I think pretty much, by any view, you would think that the acquisition of chemicals in relation to *** … would be a suspicious transaction. ****
>
> ***, isn't* [the retailer] *breaching the … licence regulation but it is right at the upper end ***.*[127]

119. CTP noted that this may in part be due to a lack of understanding amongst retailers:

> *some retailers are just not aware of the duty to report anyway, they don't know what looks suspicious and what doesn't.*[128]

OSCT informed the Committee that guidance on detecting suspicious transactions is issued to retailers – ***. However, referring suspicious transactions is entirely at retailers' discretion. In addition, when retailers do report suspicious purchases they provide very limited details. These usually focus on what was purchased and at what time but do not include any identifying details.[129]

120. Finally, whilst improvements can be made to these systems, the dual-use nature of these ingredients means that they are used commercially in a wide variety of circumstances, making it extremely difficult to monitor all purchases. This raises questions as to whether the system is fit for purpose, and whether there should be additional restrictions for certain materials.

What is being done?

121. MI5 explained that following the Manchester Arena attack there was "*vigorous action led by the Home Office to re-energise that scheme for suspicious transaction reporting, and also work on collecting the data*".[130] OSCT told the Committee that:

> *we have moved over the last year into a … faster and better *** arrangement with … *** retailers. ***.*[131]

122. The Internal Reviews explain that the priority for MI5 and CTP is to improve the processes around the purchase of explosives precursors (and in particular where that relates, or might relate, to MI5 Subjects of Interest) and that the following work is under way:

- improving the system of suspicious activity reports to control access to, or notify sales of, material that could be used to commit acts of terrorism. (***);

---

[126] Oral evidence – CTP, 8 March 2018.
[127] Oral evidence – MI5, 8 March 2018.
[128] Oral evidence – CTP, 8 March 2018.
[129] MI5 and CTP, *Operational Improvement Review*, October 2017.
[130] Oral evidence – MI5, 8 March 2018.
[131] Oral evidence – OSCT, 1 May 2018.

- development of guidelines on the thresholds for SARs;
- ***;
- greater use of data to enable faster detection of suspicious transactions ***; and
- a Home Office-led review of the policy relating to the purchase of explosives precursors. This includes possible changes to licensing arrangements and expanding the list of precursor items that are subject to monitoring or reporting.[132]

123. In relation to the policy review, OSCT explained:

> *We have laid legislation in April of this year to restrict the acquisition and possession of ***, so* [in terms of] *the three that we really worry about – *** and *** – which are the components of making TATP, which were behind the two explosive attacks over the summer:*
>
> – *** *is already restricted at certain concentrations and, as I said, we look to people to report to us kind of on that.*
>
> – *We have taken action on ***, as I have mentioned.*
>
> – ***. [Working with retailers to 'design out the threat' by substituting products with safer alternatives that cannot be used in an attack.][133]

124. Nevertheless, it is clear that retailers are key to any overall improvement. CTP noted:

> *what has happened after 2017 is they have all got more interested, a bit like the CSPs, they are really trying to help ***.*[134]

Whilst this was positive, CTP explained that these changes came with their own difficulties in terms of resourcing:

> ***
>
> *As the reporting regime spins up there will be more pressure.*[135]

125. OSCT added a further note of caution:

> *a dedicated terrorist will, you know, work hard to get round our systems…* ***.[136]

CONTEST and the Counter-Terrorism and Border Security Bill

126. As discussed in Section 4 (Extremist material online), the Counter-Terrorism and Border Security Bill is seeking to extend extra-territorial jurisdiction for a number of offences. This will also apply to those "*making or possessing explosives under suspicious circumstances*" (Section 4 of the Explosive Substance Act 1883).[137]

---

[132] MI5 and CTP, *Operational Improvement Review*, October 2017.
[133] Oral evidence – OSCT, 1 May 2018.
[134] Oral evidence – CTP, 8 March 2018.
[135] Oral evidence – CTP, 8 March 2018.
[136] Oral evidence – OSCT, 1 May 2018.
[137] *Counter-Terrorism and Border Security Bill 2018 – Terrorism Offences Fact Sheet*, 6 June 2018.

127. The use of chemicals and explosives precursors is indirectly referenced in the Protect strand of the new CONTEST Strategy, which includes the following objective:

> *Detect and prevent terrorist access to and use of materials of concern, knowledge and information that could be used to conduct attacks.*[138]

The specific actions include:

- *A range of policy interventions to prevent access by terrorists to materials of concern including legislation to ensure the security of substances in their legitimate use or sale; chemical disposal schemes; voluntary codes for businesses to secure supply chains; and capabilities to detect suspicious transactions.*
- *Working with industry to prevent access by terrorists to design out the threat through developing commercially viable safer alternatives for legitimately used products containing materials of concern, improve processes to increase greater awareness and to control access to, or notify sales of, material that could be used to commit acts of terrorism.*
- *Work with retailers and law enforcement to ensure that legislation operates effectively and regularly review the substances that require a licence and the controls around them.*
- *Continue to enhance existing explosives detection capabilities, such as explosives detection dogs and screening technologies to enable earlier detection of terrorist activity. This will include using existing detection capabilities in a wider range of spaces for a broader range of purposes as well as exploring options for adding new detection capabilities.*[139]

N. The previous system for regulating and reporting purchases of the ingredients used to make explosives such as TATP (triacetone triperoxide) and PETN (pentaerythritol tetranitrate) was out of date in dealing with the threat at the time. The Manchester Arena bombing showed this to devastating effect. We therefore welcome the updates to the current system of regulating and reporting explosives precursor purchases.

O. The Committee notes that the proposed changes to the system will result in a considerable increase in the volume of data generated. We are concerned that there must be sufficient resources to deal with this increase in data. The Home Office must ensure that proper support is in place *: we expect to see an analysis of what is required within the next six months.**

P. We are pleased to hear that progress is being made to develop relationships between retailers and the counter-terrorism network: again, this is overdue.

---

[138] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[139] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.

Q. Whilst there are changes that can – and should – be made to the current arrangements around the regulation of chemicals used in explosives, it is not possible to prevent all purchases: at a certain point the benefits that can be gained from successive tightening of the system will become marginal.

SECTION 8: ***

***

128. ***

R. ***

S. ***

T. ***

SECTION 9: JOINT WORKING

Issues around MI5 information sharing and collaborative decision making can also be seen in relation to the attacks:

- The Internal Reviews note that there are significant gaps in the recording and storage of *** intelligence on police systems, ***:[140]
  - In the case of the ***, police have incomplete records of all ***.
  - ***.
- MI5 *** two of these reports have been located on police systems. This meant that the CTP Senior Investigating Officer, although aware of ***, was not able to *** – limiting their ability to consider it in the context of other intelligence.
- On two occasions (26 February – 6 April 2016 and 21 March – 5 May 2017), MI5 suspended the investigation of Khuram BUTT. CTP was not involved in either decision to suspend the operation.

129. MI5 and CTP both work on counter-terrorism. The broad roles of each are as follows:

- MI5 are responsible for gathering secret intelligence on terrorist activity, including via human sources (agents), eavesdropping devices, physical surveillance, interception of communications, communications data, bulk datasets and equipment interference. MI5 do not, however, have any power to arrest suspects or undertake a criminal investigation with a view to prosecution.

- CTP delivers specialist counter-terrorism services on behalf of the police.[141] CTP consists of national and headquarters capabilities, together with 11 regional Counter Terrorism Units (CTUs) and Counter Terrorism Intelligence Units (CTIUs). CTP collects intelligence on terrorism and wider national security threats through a range of covert means, including handling Covert Human Intelligence Sources (CHIS),[142] communication intercept and surveillance. CTP supports MI5 in the analysis and assessment of intelligence and leads on disruptive activity pursued through criminal investigation.[143] Given the symbiotic nature of their relationship, MI5 and CTP work very closely together on counter-terrorism. This joint working is enabled through aligned structures and investigative models. These include:

  (i) An Executive Liaison Group (ELG) – this is a formal decision-making body that sets the direction for priority operations. This includes defining the intelligence and evidence-gathering objectives, creating a strategy to manage community impact and handling any media communications. The ELG is convened when executive action is being considered and is chaired by the Senior National Coordinator (CTP). It is attended by a senior representative from MI5.

[140] CTP, *Manchester Post-Attack Review*, October 2017.
[141] Although countering terrorism is a core role of all police officers and staff.
[142] Otherwise known as 'agents'.
[143] This relates to CTP's work under the Pursue strand of CONTEST, although they do operate against all four strands.

(ii) A Joint Operational Team (JOT) – this is the formal decision-making body that turns the ELG's strategy into a tactical plan. This meeting is chaired by the MI5 Intelligence Manager and is attended by the CTP Senior Investigating Officer as well as various representatives from both MI5 and CTP. The JOT decides what actions are likely to achieve the ELG's objectives.

(iii) Informal discussions – supported by the *** of MI5 and police officers across the network of police CTUs and MI5 regional stations.

Previous concerns

130. Previous ISC Reports – including the Woolwich Report and the original 7/7 Report – have raised concerns as to how well MI5 and CTP work together. One of the problems identified during the 7/7 Inquiry was that MI5 made requests of Special Branch[144] rather than fully involving them in investigative decision making – for example, asking them to run checks on an individual of interest but not explaining the background behind the request.

131. During that Inquiry, in 2006, both CTP and MI5 told the Committee that their relationship and the way they work together had changed dramatically due to the regionalisation of MI5, and with the formation of regional police CTUs. The Committee's original 7/7 Report concluded:

> *More needs to be done to improve the way that the Security Service and Special Branches come together in a combined and coherent way to tackle the 'home-grown' threat. We welcome steps that are now being taken to achieve this although, given that the 'home-grown' threat had clearly already been recognised, we are concerned that more was not done sooner.*[145]

Eight years later, the same issue arose in the Woolwich Inquiry – the Committee again concluded:

> *The Committee considers that there is insufficient coordination between MI5 and Police investigations ... MI5 and the Police must improve both the process and the level of communication … when MI5 request information from the Police, the Police should ensure that all information held – whatever their assessment of it at the time – is shared with MI5.*[146]

132. The Government responses to both the original 7/7 Report and the Woolwich Report stated that MI5 and CTP were working well together and would continue to improve in this regard: they did not indicate that any specific changes would be made in response to the ISC's recommendations.

The 2017 terror attacks

133. However, last year's attacks revealed that – three years later – there were still problems around the sharing of MI5 information with CTP, and the involvement of CTP in MI5 decision

[144] The Metropolitan Police's Special Branch was at that time responsible for dealing with issues relating to national security. In 2006, it was merged with the Metropolitan Police Anti-Terrorist branch and renamed Counter-Terrorism Command.
[145] *Report into the London Terrorist Attacks on 7 July 2005*, Cm 6785.
[146] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.

making. For example, ***, CTP had limited records ***. ***, CTP stopped receiving any intelligence. In the case of ***; however, only two reports were received by CTP. This raises concerns that the previously identified problems around information sharing have still not been addressed. CTP responded:

> *when things are not shared, either when best practice would suggest they should be or the system yet does not allow for them to be shared, it is not dissimilar from what happens, for example, within my organisation, or within MI5. These are two very closely working machines with some kind of lingering barriers and, for me, the lingering barriers, if you like, are primarily around rather dull stuff like IT and estates, and our ambition there is to further improve our information technology so that we are more integrated, and further improve our co-location and of course that all depends on us recruiting more people …*
>
> *So you will see in these reports moments where information was not shared or not shared within an organisation, and some of those are entirely expected and understandable and legitimate. My sense is that we are on a really sort of strong path here.*[147]

134. MI5 supported this view, noting that there had been improvements:

> *Since the ISC recommended* [implementing changes] *following the* [Inquiry into the] *Lee Rigby murder, things have moved forward further in terms of how we work the intelligence handling modelling together jointly, in how we review ourselves jointly.*
>
> *where there were glitches in the operational systems and process, I think I agree with the Commissioner: they don't look to me anymore … frequent than just happens in normal life, even within my own organisation, where … it is just the nature of human-based systems that, occasionally, not everything is completely happening in the most perfect way, as it doesn't in any organisation.*[148]

MI5 were keen to emphasise the overall high level of joint working:

> *I think the standard of how we share stuff is a very high one … I don't know of any system anywhere else in the world that is as close and highly developed as the partnership we have got now, that the Committee, rightly, picked on as a theme in 2013 and it remains a theme for us … just because of its sheer importance and we want to be in a position of continuously improving that and I think, actually, several of the themes … reflected back to us through the Woolwich review work are in that category of being the things that just require persistent, continuous improvement, thematically, in order to keep getting better at counter-terrorism. Or, put another way, there isn't just a switch you throw and suddenly co-operation is done and no longer an issue. It is a continuous thing.*[149]

---

[147] Oral evidence – CTP, 15 March 2018.
[148] Oral evidence – MI5, 15 March 2018
[149] Oral evidence – MI5, 15 March 2018.

135. We note that the Internal Reviews commented on "*an imbalance in the relationship between MI5 and Police (perceived or otherwise)*".[150] However, the Commissioner disputed this, noting:

> *I would want to disabuse anybody from a view that there is either competition or malice or anything which can lead to material not being shared between the organisations in a deliberate way.*
>
> *… we firmly believe we should maintain our constitutional positions, our … USPs, and those of themselves do lead to slightly different operating cultures.*
>
> *However, we come together all the time to try to maintain the best of those cultures and not allow any differences in culture to get in the way, and in these particular instances ... the issues we are talking about are I believe about processes and systems primarily.*[151]

136. The Committee queried what official protocol existed to advise staff in both organisations of joint-working procedures and were told:

> *Joint working between MI5 and the police is governed by a number of protocols and supported through a range of learning and development interventions.*
>
> *While there is no one overarching document that governs joint working between MI5 and the Police, guidance is provided on key aspects of our partnership, for example both written guidance and training is provided on the Intelligence Handling Model. *** also provides an … overview for running joint investigations …*
>
> *Both Police and MI5 receive and provide training about working together. There is a course called "Working with MI5" that is run for all new counter-terrorism Senior Investigating Officers* [SIOs]*, which provides a three-day overview of working together, underpinned by table top exercises emphasising joint decision-making … On MI5's Foundation Investigative Training, investigators receive a full day of training about working with police, and are assessed throughout on their engagement with police partners. The relationship also forms a key part of Major Incident Training which is provided to the investigative cadre. Regional stations deliver training to offer an Insight into CT Operations for police officers at all levels.*
>
> *Police Dedicated Sourcing Units (DSUs) also receive training on working with MI5 – MI5 deliver the National Security Agent Handling Course (NSAHC) and the Police Ops Managers course, for those who manage or authorise national security CHIS operations.*
>
> *Both police and MI5 staff also receive on the job training. In regional stations, the *** of police and MI5 staff ensures that teams work closely on progressing investigative objectives.*[152]

---

[150] CTP, *Manchester Post-Attack Review*, October 2017.
[151] Oral evidence – CTP, 15 March 2018.
[152] Written evidence – MI5 and CTP, 7 June 2018.

U. The Committee has raised concerns about the need for improved joint working between MI5 and CTP for over ten years. Improvements have been made but we note that this is an area that requires continuous improvement.

V. Further issues that MI5 and the police might consider are: how to ensure comprehensive dissemination of information from MI5 to CTP; cultural change to support the new structures in place to facilitate closer working; and a renewed impetus to resolve the problems caused by incompatible IT systems.

What is being done about it?

137. The Internal Reviews suggest that improvement needs to focus on a number of identified issues, including the standardising of intelligence and investigative processes, promotion of a culture of challenge, and greater involvement of CTP in decision making on MI5-led investigations.

138. MI5 and CTP were both keen to stress that there was already a high level of input by CTP into decision making on high-priority cases:

> *when it comes to the decision-making, towards the top of the pyramid, so the cases where we know there is live risk of a serious sort, we have very, very structured formal decision-making processes, which, at that level, tend to be chaired by the police, actually, the ultimate guardians of public safety.*[153]

They did, however, note limitations on ***.[154] Both organisations noted that improvements had been made in this respect through the embedding of CTP in Thames House and through the formal involvement of CTP in the lead triage process (see Section 3, Intelligence and investigations, for further details). They also noted that *** of their CHIS handlers was planned, to help more effective joint handling of agents.

139. The organisations note that IT was the primary barrier to full joint working. MI5 explained:

> *if we are honest at the moment we have a spirit of partnership and a sort* [of] *professional esprit de corps that is up here and we have IT connectivity that is kind of* [down] *here.*
>
> *This is inherently difficult for a range of reasons. The police have to be connected to a lot of other bits of police IT but we are working through how can we better integrate our systems so that data shows more readily, rather than, as currently, slightly pushing some of it up hill.*[155]

MI5 and CTP explained that this issue will be addressed through a new programme to transform counter-terrorism work, known as the 'Counter-Terrorism Step Up'. One aspect of this brings together police colleagues with MI5, SIS and GCHQ counterparts to launch a series of initiatives to improve the exchange of data between organisations.

---

[153] Oral evidence – MI5, 15 March 2018.
[154] CTP, *Manchester Post-Attack Review*, October 2017.
[155] Oral evidence – MI5, 15 March 2018.

W. The Committee welcomes the number of initiatives focused on improving the flow of information between MI5 and CTP; however, it is important that this results in real, practical change. The Committee expects a report on how this is working and what tangible benefits have been seen in six months' time.

Leaks

140. In countering the terrorism threat, MI5 and CTP must join up not just with each other and with other UK organisations (as we explore further in Section 15, Data and information), they must share information with their liaison partners in other countries. Sharing such highly sensitive information depends on trust – as it does in any relationship – and intelligence leaks are extremely damaging. They impact on investigations, can irreconcilably damage intelligence-sharing relationships and erode public trust in institutions.

141. Following the Manchester Arena attack on 22 May 2017, there was extensive reporting in the US media of the identity of the suspected bomber, along with a number of crime scene photographs. This was strongly condemned by the UK and US authorities. The intelligence-sharing relationship was at risk: but, far more importantly, the leaks may have added to the distress already being suffered by the victims and families.

142. This was of considerable concern to Members of Parliament and a high-profile issue in the media at the time. US Secretary of State, Rex Tillerson, commented at a London press conference on 26 May:

> *We take full responsibility and we obviously regret that this happened. The President has been very strong in his condemnation, and has called for an immediate investigation and prosecution of those who are found to have been leaking any of this information to the public.*

143. The Home Office explained that in the immediate aftermath the then Home Secretary wrote to Department of Homeland Security Secretary John F. Kelly and Attorney General Jeff Sessions, setting out the seriousness of the UK Government's concerns. The US administration confirmed that it was taking the matter extremely seriously and conducting internal investigations into the matter.[156]

144. However, MI5 revealed that from a national security perspective there was at no point a pause in intelligence sharing with US counterparts. CTP explained that intelligence sharing was paused, but only temporarily. CTP also commented that very little had changed in terms of intelligence-sharing processes as a result of the incident. The Home Office stated:

> *The Home Office's Permanent Secretary, Philip Rutnam, met with Deputy Attorney General, Rod Rosenstein in October 2017* [to discuss the issue]. ***.[157]

At the time, the US Government condemned this leak of information and regretted its occurrence. More recently, the Deputy Attorney General has committed to tightening the

[156] Written evidence – Home Office, 9 May 2018.
[157] Written evidence – Home Office, 9 May 2018.

controls around the sharing of information in government. This is a welcome step. The Home Office did note, however, that:

> *it is also vitally important to national security and our efforts in tackling the threat of terrorism that there is a close relationship with regards to intelligence sharing between UK and US agencies. Maintaining that close relationship is a priority, and it would be damaging to the safety of the United Kingdom to overly restrict our current arrangements.*[158]

On 10 October 2018, the Office of the Inspector General, U.S. Department of Justice (DOJ), issued a statement, which noted that there were:

> *findings of misconduct by three FBI employees and one FBI task force officer for violating DOJ and FBI computer rules of behaviour and FBI policy by forwarding a United Kingdom Intelligence report regarding the Manchester Arena bombing.*[159]

X. The Committee considers that the Government failed to tackle the leaking of information about the Manchester Arena attack sufficiently robustly. Leaking our information – and potentially causing distress to the victims and families in so doing – will not be tolerated. The US administration recognised the seriousness of the situation and we welcome the thorough investigation they undertook.

[158] Written evidence – Home Office, 9 May 2018.
[159] Office of the Inspector General, U.S. Department of Justice, *Investigative Summary*, 10 October 2018.

SECTION 10: LOW-LEVEL, PERIPHERAL AND CLOSED SUBJECTS OF INTEREST

The question of how low-level, peripheral or Closed Subjects of Interest (SOIs) are managed by MI5 is relevant to three of the attacks:

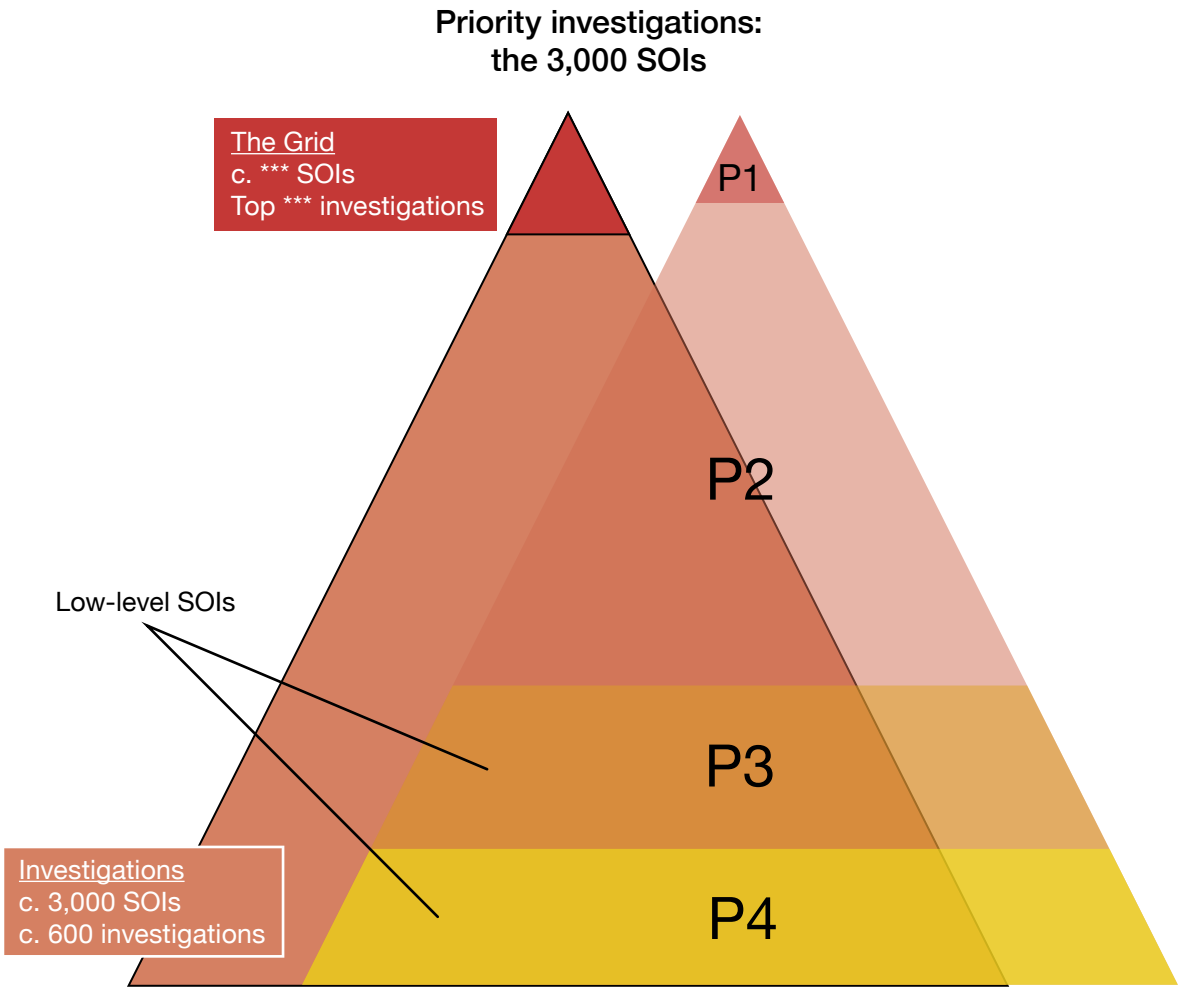
- Westminster: from 2004 onwards, Khalid MASOOD appeared on the periphery of several investigations, and he was directly investigated as a low-level SOI in 2010. He was closed as an SOI in his own right in 2012. He continued to appear on the periphery of a number of investigations between 2012 and 2016.
- Manchester Arena: SALMAN Abedi appeared on the periphery of an investigation between 2013 and 2014 and was briefly investigated in 2014 and 2015. From mid-2018 ***.
- London Bridge: of the three attackers, only Khuram BUTT had been investigated by MI5. From *** 2015 he had been the principal subject of Operation BEGONIA, which was later downgraded in priority and briefly suspended completely in both 2016 and 2017 due to competing resource pressures within MI5. At the time of the attack Operation BEGONIA was being considered for closure.[160]

What is a 'low-level SOI'?

145. Incoming intelligence and leads can – if they indicate sufficient national security risk – generate new MI5 investigations. These investigations are then categorised (from highest to lowest) as Priority 1A, Priority 1B, Priority 2H, Priority 2M, Priority 3 or Priority 4; these are abbreviated to P1 (encompassing P1A and P1B), P2 (encompassing P2H and P2M), P3 and P4. As at 27 April 2018, the split of MI5's investigations by priority was as follows: *** P1A ***; *** P1B investigations; *** P2H investigations; *** P2M investigations; *** P3 investigations; and *** P4 investigations.[161]

146. MI5 devote a great deal more attention to the top of this pyramid than the bottom: P3 or P4 investigations attract considerably fewer resources than are dedicated to higher-priority investigations, and the individuals within them are relatively speaking of much less interest than individuals undertaking attack planning or serious extremist activity. Therefore SOIs in P3 or P4 investigations can be thought of as 'low-level SOIs'.[162]

[160] We note that MI5 were giving consideration to investigative actions that were proportionate ahead of closure of the investigation as to how best to manage the risk that BUTT posed (including placing him into other investigations).
[161] Written evidence – MI5, 7 June 2018.
[162] We note that 'low-level SOI' is not a term used by MI5, but we have used it in this Report for ease of reference.



What is a 'peripheral SOI'?

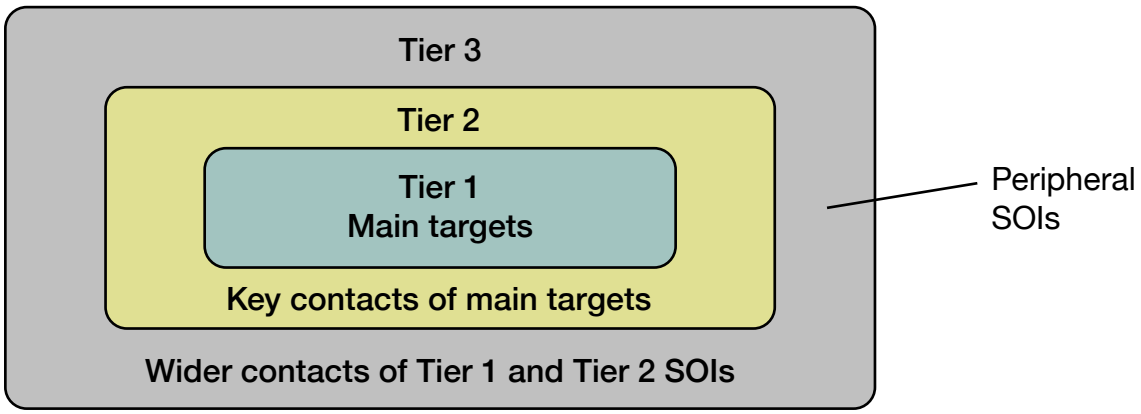
147. In addition to the priorities attached to particular investigations, every SOI within an investigation is prioritised according to three tiers:

- 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.

A Tier 3 SOI can be thought of as a 'peripheral SOI'.[163] As at 27 April 2018, there were *** Tier 1 SOIs; *** Tier 2 SOIs; *** Tier 3 SOIs; and *** undetermined SOIs.[164]

[163] We note that 'peripheral SOI' is not a term used by MI5, but we have used it in this Report for ease of reference. We include within this definition identifiers (e.g. mobile phone numbers, names and email addresses) which appear at the very periphery of the investigation (e.g. in the contacts lists of Tier 1 SOIs which are not opened by MI5 as SOIs in their own right).
[164] Written evidence – MI5, 7 June 2018.

148. It would be possible for an SOI to be both 'peripheral' and 'low-level' (for example, a Tier 3 SOI in a P3 investigation).



What is a 'Closed SOI' and how are they managed?

149. Individual SOIs within an active investigation may be 'closed' if it is established that they are not, or are no longer, engaging in Islamist extremist activity. The SOIs within an investigation may also become Closed SOIs when the investigation itself concludes (unless they are also connected to other current investigations, in which case they will be reallocated to those investigations). The Closed SOI category forms a very large pool, currently at around 21,000 people.

150. At the point of closing an SOI, MI5 and CTP jointly consider:

- the likelihood of the individual engaging in new activity of national security concern following closure; and
- the potential threat to national security were that SOI to engage in new activity of national security concern.

151. Closed SOIs are then categorised as High, Medium or Low residual risk (the vast majority are in the Low category). MI5 retain a file on every Closed SOI, but they are no longer under active investigation by MI5. It is possible that the individual will be recommended, as a result of the investigation, to another organisation for further investigation, for example the police or HM Revenue and Customs.

152. In 2013, MI5 and CTP introduced a new system for managing emerging and residual threats by monitoring Closed SOIs. This is intended to provide a structured way of examining the threat posed by Closed SOIs, whereby CTP and MI5 jointly assess the risk that these SOIs will re-engage with extremist activity. Under the system, those Closed SOIs who are judged to pose a High or Medium residual risk are assigned to the most appropriate MI5 regional station, who work with their police counterparts to use basic investigative tools to review these individuals. ***.

153. In 2015, MI5 introduced a process called Operation CLEMATIS, which involves comparing *** against ***. This was initially conducted ***, but from ***. MI5's Science Advisory Council advised as part of the Internal Reviews that ***:

> *In the short term we believe CLEMATIS … ****.[165]

154. All Closed SOIs highlighted by CLEMATIS (***)[166] are reviewed for consideration for possible further action. Those who are assessed to meet the threshold for further investigative enquiries are passed on to Operation DAFFODIL, ***.

155. If DAFFODIL finds any concerns of possible re-engagement in extremism or terrorism, this is treated as a new piece of incoming intelligence (i.e. a new 'lead') and is fed into the MI5 system in the normal way for assessment, prioritisation and potential further action. MI5 explained that ***:

> *** *CLEMATIS* ***.[167]

156. In addition to CLEMATIS and DAFFODIL, MI5 have informed us that they are also currently in the process of categorising all their Closed SOIs in a more granular way, and treating them according to the level of risk they are assessed to pose:

> *we are in the midst right now of … a large pile of work to … sub categorise … closed SOIs, because there is a range of people in there … ****. So there is a range of types in there and we are in the process of categorising those now into … ****.[168]

Y. The Emerging and Residual Threats system, CLEMATIS and DAFFODIL all clearly represent major steps forward in MI5's management of Closed Subjects of Interest (SOIs). We support improving these operations yet further, including progressing the Science Advisory Council's recommendation that CLEMATIS should be run *. We also support MI5's current work to categorise its entire pool of Closed SOIs into risk bands and to treat the higher-risk individuals accordingly, although we were surprised to learn that they had not already been subject to such categorisation.**

Westminster attacker: Khalid MASOOD (peripheral/low-level/ Closed SOI)

157. On a number of occasions from the 1970s onwards, CTP had investigated MASOOD in relation to criminal activity and he had subsequently been convicted of various offences. These offences, however, had no connection to extremism. He was first formally identified in the national security context in August 2010 (MI5 only consider individuals to be fully identified when their full name, address and date of birth have been confirmed). It could then be seen

[165] MI5 and CTP, *Operational Improvement Review*, October 2017.
[166] As at the time the Internal Reviews were produced in autumn 2017.
[167] Oral evidence – MI5, 15 March 2018.
[168] Oral evidence – MI5, 15 March 2018.

that his telephone numbers and email addresses had been recorded on the periphery of other investigations since 2004, but he had not been fully identified at the time:

- In April 2004, a mobile phone number which we now know to have belonged to MASOOD was one of around 100 found in the contact list of Waheed MAHMOUD, who had been arrested under Operation CREVICE.[169]

- Between 2004 and 2009, several email addresses and phone numbers which we now know to have belonged to MASOOD appeared on the periphery of MI5 investigations arising out of Operation CREVICE. Again, these were not identified at that time. (In 2005, MI5 checked one of these telephone numbers and correctly identified the account as belonging to a 'Mr K Masood' at an address in Crawley, although this was not sufficient to constitute full identification.)

- In 2009, MI5 received intelligence that someone called 'Masood' was engaging in extremist activity in Saudi Arabia.

- In January 2010, MI5, as part of Operation E, sought to establish whether an (unidentified) individual they suspected of engaging in extremist activity in Saudi Arabia was in fact the 'Masood' referenced in the 2009 reporting. As such, MASOOD – albeit still not fully identified at this time – was then formally investigated as an SOI for the first time. By March 2010, however, MI5 had confirmed that the unidentified individual in Saudi Arabia was not in fact MASOOD. As a result, MI5 assessed that MASOOD was less likely to be engaging in Islamist extremist activity and he thus became a more peripheral figure in the investigation.

158. After MASOOD was fully identified in 2010, he continued to be an open SOI (albeit peripheral) under Operation E. He was briefly *** and he was subsequently closed as an SOI in October 2012. Further intelligence from 2012 to 2016 showed MASOOD to be an occasional contact of individuals linked to Al Muhajiroun, but those contacts were insufficient to warrant investigation in his own right. In June 2016, Operation E, to which MASOOD was still linked, ***.

Z. From the date of his phone number first appearing on the periphery of an investigation, it took MI5 over six years to identify Khalid MASOOD. This is despite email addresses and phone numbers, which we now know to have belonged to him, being in contact with known extremists on numerous occasions, and his being mentioned in reporting. Whilst we recognise that 'joining the dots' between thereto-unconnected pieces of information and identifiers is a highly complex task, we nonetheless urge MI5 to consider what more can be done to connect those seen on the peripheries of investigations.

Manchester Arena attacker: SALMAN Abedi (peripheral/Closed SOI)

159. In December 2010, SALMAN first came to MI5's attention when he was seen associating with a former member of the *** who was the subject of a low-priority investigation. No

[169] This Committee has previously reported on the links between the CREVICE plotters and two of the July 2005 London bombers (*Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, Cm 7617). MAHMOUD was convicted of a bomb plot in 2007.

other intelligence of national security concern was found concerning SALMAN, however, and therefore no further action was taken at that time.

160. ***, SALMAN's father – RAMADAN Abedi – ***. *** had travelled to Tripoli with his sons, SALMAN and HASHEM, in August 2011 in order to deliver medical supplies and aid to rebels fighting the Gaddafi regime. ***.

161. In December 2013, SALMAN was suspected of being an individual who had been observed acting suspiciously alongside an existing SOI, although he only became an SOI in his own right for the first time in March 2014. MI5 later concluded that SALMAN was not in fact the unidentified individual in question, and he was closed as an SOI in July 2014. He was judged to pose a low risk, and did not face any further scrutiny under the system for managing emerging and residual threats.

162. In 2015, SALMAN was identified as being the owner of a telephone number which had been seen previously *** in contact with ***, a known extremist who was under investigation. SALMAN was seen to have remained in contact with ***. That same phone number had also been seen in *** 2013 in connection with another individual suspected of extremist links: *** his friend 'Salman' in Manchester, for whom he gave the telephone number. However, no further actions had been taken in relation to the phone number at that time.

163. From mid-2015 onwards, SALMAN was mentioned on several occasions in *** reporting, which included information as to his espousal of pro-Daesh views ***. He was not, however, actively investigated – in part due to *** view that he would not pose a threat in the UK. In October 2015, a telephone number associated with SALMAN was assessed *** to be a contact of individuals of interest overseas; SALMAN was briefly reopened as an SOI based on the belief that this was a direct link, but was almost immediately closed again when investigators established that the contact had been second-level rather than direct.

164. ***.

CLEMATIS in relation to SALMAN

165. On 3 March 2017, the CLEMATIS process (***) flagged *** Closed SOIs, including SALMAN. SALMAN had been selected due to ***. This was investigated, and *** CLEMATIS ***. Further searches on SALMAN were then carried out under CLEMATIS and these led to the ***. MI5 then found that SALMAN ***. They therefore assessed that SALMAN was overseas, probably in Libya.

166. On 8 May 2017, the CLEMATIS team assessed that SALMAN should be considered for referral into Operation DAFFODIL for further low-level investigative enquiries in order to identify whether he had re-engaged in Islamist extremist activity, ***. A prioritisation meeting was scheduled to take place on 31 May 2017 to discuss whether SALMAN (one of *** Closed SOIs under consideration) should be referred into DAFFODIL. As MI5 put it, "*the plot then moved faster than the process*"[170] and SALMAN committed his attack nine days prior to that scheduled meeting.

[170] Oral evidence – MI5, 15 March 2018.

AA. We are encouraged that the CLEMATIS process correctly identified SALMAN Abedi as being of concern. However, there is clearly a problem in terms of timescales: in this case, the activity which had triggered the concern *. Had he been flagged and considered for referral sooner, then SALMAN might have been subject to investigation under DAFFODIL before he committed an attack.**

London Bridge attack: Khuram BUTT (active SOI)

167. Operation BEGONIA was opened by MI5 in *** 2015 following reporting that BUTT aspired to conduct an attack in the UK. A significant amount of coverage, *** was put in place following this initial reporting. This coverage did not find any indication that BUTT was taking steps to plan an attack. As a result of there being no further intelligence on BUTT's attack aspirations, BEGONIA was downgraded from a P2H to a P2M investigation in September 2016.

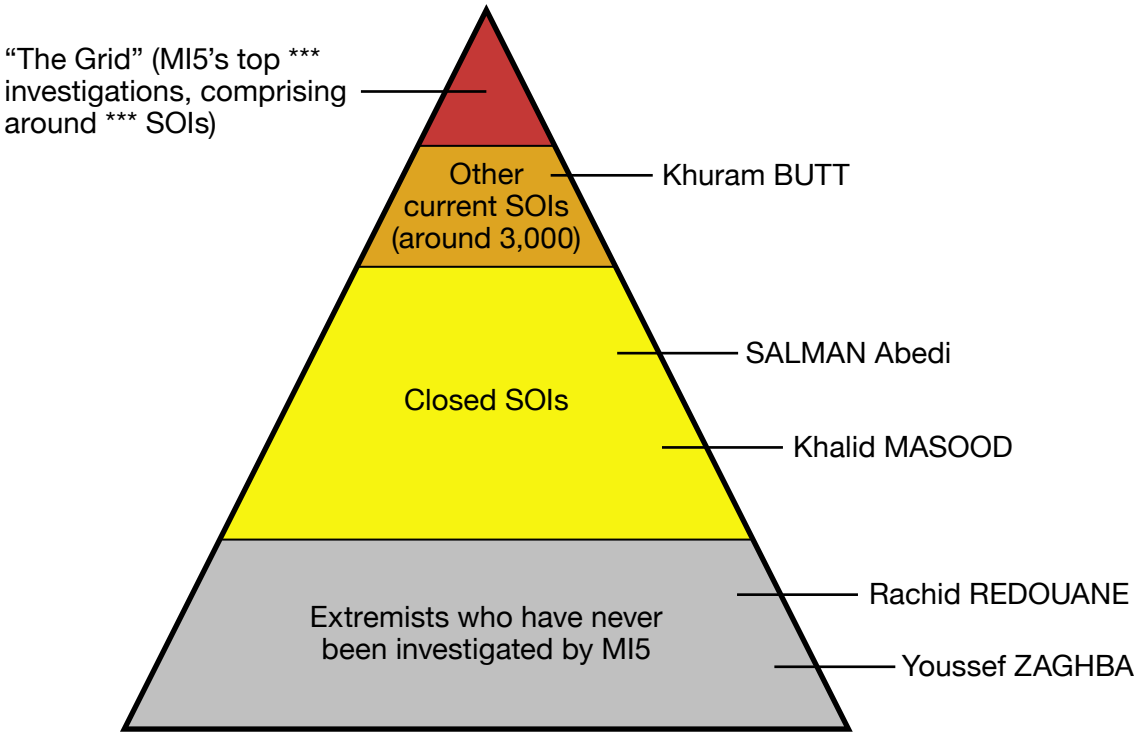
168. The investigation into BUTT was suspended twice – from February to April 2016 and from March to May 2017 – in each case due to competing resource pressures from higher-priority investigations. After the second suspension, the investigation was resumed on 5 May 2017: at this point MI5 were minded to close the investigation, but decided first to increase coverage in order to ensure they had a full picture of the risk posed by BUTT. Discussions were continuing about how BUTT would be managed and what ongoing investigative actions were required at the time the attack took place.

169. The other London Bridge attackers – Youssef ZAGHBA and Rachid REDOUANE – were not investigated by MI5 before the London Bridge attack:

- MI5 had received one piece of intelligence on ZAGHBA in June 2016 from Italian liaison regarding ZAGHBA's attempted travel from Italy to Istanbul in March 2016. The Italian authorities assessed that he wanted to travel onwards to Syria and requested traces on ZAGHBA from MI5 (this is covered in more detail in Section 11 on Travel).

- In connection with their investigation into BUTT, MI5 had received a number of strands of intelligence regarding a Moroccan male named 'Rashid', who they assessed to be a peripheral and social associate of BUTT. Following the attack, analysis identified 'Rashid' as REDOUANE.

Where the 2017 attackers fit in the hierarchy of SOIs



Managing low-level, peripheral and Closed SOIs: past problems and planned improvements

Previous ISC reports

170. This Committee has previously identified problems with MI5's management of low-level, peripheral and Closed SOIs:

- In 2014, the *Report on the intelligence relating to the murder of Fusilier Lee Rigby*[171] (the 'Woolwich Report') raised issues around the handling of low-level, peripheral and Closed SOIs.
- In 2006 and 2009, the *Report into the London Terrorist Attacks on 7 July 2005*[172] (the 'original 7/7 Report') and *Could 7/7 Have Been Prevented?*[173] (the '7/7 Review') respectively raised issues concerning peripheral and Closed SOIs.

Low-level SOIs

171. In its Woolwich Report, the Committee considered the investigative and prioritisation process used within MI5, particularly in relation to low-priority investigations and SOIs. The Committee found that there were considerable delays in processing new leads where the information did not immediately relate to a threat to life (i.e. lower-level priorities). The Committee concluded:

---

[171] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.
[172] *Report into the London Terrorist Attacks on 7 July 2005*, Cm 6785.
[173] *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, Cm 7617.

> *The eight months it took for MI5 to start investigating Adebowale* [one of the two Woolwich attackers] *(three months to identify him followed by five months of inaction) is unacceptable.… There is a problem with the time taken to investigate low priority cases and MI5 must seek to address this by introducing deadlines.*[174]

172. The Committee also discovered that whenever an 'Intelligence Operations Centre' (a major incident room relating to a high-priority time-sensitive operation) was opened, MI5 dropped some lower-priority investigations entirely. The Committee recommended that a funding model should be considered which prevents this from happening, allowing lower-priority investigations to continue uninterrupted.

173. However, this specific issue arose again in relation to the 2017 attacks when the investigation into BUTT, as a lower-priority investigation, was suspended when higher-priority investigations reached a crescendo of activity (albeit that in this case the suspension of the investigation probably did not have a direct impact on his ability to carry out the attack).

Peripheral SOIs

174. In the original 7/7 Report, this Committee found that two of the bombers had been seen previously on the periphery of a major terrorist investigation (Operation CREVICE), but they were not themselves priority (i.e. Tier 1) SOIs in that investigation, and were only peripheral. As there had been more pressing priorities at the time, MI5 did not immediately follow up to investigate the peripheral SOIs in the investigation further, and even when staff were freed up to start to examine them they were soon diverted back to what were considered higher investigative priorities.

175. In relation to the 2017 attacks, the issue of MI5 not having the resources to follow up on people who appear in the margins of investigations was seen again in the case of MASOOD, who had been a contact of known extremists since 2004 but was only fully identified in 2010.[175]

176. In the Woolwich Report, this Committee highlighted the lack of any MI5 strategy for assessing the 'cumulative effect' of individuals who appeared as peripheral SOIs in multiple investigations. The Committee concluded:

> *MI5 does not currently have a strategy for dealing with Subjects of Interest who occur on the periphery of several investigations. This is one of the key issues which has arisen during the course of our Inquiry and 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 SoIs, MI5 must take this 'cumulative effect' into account. They should ensure that interactions between SoIs are highlighted when making investigative decisions.*[176]

177. MI5's failure fully to take into account the cumulative effect of individuals appearing on the periphery of numerous investigations appears also to be relevant in the cases of MASOOD

---

[174] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.
[175] We note, however, that MI5 consider that an extensive investigation into MASOOD would not have met their necessity and proportionality tests, and thus even if resources had been available MI5 would still not automatically have followed up his case.
[176] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.

and SALMAN. Both had been in contact with several extremists over a period of years, ***, but it is not clear that the accumulation of minor 'flags' had been fully taken into account in either case.

178. More generally, the Woolwich Report revealed wider problems in the management of both low-level and peripheral SOIs: a number of CTP and MI5 systems and databases developed since 2008 to track these individuals had failed to deliver as intended, with the volume of suspects involved being cited as the main reason for failure.

Closed SOIs

179. In its Woolwich Report, the Committee concluded in relation to Closed SOIs:

> *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…. 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.*[177]

180. In its 7/7 Review, the Committee noted that one of MI5's 'lessons learned' from the attacks was the creation of a 'legacy team', whose role it would be to review Closed SOIs from previous major operations and to follow up on intelligence that, given limited resources and the original operational focus, was not prioritised for further action at the time – this could include following up on peripheral SOIs from closed operations. The Committee noted that as the legacy team had only been operational for one year (at that time) it was too early to conclude on its effectiveness, but mentioned that MI5 had reported that the team had already generated some useful leads.

181. In relation to the 2017 attacks, the issue of how often Closed SOIs were subject to review (if, indeed, they were reviewed at all) arose again in the cases of the two Closed SOIs: MASOOD had not been flagged as potentially posing a renewed risk by any review of Closed SOIs prior to his attack, and although SALMAN had been flagged by the CLEMATIS process (see above) MI5's systems moved too slowly, and he had not been reviewed before he launched his attack.

Changes in the handling of low-level, peripheral and Closed SOIs

182. The Government did not indicate that any specific changes would be made directly to the handling of low-level, peripheral or Closed SOIs as a result of the issues that the Committee had identified and the recommendations we made in either of the 7/7 Reports or the Woolwich Report.

183. In that context, we note that the Internal Reviews make the following recommendation:

> *The current distribution of resources within the investigative machine should be moved marginally* [away from Priority investigations] *in favour of closed/discovery and leads work.*

---

[177] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.

184. This strongly echoes the recommendations made by this Committee since 2006 regarding the balance of resources between major investigations and low-level or seemingly dormant SOIs, as outlined above.

185. When asked about the Government's failure to respond properly to the Committee's previous recommendations on this subject, OSCT informed us that it would "*establish an action tracker for past Committee recommendations to ensure that suitable progress is being made in all relevant areas*".[178] OSCT did explain that low-level, peripheral and Closed SOIs have for a long time been a particularly difficult threat to manage, and recently the problem has worsened:

> *Attempts to effectively address this issue have been ongoing over the last decade. Each new idea or solution has been an improvement on the previous one, with lessons learned and successes built upon.*
>
> *Ultimately, though, this* [is] *one of the toughest challenges that counter terrorism investigation faces, and if there were a perfect solution, it would have already been found.*
>
> *One of the reasons this has taken so long is because the challenge is continually evolving. In the past, the speed at which low-level, peripheral or closed subjects of interest moved to posing an acute threat took a long time, and the agencies and CT policing would be able to see that move much more obviously. However, now that change from a low-level, peripheral or closed subject of interest to an acute threat can happen much more quickly.*[179]

186. The Internal Reviews concluded that a new approach to the overall management of existing Closed SOIs should be developed by MI5 and CTP, to include:

- ensuring all incoming intelligence on Closed SOIs is treated in the same way as intelligence on new threats (due by October 2017);[180]
- a new approach to managing Closed SOIs (and potentially other SOIs) by sharing more information with more of MI5's partners, and establishing mechanisms for a joint approach to managing risk (with pilots beginning in November 2017);[181]
- categorising the existing c. 21,000 Closed SOI records to enable risk-based consideration for interventions and the possible use of further behavioural 'tripwires';
- MI5 reinforcing existing procedures to ensure that all suitable candidates are referred to Prevent at the point of closure;[182] and
- improvements to MI5's CLEMATIS process – with more data, greater frequency and improved co-ordination with partners.[183]

---

[178] Written evidence – OSCT, 9 May 2018.
[179] Written evidence – OSCT, 9 May 2018.
[180] MI5 and CTP, *Operational Improvement Review*, October 2017.
[181] MI5 and CTP, *Operational Improvement Review*, October 2017.
[182] MI5 and CTP, *Operational Improvement Review*, October 2017.
[183] MI5 and CTP, *Operational Improvement Review*, October 2017.

187. We asked MI5 and CTP whether there was an argument for selecting a proportion of Closed SOIs at random and conducting a brief but intensive investigation into their current activities. They stated that this was not put forward as a recommendation by the Operational Improvement Review since any investigative response must be necessary and proportionate:

> *In all investigations, actions taken must be proportionate to what is sought to be achieved, and this involves balancing the intrusiveness of the activity against the need for the activity in operational terms, recognising the effect on privacy of the SOI and any collateral intrusion.*[184]

188. The CONTEST 2018 Strategy indicates that further improvements are intended in relation to low-level, peripheral and Closed SOIs, stating:

> *Last year's attacks in London and Manchester highlighted both the challenge of detecting individuals who may be inspired to commit terrorist acts in the UK, and the pace at which plots can move to acts of violence. This places a renewed importance on our understanding of those individuals who are vulnerable to radicalisation or who are (or have been) of interest to the police and the security and intelligence agencies due to their possible links to terrorist-related activities, but who may not be currently the subject of any active investigations. Responding to this changing threat requires a new approach, one that combines improved intelligence sharing with a more effective local approach that allows effective early interventions to protect the public.*[185]

189. In terms of specific actions, it states that over the next three years the Government will:

> *develop a series of multi-agency pilots to trial ways to improve information sharing and enrich our understanding of the threat at the local level, including of closed and closing subjects of interest.*[186]

BB. Overall, it is clear that MI5 are now taking serious steps to improve their management of Closed SOIs, and we welcome this. It is disappointing, however, that previous recommendations of this Committee have clearly not been taken on board until now.

[184] Written evidence – CTP and MI5, 19 April 2018.
[185] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[186] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.

SECTION 11: TRAVEL

A number of issues relating to travel monitoring and restrictions arise in the context of the Manchester Arena and London Bridge attacks, for example:

- MI5's decision not to place travel monitoring or travel restrictions on the Manchester Arena attacker, SALMAN Abedi;
- the length of time officials spent considering whether to make a recommendation to the Home Secretary regarding the refusal of a passport application for one of the London Bridge attackers, Khuram BUTT; and
- problems with information sharing with foreign liaison partners on London Bridge attacker, Youssef ZAGHBA.

190. MI5 and CTP rely on a range of tools to alert them to Subjects of Interest (SOIs) travelling abroad, potentially for extremist purposes, or SOIs re-entering the UK. Two examples are ***.[187]

191. MI5 and CTP also have a number of powers to allow them to disrupt an SOI's travel should it be judged necessary and proportionate to do so. Those powers relevant to the 2017 attacks include:

(i) Ports examination under Schedule 7 of the Terrorism Act 2000:

An examining officer may stop, question, search and detain, individuals and goods at UK ports and the border area to determine whether they are or have been concerned in the commission, preparation or instigation of an act of terrorism. This is usually achieved through questioning the individual and searching their possessions. The examination can last up to a maximum of six hours, after which the person must be released or arrested, unless detained under another power. Ports examinations under Schedule 7 are often referred to as a 'Port Stop'.

(ii) Use of the Royal Prerogative:

A British passport may be refused or withdrawn from an individual if it is considered necessary and proportionate, and the Home Secretary is satisfied that it is in the 'public interest' to do so. This may be the case where a person whose past, present or proposed activities, actual or suspected, are believed by the Home Secretary to be so undesirable that the grant or continued enjoyment of passport facilities is contrary to the public interest. For example, passport facilities may be refused to individuals who seek to engage in fighting, extremist activity or terrorist training outside of the UK and who may subsequently return with knowledge and capabilities that they can use to conduct an attack on UK soil.

187 ***

Decision not to monitor or restrict travel

192. During SALMAN Abedi's time under active investigation (March 2014 to July 2014) and as a Closed SOI from July 2014 onwards, MI5 and CTP received information informing them of SALMAN's ***, frequent travel to Libya ***. However, he was not, at any point, subject to any form of travel monitoring or travel disruption.

193. The Committee found this highly surprising, and questioned MI5, who explained that SALMAN was predominantly a Closed SOI (only having been under investigation as a Tier 3 SOI for three months in 2014 and one day in 2015):

> *** *It was open to investigators to request a Ports Action* *** …
>
> *we concluded that he should have been placed under Ports Action ***, the better decision would have been* [to] *have put him on Ports Action on what was known, and that is the conclusion we have reached.*[188]

The Committee asked MI5 what might have happened had SALMAN been subject to travel monitoring:

> *the conclusion was we cannot see it would have made a difference because of the timeline that few days window would have given us, but in principle it was the right thing it should have happened* ***.[189]

194. MI5 did not consider it necessary or proportionate at the time to subject SALMAN to travel monitoring. ***.[190] ***.

CC. SALMAN Abedi should have been subject to travel monitoring and/or travel restrictions. *, MI5 should have put alternative measures in place to alert them to SALMAN Abedi's movements.**

DD. The Committee notes MI5's assessment that had SALMAN Abedi been placed under travel restrictions, there still may not have been sufficient time to identify or act on his attack planning. It would, nevertheless, have provided more of an opportunity.

Improvements to travel monitoring and restrictions

195. MI5 have implemented a number of changes to the way they monitor both Active and Closed SOIs.[191] From November 2017, ***:

> *part of the work that we did following the attacks* [was] *to just take stock of our policy ***. … So our policy as of today, having changed last year, is now that* ***.[192]

Whilst the Committee welcomes the change in policy regarding the monitoring of Active SOIs, we query why the *** was not always the *** policy. It seems surprising that MI5 and

---

[188] Oral evidence – MI5, 25 April 2018.
[189] Oral evidence – MI5, 25 April 2018.
[190] ***
[191] These changes were flagged up in the *Operational Improvement Review* but MI5 note that the review of these procedures was already under way.
[192] Oral evidence – MI5, 25 April 2018.

CTP have not been using the full range of capabilities available to them (where necessary and proportionate to do so).[193]

196. MI5 also noted substantial changes to their policy on the use of travel monitoring for Closed SOIs:

> *we are in the process now of implementing a shifted policy approach, *** – but we are currently tiering the Closed Subjects of Interest and for probably the first three tiers within that very large cohort we will be mandating that, again, *** but, again, with provision to depart from that *** as the case may demand.*[194]

The Committee asked if, as a Closed SOI, SALMAN Abedi would have been placed in the top three tiers of the new system, and thereby have been *** subject ***.[195] MI5 commented that ***:

> *we are still in the early stages of the new approach bedding in but ***.*
>
> *We are doing this knowing, of course, that we are giving ourselves additional complexity in the system, which itself will mean that there will be, you know, there is bound to be a percentage of imperfections in there about who is which side of which line, but it will be a better understanding, a better textual understanding of that otherwise tens of thousands lump.*[196]

197. Such a significant increase in *** will inevitably have resource implications; however, the Commissioner explained:

> *So from a police point of view, you may be aware that we have fairly dramatically reduced the number of schedule 7 stops over the last several years, noted by Max Hill, from 61,000 in 2012 to 17,000. So our people are less busy in volume terms, ***. So we would say that is a more proportionate use and we don't believe that – from a police point of view I can't speak for MI5 – that such a change at the moment is likely to put a particularly large burden on us in volume terms.*[197]

Separately, MI5 noted that while the numbers would increase, that did not mean a commensurate increase in leads or investigations as a result:

> *Last month we received ***, compared to, across the previous year, the monthly average was in the low ***, give or take. Typically our investigators had to rate their value of all the various streams of information they receive and typically *** are useful sort of building block intelligence. They are rarely pivotal to the course of an investigation …*
>
> *If these changes work as we intend, then in logic we will be raising our bar somewhat for the things that get deeper attention.*[198]

---

[193] MI5 and CTP have commented that they select the appropriate tools to manage the risk that individuals pose.
[194] Oral evidence – MI5, 25 April 2018.
[195] ***
[196] Oral evidence – MI5, 25 April 2018.
[197] Oral evidence – CTP, 25 April 2018.
[198] Oral evidence – CTP, 25 April 2018.

198. To support this change, two additional processes around CTP engagement with individuals have been rolled out:

- ECHINACEA – allows CTP officers based at ports to request enhanced screening checks against 'unknown' CTP nominals (e.g. an individual identified as potentially being linked to extremism but who has not yet been designated as an SOI). Any traces and/or links to current investigations may result in the officer instigating a Schedule 7 examination.

- FREESIA – proactive monitoring of all 'SX Ports Alerts'. These are requests *** to use their powers under Schedule 7 of the Terrorism Act 2000 to detain and interview individuals. The police officer may use their discretion as to whether or not to conduct a Schedule 7 examination. FREESIA enables ***.

EE. The Committee supports the policy change being implemented by MI5 and CTP in respect of the use of travel monitoring for Closed SOIs. We note, however, the impact that these changes will have on day-to-day resourcing: both organisations will need to assess these during the implementation phase.

Royal Prerogative

199. British citizens do not have a statutory right to a passport. The Home Secretary holds the power to issue, withdraw or refuse a British passport under the Royal Prerogative.

200. There are a range of circumstances under which a passport can be withdrawn or refused – including if it is deemed not to be in the public interest. It can be used as a disruptive power: a passport may be refused to an individual who seeks to engage in fighting, extremist activity or terrorist training outside of the UK and may return with enhanced capabilities that they can use to conduct an attack on UK soil.[199]

201. When it is considered that an individual's passport should be withdrawn, or their application refused, their case is examined by *** legal advisers to determine if it meets the legal threshold. If it does, a recommendation letter is sent to the Home Office. The Home Office checks the case, after which a submission is sent to the Home Secretary for consideration. If the Home Secretary agrees with the recommendation, HM Passport Office (HMPO) will be notified and the passport cancelled or application refused. The individual then has three months to challenge the decision via a Judicial Review.[200]

202. ***:

> ***.[201]

The Home Office confirmed that the Royal Prerogative power is used relatively infrequently:

> *between 2013 and 2017, the Royal Prerogative was executed against … 84 individuals; they have the right to review, to have a review of that, and there were 38 reviews that were conducted, five passports returned. They*

[199] Home Secretary, written statement to Parliament, 'The issuing, withdrawal or refusal of passports', 25 April 2013.
[200] ***
[201] ***

> *also have a right to ask for a Judicial Review and we have successfully defended three challenges in the High Court on that.*[202]

203. The process for providing a recommendation for the use of the Royal Prerogative can be seen in the case of the London Bridge attacker, Khuram BUTT. BUTT *** while he was under active investigation by MI5 in 2015, ***. In November 2015, BUTT applied to renew his passport. Officials decided to ask HMPO ***. In January 2016, BUTT's travel was monitored whilst officials began to create a case for the refusal of his passport application using the Royal Prerogative.

204. *** reporting indicated that whilst BUTT was supportive of Daesh, ***. As a result, officials judged that it was becoming unjustifiable to withhold BUTT's passport any longer.[203]

205. The Committee questioned why this critical process took so long. However, it appears that the timeframe was driven by the investigation:

> *Essentially that was a function of Butt's own activity and intention assessed mindset … The only overseas travel of any significance – not extremist significance, but significance in his life – that I am aware of was he did do the Hajj I think in early 2015 or 2016. But the 2016 story of Butt was ***. But then, in the light of the developing intelligence picture, where it then looked as though ***.*[204]

206. The Committee was told that the Royal Prerogative power is capable of being used at pace if it is operationally necessary. CTP also highlighted that it has the power under Schedule 1 to the Counter-Terrorism and Security Act 2015 to prevent individuals travelling for 14 days, and that this can be used immediately:

> *So it is a temporary power, so it prevents the traveller on that occasion* ***.[205]

Problems around information sharing with, and by, foreign liaison partners

207. MI5 and CTP work closely with a number of international partners, collaborating operationally, sharing intelligence regularly and co-operating on a number of sensitive issues. Information is shared with European partners (for both CTP and MI5) in a number of ways – including bilaterally and on a wider sharing basis via the Schengen Information System (SIS II), the EU's law enforcement information-sharing system. The UK Border Force checks all entrants to the UK against information held on SIS II.

208. On 15 March 2016, the London Bridge attacker Youssef ZAGHBA attempted to fly from Marconi airport, Bologna, to Istanbul. ZAGHBA only had a *** and told officials he was going to Istanbul "*to be a terrorist*". He immediately corrected himself to "*tourist*". The Italian authorities placed ZAGHBA on SIS II. However, he was incorrectly listed under a serious crime alert rather than in relation to national security issues, meaning it was not

---

[202] Oral evidence – Home Office, 1 May 2018.
[203] ***
[204] ***
[205] Oral evidence – CTP, 25 April 2018.

referred to MI5 by the National Crime Agency.[206] Furthermore, despite the Italians listing ZAGHBA as requiring a 'specific check' at 'Port', there were no indications of what specific action was being requested. SIS was informed by a partner agency on 15 April 2016 about the 15 March incident. Traces[207] were requested on ZAGHBA and any contacts he had in the UK with individuals linked to Islamist extremism ***. The note was 'triaged'; however, it was not translated by SIS until 49 days later and, as a result, MI5 did not receive the note until six days after that. There is no record of an MI5 response, and the note was not filed in MI5's corporate system.

209. ZAGHBA was able to travel between the UK and Italy on three occasions between May 2016 and January 2017, with no action taken other than the UK Border Force noting his arrival at a UK port (in line with standard policy in response to a hit against SIS II). Whilst the Italian authorities were notified of these events, no follow-up requests or further information were provided. The Committee raised these failures with MI5. They responded: "*As David Anderson says in his review, the story of that ZAGHBA trace request is not a particularly happy one.*"[208]

210. The Committee queried the significant time delay between SIS' receipt of the note and MI5's receipt of a translated version eight weeks later. The Internal Reviews note that this is not an unusual timeframe for action in response to an unsolicited note from a partner agency. The reviews note that, at the time of receipt, there was no dedicated full-time translation resource ***, who were then operating under high operational demands and with temporary staff shortages. SIS assessed the note to be a routine record of an aspiring traveller and it was not therefore regarded as a high priority.[209]

211. The Committee questioned why the lack of a 'full-time translation resource' was an issue, given that SIS officers undertake language training before being posted overseas. MI5 explained:

> *of course ***, they are *** speakers and so they can do that, but unless it is flagged as an urgent thing, it probably is not going to be top of the pile.*[210]

In terms of translation more generally, MI5 noted:

> *the reality of the volume of this business though is that a lot of it does come to us in English and they translate themselves and it is just inconsistent. When we look right across all those 30 countries, or the 100 odd that we work with globally, most requests addressed to us come in English, because they want to frame it so that we are actually more likely to respond. When it doesn't, then a translation is necessary.*[211]

---

[206] MI5 have noted that there was nothing within the SIS II entry to suggest that there were counter-terrorism concerns associated with ZAGHBA. There was no information given in the 'types of offences' category and there was nothing in the entry to indicate that he had attempted to travel to Syria.
[207] A trace is a request for a check across MI5 databases to determine if the Agency holds information on the individual in question.
[208] Oral evidence – MI5, 25 April 2018.
[209] MI5, *London Bridge Post-Attack Review*, October 2017.
[210] Oral evidence – MI5, 25 April 2018.
[211] Oral evidence – MI5, 25 April 2018.

212. A further concern is that the processes and systems used for information sharing with foreign partners appeared not to have worked in this case. MI5's response indicates a more general flaw in the system:

> *the issue around the ZAGHBA case in SIS II and so on, for some countries there is just difference of use of the systems … SIS II is fundamentally a criminal system for law enforcement and putting entries on it is about flagging the travel of suspects and criminals. It has a category on it where the country making the entry can put a specific flag that this is terrorism related. It did not do that in the ZAGHBA case, so when he travelled and it hits the standard alert at the UK border, it doesn't throw up "This is for a terrorism reason", and so it doesn't then connect into our shared world and that is one of the things where we are trying to get a system correction across the whole of Europe.*[212]

MI5 are seeking to address this through the Counter Terrorism Group (CTG) – in which all EU Members, Norway and Switzerland are represented:[213]

> *So one of the things I am … going to raise … at the table at the meeting is, can we all agree that, where it is terrorism related, we do our best to actually flag that on the system. That is harder for some countries to do than others because of which agencies are doing the entering and it is horrifyingly complicated …*

213. It is clear that the differences in structures between countries do not help matters, as MI5 explained:

> *there are still differences in the legislative definition between different jurisdictions, and sometimes subtly so, and more importantly there are differences in practice which derive from the different responsibilities that differently constituted agencies have in different constitutions … most European countries don't have something that looks exactly like MI5, they have something else that might have grown out of law enforcement roots, or might still be part of a wider policing structure. Some have ones like us and others have things that derive from more recent military connection, particularly some of the east Europeans are that way, some are not, and it is quite hard trying to corral all the detail of that to common practice and consistency, but we used our Presidency of the Counter Terrorism Group last year, which we hung on to, to shift the dialogue on some of this.*[214]

However, MI5 reassured the Committee that, in their view, the problem is not insurmountable:

> *we just need to have better discipline from differently built services around Europe about how they use these systems so there is consistency, so that when one thing happens, where it originates from one country, it flags in the same way for any other country and any other border crossing.*[215]

---

[212] Oral evidence – MI5, 25 April 2018.
[213] The CTG was established in 2001 in response to the 9/11 attacks. Whilst EU-facing, the CTG is not an official EU institution.
[214] Oral evidence – MI5, 25 April 2018.
[215] Oral evidence – MI5, 25 April 2018.

214. One factor which cannot be ignored is the potential impact of Brexit on the intelligence Agencies' ability to collaborate with international partners. MI5 commented:

> *Of course that whole arrangement is then dependent on a political future … depending on what happens in the Brexit deal, there is a dependency for us here in the security world, we need that continued access to SIS II, for all the reasons we are talking about.*[216]

CTP supported this view, noting:

> *we are very keen, obviously, not to get stuck in politics or undermine anybody's negotiating position but we want the same access that we currently have in essence.*[217]

FF. Regardless of operational demands, an eight-week delay between the receipt of a trace request from a partner agency and onward dissemination is far too long. Delays of this nature could have a very significant impact on an operation, not just here in the UK but in other countries too.

GG. The Committee acknowledges the difficulties of working with partners with different organisational structures and ways of working. We welcome the progress made during the UK's Presidency of the Counter Terrorism Group on national security collaboration: the UK's exit from the EU must not impact on the information-sharing relationships and powers currently available to the UK intelligence community.

CONTEST

215. The revised CONTEST Strategy covers issues around travel under both the Pursue and Protect strands. Under Pursue, it sets out that individuals wishing to engage in terrorism will be stopped from travelling overseas to Syria and Iraq and refers to the powers in the 2015 Counter-Terrorism and Security Act – in particular the temporary seizure of passports at the border.[218] In terms of those who have already travelled to the conflict zones, it states that more than 900 individuals of national security concern have travelled from the UK to engage with the conflict in Syria, of whom approximately 20% have been killed while overseas and around 40% have already returned – thereby leaving around 360 still overseas who may have received training and indoctrination and therefore pose a significant threat to the UK. The strategy notes that individuals who have travelled to the conflict zone must expect to be investigated by the police on their return to determine if they have committed criminal offences or to assess if they pose a threat to national security.

216. Under the Protect strand, one of the objectives listed is to "*detect and deal with suspected terrorists … at the border*".[219] The strategy includes border checks to identify individuals of interest, measures to improve screening and detection technologies, and the ports powers available to the police under Schedule 7 of the Terrorism Act 2000. It also notes the need to ensure that "*other countries have the right information* [and] *can take appropriate action by*

[216] Oral evidence – MI5, 25 April 2018.
[217] Oral evidence – CTP, 25 April 2018.
[218] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[219] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.

stopping individuals associated with terrorism at the border",[220] saying that "*we have increased the amount of information we share with trusted partners and multilateral bodies (including the Schengen Information System, Europol and Interpol capabilities*".[221]

217. We note however that there are no actions proposed, or new powers suggested, to tackle the problems exposed by the 2017 terrorist attacks – in particular in relation to the problems around information sharing with European partners which will inevitably come under increasing focus post-Brexit.

Counter-Terrorism and Border Security Bill

218. In the context of travel-monitoring tools and disruption powers, the Bill proposes two updates to Schedule 7 of the Terrorism Act 2000:

- It will ensure that CTP is able to use the full period of pre-charge detention (provided under the Terrorism Act 2000) to question a terrorist suspect before having to release or charge them.[222]
- The Bill will also respond to Lord Anderson's concerns around self-incrimination, enshrining in law the protection against self-incrimination where someone is questioned at a port under Schedule 7.

[220] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[221] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[222] *Counter-Terrorism and Border Security Bill 2018 – Counter-Terrorism Powers Fact Sheet*, 6 June 2018. The Bill will also ensure that periods spent receiving hospital treatment, or travelling to or from a hospital, will be excluded when calculating the time that a suspect has spent in detention under suspicion of being a terrorist.

SECTION 12: DISRUPTIVE POWERS

A variety of disruptive tools were considered during the course of the investigation into Khuram BUTT, the perpetrator of the London Bridge attack, including:

- delaying, or recommending the refusal of, the issuing of BUTT's new passport to prevent overseas travel;
- exploring a potential charge for fraud; and
- exploring whether BUTT's accessing of extremist material online, identified after his arrest, could provide a basis for criminal charges.

219. Disruptive powers are used by MI5 and CTP to dissuade or prevent individuals from engaging in terrorist-related activities. MI5 note that their primary aim is always to prosecute on a terrorism charge; however, where this is not possible, disruptive powers provide an opportunity to manage the risk.

220. Disruptive powers considered may include: warnings issued to individuals noting that their activities are being monitored by the authorities; ***; and the issuing of Terrorism Prevention and Investigation Measures (TPIMs).[223] MI5 explained:

> *Disruptive powers … is the term we use for everything in addition to and alongside prosecution that we can reach for that can make a difference to the risk presented by individuals … over the years, it has become a richer toolkit with new legislation incrementally over the years, particularly in the counter-terrorism space, as the problems have got worse …*
>
> *We now have quite a rich range of choices, including some relatively novel things developed under English law, *** … we have developed a systematic approach to their use in different cases according to the risk that different individuals present … being able to deport for national security reasons people who are foreign nationals, being able to deprive British citizenship, ***, excluding people from the UK, refusing visas, TPIMs and a range of police powers at ports.*[224]

CTP described a recent case:

> ***.[225]

221. The Home Office told the Committee that in 2017 it had used:

- 104 deprivations of British citizenship;
- 26 exclusions (all on national security grounds);[226]

[223] Terrorism Prevention and Investigation Measures (TPIMs) place restrictions on individuals who are assessed to pose a terrorist threat, but who either cannot be prosecuted, for example because of insufficient disclosable evidence, or who have been prosecuted, served their sentence and released but are assessed to continue to pose a threat.
[224] Oral evidence – MI5, 25 April 2018.
[225] Oral evidence – CTP, 25 April 2018.
[226] The UK can deprive individuals for reasons other than national security.

- 14 Royal Prerogative cases; and
- 9 Temporary Exclusion Orders.[227]

As of May 2018 there were eight TPIM notices in force.[228]

MI5 explained that recent developments have led to an increase in their use of disruptive powers:

> *Because of the Syria-related situation and the large numbers of travellers, we collectively, and with the Home Secretary's use of her Secretary of State authority, have taken a position … we have rather deliberately pushed to the edge of what we think the system can bear and authorise, not beyond it, but we have not shrunk from using these things to their, you know, full extent … we want to know where the legal boundaries are and we then want to live right up to them fully and inhabit that space, particularly in the threat world that we live in.*[229]

222. During the 2017/18 financial year, the police made 445 terrorism-related arrests compared with 379 in the previous year, representing a 17% increase. Of the 2017/18 arrests, 141 (32%) were made under Terrorism Act legislation, compared with 59 (16%) in the previous year. CTP did note, however, that this rise was primarily due to the 64 post-attack arrests.[230]

Impact of disruptive activity against Khuram BUTT

223. BUTT had been investigated by MI5 as a priority Subject of Interest (SOI) from *** 2015, when MI5 opened Operation BEGONIA following reporting that BUTT aspired to conduct an attack in the UK.[231]

224. BUTT displayed a high level of operational security throughout the period MI5 investigated him. This included:

- ***;
- ***;
- ***.

On several occasions reporting indicated that BUTT advised his associates to deploy similar operational security practices.

225. In November 2015, officials decided to ask HM Passport Office ***[232] ***.[233] The Committee was concerned that this demonstrated that the use of disruptive activities could

[227] Temporary Exclusion Orders (TEOs) temporarily disrupt the return to the UK of a British citizen suspected of involvement in terrorist activity abroad. This is achieved through the cancelling of the individual's travel documents and adding them to watch lists (e.g. 'no fly' lists).
[228] Written evidence – Home Office, 10 October 2018.
[229] Oral evidence – MI5, 25 April 2018.
[230] Written evidence – CTP, 16 May 2018.
[231] By September 2016, the investigation had been downgraded on the basis that BUTT was planning to travel overseas.
[232] ***
[233] ***

potentially have a negative impact on the behaviour of SOIs. The Committee was informed that this was a risk, but that:

> *we seek to make judgements, case by case, on what we believe the likely effect of an intervention has been and, in the end, that is a judgement, it is not a particularly scientific thing and it will fluctuate across time. So we try jointly to reach clever judgements about what is the particular form of risk posed by this individual, for instance will they pose more risk if they are still in the UK or if they travel overseas, and we try, we force ourselves, to count as part of our quarterly casework review mechanism, where do we think we have had a disruptive impact and has that been an enduring and strong disruptive impact or has this just had a short-term tactical effect or, worse, are there cases where we think it has had a counterproductive impact? That doesn't happen very often at all but we do try to be as objective as we can be about the effect, case by case and trending across time, about the use of the whole toolkit.*[234]

226. In July 2016, there was a potential disruption opportunity presented by BUTT's suspected engagement in bank fraud, and CTP arrested BUTT in October 2016.[235] However, by June 2017 it was decided[236] that no further action (against BUTT) could be taken, due to a lack of evidence. During BUTT's arrest in October, CTP had discovered files that it considered "*may be successfully used in a prosecution under the Terrorism Act*" (offering a further means of disruption); however, ***[237] and the issue was not explored further.[238]

The Behavioural Science Unit

227. The Behavioural Science Unit (BSU) are a team of behavioural and social science specialists within MI5. They provide support to investigative desk officers and agent handlers to help them understand their SOIs better, and advise on a range of approaches to agent-handling issues.

228. The Committee asked MI5 whether the BSU had any input into assessing the impact of disruptive activity on SOIs. MI5 noted:

> *on occasions they have run more of a longitudinal set piece study of the effect of interventions; two big studies in particular, one in 2012 and one in 2017, looking at the effects of the interventions that we make.*
>
> [The study found that] *very commonly interventions will provoke heightened levels of operational security awareness on the part of extremists …***, *so that is sort of baked into all of our operational planning from the beginning.*
>
> *The second interesting element that does emerge … is the question around … thwarted travellers. In the case where a UK-based extremist wishes to travel (most typically these days to Syria) we have a strategy, not observed in every single case, it is always a case-by-case judgement … but*

---

[234] ***
[235] For bank and Department for Work and Pensions fraud.
[236] CTP decided in consultation with the Crown Prosecution Service.
[237] MI5, *London Bridge Post-Attack Review*, October 2017.
[238] MI5, *London Bridge Post-Attack Review*, October 2017.

> *by and large we seek to ***. It is true though that taking those actions, as we have broadly successfully done over the last two or three years, does in the minority of cases lead to that ***.*[239]

229. In relation to BUTT, the BSU's assessment:

> [was] *within the methodology that we run around spontaneous and volatile extremists and he was judged to be … a moderate risk as a spontaneous volatile extremist and subsequently that judgement was revisited and he was categorised as unresolved. So … the Behavioural Science Unit was involved in looking specifically at Butt. This was some time after the initial reporting around him which contained threat, this was later, when he had gone through his period of aspiring to travel overseas but not then following up on that aspiration.*[240]

However, it does not appear that the BSU were asked to provide specific advice regarding the use of disruptive powers on BUTT, or indeed whether the BSU were notified of ***:

> *This specific report … was not referred to the BSU. Investigative sections are the central decision makers and may seek advice from the BSU if they need support in understanding an individual's behaviour and the circumstances. Intelligence is not routinely routed through the BSU, and in this instance the investigator did not consider that there was a requirement for BSU assessment. BSU advice is based on the whole case rather than individual pieces of intelligence. To route every piece of intelligence through the BSU would unnecessarily clog the system and preclude the provision of a holistic assessment.*[241]

230. During its Inquiry into the murder of Fusilier Lee Rigby, the Committee had been impressed by the potential the BSU offered and recommended that MI5 should integrate their advice more thoroughly into investigations. The Committee requested an update on this from MI5:

> *I think we have developed a BSU role since that time on the extent to which we use them* [to assist with] *CHIS, assessment of SOIs, and actions that we take about them, and, in relation to SOIs, assessment of the risk that potentially unstable people might represent. So they have been particularly acutely used since that time in the space of, you know, "more vulnerable individuals" and the "lone actors" sort of the space, so I think you would find the difference between 2013 and 2017, I guess is what we are looking at today, quite a marked shift in BSU integral involvement.*
>
> *The one other very quick addendum I would suggest is that, in the operational improvement review, in the work we are now doing to take our methodology one stage further, the BSU again is strongly woven through that. So behavioural science informs at its core the analytical work we are looking to use as we head forwards around data.*

---

[239] Oral evidence – MI5, 25 April 2018.
[240] Oral evidence – MI5, 25 April 2018.
[241] Written evidence – MI5, 16 May 2018.

> *So we have got an incubator happening right now in Thames House, with GCHQ in place and other colleagues there, with behavioural science methodology very strongly sort of at the centre of that particular piece of work.*[242]

HH. The Committee is reassured to see the Agencies have taken on board our previous recommendation that the Behavioural Science Unit be better integrated into the investigative process. We expect to be kept updated on progress, with a full report on this matter in 12 months' time.

[242] Oral evidence – MI5, 25 April 2018.

SECTION 13: FAMILIES AND PREVENT

- SALMAN Abedi and his brother HASHEM Abedi were alleged co-conspirators in the Manchester Arena attack.
- Prior to the Manchester Arena attack, MI5 had ***. This raises queries as to MI5's approach to dealing with ***.
- Prevent issues are also relevant to the Parsons Green attack.

Prevent

231. As noted earlier in the Report, the Prevent strand of CONTEST covers the Government's counter-radicalisation work to stop people becoming terrorists or supporting terrorism. Prevent seeks to reduce the number of people drawn to violent extremism in the UK by investing in a community-driven approach, working closely with mainstream and moderate groups in the British Muslim community (although the programme addresses all forms of terrorism, including that inspired by far-right extremism). It also works to rehabilitate people who are, or have been, involved in terrorism and safely reintegrate them into society.

232. Prevent includes working with industry to remove terrorist material from the internet; supporting civil society groups to deliver effective counter-narrative campaigns; and working with vulnerable people to reduce the risk of them being drawn into extremism, through the Channel programme.

233. OSCT has noted the importance of local work with communities and civil society organisations. It told the Committee that, in 2016/17, 169 community-based projects were run to tackle the threat from radicalisation in local communities which reached over 53,000 people.[243]

234. Individuals are referred to Prevent through different channels including teachers, healthcare workers, the police and members of the public. All referrals are assessed by the police to consider whether the individual is already under investigation, if there is a genuine vulnerability and if that vulnerability is related to terrorism. Those referrals that relate to individuals *** will be passed to the relevant *** team. If this is not the case, the police manage the referral and any subsequent action through the Prevent Case Management (PCM) process.[244]

235. Policing is the largest source of referrals into Prevent – accounting for 33% of referrals in the first three quarters of 2017/18 ***.[245]

236. Prevent (and its related programmes) rightly fall within the Home Affairs Select Committee's (HASC's) remit.[246] Therefore this Inquiry has only considered those aspects of Prevent relevant to the 2017 terror attacks.

---

[243] Written evidence – OSCT, 8 May 2018.
[244] Written evidence – OSCT, 8 May 2018.
[245] Written evidence – MI5 and CTP, 16 May 2018.
[246] HASC published a Report on the Prevent strategy on 30 January 2018.

Families and Prevent

237. In some cases, a Prevent referral may lead to consideration of the family environment. The Committee questioned the strategy when multiple members of the same family are under consideration. We were told:

> *So it is an area that is woven through … quite a lot of our casework and where we are always up at pains not to make assumptions in either direction ... it is often the case that, when we are investigating a particular extremist, another family member, perhaps more than one other family member, will also be* [at issue] … *to some degree or another. I think that occurs in* [some of the cases] …
>
> *It is also the case that in* [some of] *our casework …* [the individual has] *got members of their families who are actively opposed to their extremism and, in* [some] *cases, family members who have been trying actively to persuade the extremist to desist.*
>
> *So we cannot make ready judgments about this is a "You always should suspect the family" or "You should always believe the family is a helpful influence".*[247]

The Channel programme

238. The Channel programme, which operates under the Prevent strand, was launched in 2007 as a project to identify and support people (across England and Wales) who are at risk of radicalisation. Individuals are referred to a Channel panel, which is chaired by the relevant local authority and includes the police as well as representatives from a variety of different agencies. Statutory guidance includes advice on which agencies to invite to panels, according to the circumstances of the individual case, but generally panels include representatives from health (including mental health), education, housing and social care.

239. The panel meets to discuss each case and to assess the extent of the vulnerability of the individual. If the panel decides the individual does not need further help, the referral is closed. In other cases, the panel will offer the individual a support package tailored to their needs.[248] Channel interventions can take a variety of forms, including help with youth services, education, employment and housing. Ideological mentoring to provide the individual with the skills to protect themselves from being drawn into terrorism-related activity can also be provided.

240. Participation in the Channel programme is entirely voluntary. OSCT told the Committee that, as of March 2018, over 1,300 people had been supported through the programme (since 2012), including 300 in 2016/17 alone. Some 79% of those who received support from the programme in 2016/17 left the programme with their vulnerability to be drawn into terrorism judged (by the assigned Channel panel) as having been successfully reduced.[249]

---

[247] ***

[248] Written evidence – OSCT, 8 May 2018.

[249] Written evidence – OSCT, 8 May 2018.

241. Those individuals who choose not to participate in the Channel programme, or who leave the programme before the Channel panel decides they are ready, may be offered an alternative form of support or are managed by the police through police-led PCM.[250]

Issues raised previously

242. In its 2014 Report on the murder of Fusilier Lee Rigby, the Committee noted a failure to refer individuals to 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.*[251]

The Committee concluded:

> *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.*[252]

243. However, the Government disagreed with the Committee, responding that it was "*disappointed that the high priority which has been afforded to this important work* [Prevent] *was not acknowledged … Police and other partners now routinely consider preventative interventions where appropriate.*"[253]

The Abedi family

244. Multiple members of SALMAN Abedi's family ***.

RAMADAN Abedi (Father)

- SALMAN Abedi's father, RAMADAN Abedi ***, is a British-Libyan national.
- RAMADAN was ***.
- ***.
- ***.
- ***, there is no evidence of any Prevent or Channel referrals for any member of the Abedi family.

[250] Written evidence – MI5 and CTP, 16 May 2018.
[251] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.
[252] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.
[253] *Government Response to the ISC Report on the intelligence relating to the murder of Fusilier Lee Rigby*, Cm 9012.

ISMAIL Abedi (Brother)

- One of SALMAN Abedi's brothers, ISMAIL Abedi ***, also a British-Libyan national, ***.
- ***.
- ***.
- ***.

245. ***:

> ***
>
> *So we cannot even now look at the Abedi case and say it is obvious because of the father's activities over the years that two or three of the sons would become extremists, but it is relevant to the story, clearly.*[254]

Nevertheless, post-attack it appears highly likely that SALMAN and HASHEM's extremist views were influenced by their father RAMADAN Abedi and fostered by other members of their immediate family.[255]

246. In such cases, it is clear that Prevent referrals should have been considered and the Committee questioned what appeared to be a failure of the system. OSCT explained that, as MI5 had previously investigated SALMAN Abedi, any decision about the further management of his case – whether to reopen the investigation or to refer him to police for PCM – would have been an operational matter for MI5 to consider in consultation with the police.[256] This is reflected in the Internal Reviews, which explain:

> *during the MI5 investigation closure process, the investigative team must consider referring to PREVENT any SOIs* [Subjects of Interest] *who are not being taken forward by another active investigation or lead. The investigator must justify any decision not to refer to PREVENT and this must be signed off by an MI5 investigative team leader.*

247. However, in the case of SALMAN Abedi, MI5 noted that Prevent had not been actively considered:

> *the interventions that were made around or the action that was taken in respect of SALMAN Abedi was the fact that he was investigated for two periods ***. As far as we can determine from the records, there was not a decision, a conscious decision, made around Prevent referral.*[257]

CTP told the Committee:

> *we have no evidence that North-West* [Counter Terrorism Unit[258]] *considered a Prevent referral. You would expect it to be considered but there is no*

[254] Oral evidence – MI5, 25 April 2018.
[255] ***
[256] Written evidence – OSCT, 8 May 2018.
[257] Oral evidence – MI5, 25 April 2018.
[258] The North-West Counter Terrorism Unit is one of 11 such CTP units across the UK. It is responsible for police work to prevent, disrupt and prosecute terrorists in Greater Manchester, Cheshire, the Isle of Man, Lancashire and Merseyside.

documented rationale about whether it was considered and rejected or whether it was never considered.

I would have expected to have seen a consideration and a rationale about why it was not … I would expect to see a consideration and a decision made and the decision could be positive or negative.[259]

248. CTP emphasised that Prevent referrals generally had improved, but acknowledged that there is still a lack of consistency in approach:

we spent three years kind of changing the culture of focused Pursue-led operations into understanding the safeguarding risks, so if Prevent, with a capital P, was all about safeguarding, we have got a much better culture amongst senior investigating officers that the default part of their strategy that they have to have a Prevent strategy when they are investigating their case.

So we have got better at that and that includes the conversations that happened jointly and in partnerships. It is not consistent. It is still a training issue. It is still a cultural issue, but you would have expected in a case where there were vulnerable children in a house for Prevent to be considered.[260]

249. MI5 offered their perspective:

I think in truth the picture on this has improved across time, though inevitably it is probably still imperfect now. So we are now in a position where we have … much stronger clarity around the mandation of Prevent referrals for people who arise in the course of investigations and are judged to be vulnerable or some way along a radicalisation pathway towards Prevent. We are currently piloting the national multi-agency centre, partly for these reasons. I gave a talk last week to a range of colleagues from other departments, HMRC and the Department for Work and Pensions, so we are trying a range of things at the moment to build a more convincing multi-agency set of tools to do things about such cases.

It probably will remain true that there will be hundreds and hundreds of young people who are subject to a degree of radicalisation in the home, and we will not always know and even if we do know, we will not always have a satisfactory set of interventions that will change the course of their radicalisation, but we are much more consistent now, considering this … through our casework.[261]

II. SALMAN Abedi should have been considered for a Prevent referral after his closure as an SOI in July 2014. It is concerning that there is no evidence of a discussion between CTP and MI5 as to a potential referral.

[259] Oral evidence – CTP, 25 April 2018.
[260] Oral evidence – CTP, 25 April 2018.
[261] Oral evidence – MI5, 25 April 2018.

JJ. The Committee is surprised that at no point were any members of the Abedi family referred to the Prevent programme – *. It is highly disappointing that Prevent was, once again, not applied to SOIs who later went on to instigate an attack – an issue this Committee has previously criticised.**

Changes to Prevent

250. Government policy around Prevent has been to isolate the brand from association with the Agencies, so as to avoid allegations that the programme is 'spying' on specific communities. Inevitably, this has led to a number of process and policy issues restricting MI5's use of the Prevent referral system. For example, MI5 are not currently involved in the design of the Prevent programmes (these are created using Joint Terrorism Analysis Centre (JTAC) and police information). This means that the Prevent programmes lack the potential benefits gained from MI5's knowledge of local intelligence (e.g. locations and institutions closely associated with former SOIs) and input from the Behavioural Science Unit on ways in which people engage or disengage with extremism and terrorism.[262]

251. The Internal Reviews propose three overarching recommendations ***:

- *Processes for Prevent referrals should be reinforced to ensure all suitable candidates are referred on closure.*
- *More Prevent and Channel data should be shared with MI5 where appropriate and necessary, in the interest of national security.*
- *Training, guidance and awareness raising activities* [around Prevent referrals] *should be bolstered.*[263]

CONTEST

252. The CONTEST Strategy sets out three key objectives regarding Prevent:

- *Tackle the causes of radicalisation and respond to the ideological challenge of terrorism.*
- *Safeguard and support those most at risk of radicalisation through early intervention, identifying them and offering support.*
- *Enable those who have already engaged in terrorism to disengage and rehabilitate.*[264]

To achieve this, the Government has committed to:

- *Focus our activity and resources in those locations where the threat from terrorism and radicalisation is highest.*

---

[262] In addition, *** OSCT has noted that the new CONTEST strategy contains links with Pursue along with objectives including a focus on the known threat, Desistance and Disengagement programme and online work – all of which have clear links to the Agencies.
[263] MI5 and CTP, *Operational Improvement Review*, October 2017.
[264] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.

- *Expand our Desistance and Disengagement Programme with an immediate aim over the next 12 months to more than double the number of individuals receiving rehabilitative interventions.*

  …

- *Build stronger partnerships with communities, civil society groups, public sector institutions and industry to improve Prevent delivery.*

- *Re-enforce safeguarding at the heart of Prevent to ensure our communities and families are not exploited or groomed into following a path of violent extremism.*[265]

253. The new element is the Desistance and Disengagement programme, piloted in 2017. The programme is designed for individuals subject to court-approved conditions, for example individuals who have been convicted of terrorism and/or terrorism-related offences who are on probation licence; those on Terrorism Prevention and Investigation Measures (TPIMs); and those who have returned from conflict zones such as Syria or Iraq and are subject to Temporary Exclusion Orders (TEOs). The Desistance and Disengagement programme differs from Channel in that an individual's engagement with it can be mandated, and non-compliance could lead to being charged for breach of conditions or being recalled to prison.[266]

Counter-Terrorism and Border Security Bill

254. The 2018 Counter-Terrorism and Border Security Bill seeks to amend sections 36 and 38 of the Counter-Terrorism and Security Act 2015, to grant local authorities the power to refer individuals to the Channel programme. The Home Office argues that doing so will ensure a timelier referral for those at risk of being drawn into terrorism.[267] The Minister of State for Security and Economic Crime notes:

> *This change will improve the efficiency of Channel panels and so ensure that such individuals receive the support they need in a timely manner to guide them away from such activity.*[268]

Parsons Green

255. Ahmed HASSAN, the Parsons Green attacker, was not – and had never been – an MI5 SOI. HASSAN did come to the attention of MI5 on one occasion on 2 February 2016 during a discussion with CTP, ***.

256. In HASSAN's asylum application interview on 18 January 2016, he claimed to have arrived in the UK illegally via a freight lorry in October 2015. During the asylum interview HASSAN claimed to have been taken by force by Daesh, trained to kill against his will and

[265] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[266] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[267] *Counter-Terrorism and Border Security Bill 2018 – Channel Panel Measures Fact Sheet*, 6 June 2018.
[268] The Rt Hon. Ben Wallace MP, Minister of State for Security and Economic Crime, quoted in *Counter-Terrorism and Border Security Bill 2018 – Channel Panel Measures Fact Sheet*, 6 June 2018.

had spent several hours a day in a mosque undertaking religious study. HASSAN stated that he had not received weapons training and had not been sent to the UK to work for Daesh.[269]

257. Details of his asylum application *** HASSAN was subject to a Prevent referral. The referral set out the claims made in HASSAN's asylum interview and indicated that he suffered from post-traumatic stress disorder (PTSD).[270] Between June 2016 and September 2017, HASSAN was an active Channel case. Nine formal Channel panel meetings were held to discuss his case (although none were held between January 2017 and June 2017).

258. During the course of its Inquiry, the Committee requested evidence regarding HASSAN's Prevent referral and participation in the programme. MI5 and CTP indicated that this was a matter for the Home Office. However, despite repeated requests, the Home Office failed to provide any evidence in sufficient time for it to be included in the Inquiry. It subsequently indicated that rather than provide evidence it would copy to the Committee the letter that it was providing to the HASC. At the time of writing the Committee has just received this, which can be found at Annex A.

259. It is clear to the Committee that there have been fundamental failings in the manner in which HASSAN's case was dealt with by the Home Office, CTP and Surrey County Council. The litany of errors that resulted in HASSAN's attack-planning passing unnoticed, despite his participation in the Channel programme, highlights deep-rooted issues in the administration of the Prevent strand of CONTEST.

260. The Committee notes here a number of questions about HASSAN's case:

(i) Why, despite HASSAN's revelations to authorities of his interactions with Daesh, was support from a Home Office-approved Intervention Provider[271] not requested?

(ii) Why did the Channel panel ignore his ongoing mental health issues and instances of going missing from foster care, even when these issues were raised by a member of the panel?

(iii) Why did the panel not have, or request, information relating to HASSAN's asylum application – particularly when it was noted that the process was causing HASSAN distress?

(iv) Why, despite HASSAN being under the care of Surrey County Council Children's Services, were they not in attendance or providing adequate reporting to the panel?

261. HASSAN's case also raises wider questions particularly relating to individuals in a similar position:

- How many cases exist of individuals displaying similar characteristics to HASSAN (e.g. have reported contact with Daesh, have missed official appointments, show signs of absconding from foster care)?

---

269 ***

270 Written evidence – MI5, 4 March 2018.

271 Intervention Providers offer specialised mentoring to individuals engaged in the Channel process to address issues around radicalisation.

- In how many other cases has a member of the Channel panel raised concerns regarding a participant's behaviour, but no action has been taken? What process should be triggered? Are additional reviews carried out? Are CTP/Security Services notified?

- How many individuals fail to attend initial asylum screening interviews? What process should be triggered? Are these individuals flagged to CTP and Security Services?

- What plans does the Government have to raise issues with the Dublin Treaty (i.e. regarding the limitations around what actions can be carried out in relation to unaccompanied minors) with European partners?

262. The Committee views the Home Office response (as detailed in the attached Annex A) as weak, lacking in clarity and unacceptable in light of the seriousness of the failings. The Committee will write to the Home Secretary requesting the primary evidence and full answers to each of the questions and issues outlined above.

KK. The Committee considers the Home Office's failure to provide evidence relating to Ahmed HASSAN's case such that the Committee could consider it as part of this Inquiry as unacceptable. There are a number of fundamental failings in the handling of HASSAN's case: the Committee hopes that the Home Affairs Select Committee will instigate a thorough review of the Prevent programme in relation to this case.

SECTION 14: PROTECTIVE SECURITY

Protective security issues arise in the following context:

- In Manchester, the issue of protective security for major venues arises.
- In Westminster, London Bridge and Finsbury Park, the issue of protective security for crowded pavements arises.

263. 'Protective security' is the use of routine physical or procedural measures designed to remove, reduce or mitigate threats to people, buildings, information or other assets. Simple examples of protective security measures are locking the front door of your house to protect against burglary and password-protecting your mobile phone to protect against unauthorised access to your data. A more complex example would be an architect designing a housing estate to ensure that there are no concealed areas, thus minimising the risk of criminal activity. Proactive measures that do not relate to a specific individual threat – such as installing CCTV or undertaking routine security patrols – are also considered to be protective security. In a counter-terrorism context, examples of protective security include search and screening procedures, laminated glazing or Hostile Vehicle Mitigation Measures.

Responsibility for protective security policy and advice in Government

264. The Government's work to improve protective security arrangements to prevent a terrorist attack is covered by the Protect strand of CONTEST, which is managed by OSCT in the Home Office. This includes:

- strengthening UK border security;
- reducing the vulnerability of the transport network;
- improving the resilience of Critical National Infrastructure; and
- reducing the vulnerability of crowded places, specific vulnerable groups and high-profile individuals from terrorist attack.

265. In terms of frontline work, cyber-related protective security sits with the National Cyber Security Centre (NCSC), which is part of GCHQ. An example of NCSC's work includes providing individual advice to public and private sector organisations on how their computer systems can be made more secure, as well as offering general computer security advice to the public.

266. Responsibility for advising on non-cyber protective security lies with the National Counter Terrorism Policing Headquarters and the Centre for the Protection of National Infrastructure (CPNI), the latter of which is accountable to the Director General of MI5. Examples of CPNI's work include advising developers of high-profile buildings on designs that will minimise the risk – and mitigate the consequences – of terrorist attack, and advising the managers of sensitive sites (e.g. airports, power stations) on the design of perimeter security needed to prevent breach and hostile reconnaissance. Day-to-day advice on protective security

at less high-profile sites is provided by written circulars from CTP, and through bespoke advice and guidance from Police Counter Terrorism Security Advisers (PCTSAs).

Responsibility for implementing physical protective security measures

267. Broadly speaking, it is the owner of a public place who has responsibility for ensuring the safety of members of the public in that space, and this responsibility extends to installing physical and other counter-terrorism measures, where it is appropriate and proportionate to the threat to do so. OSCT explained how Government assists owners of certain crowded places and Critical National Infrastructure sites in doing this:

> *… they will get a lot of support, one, to encourage them to design out the threat … on a user pays basis, so them putting in bollards or hardened glass or whatever… they are supported in that by 170 … counter-terrorism security advisers as part of CT police.*

268. OSCT noted:

> *Interestingly,* [owners] *normally accept our advice … there is considerable appetite in the industry to help … there are great opportunities in making sure we enhance that engagement with them by providing them with the requisite guidance and very relevant information to them about the threat.*[272]

269. However, it is not always clear who is responsible for a particular public place – especially on complex sites where the ownership may be split between multiple freeholders and leaseholders. CTP specifically cited the barriers around Buckingham Palace as an example where "*it is not obvious who should pay for what and it never has been*".[273] More generally, OSCT explained:

> *The issue arises around crowded spaces where you may have multiple owners in one space, a shopping centre, let's say, or a town square. There … we do act in seeking them, … on a voluntary basis, to … put in place the right kind of procedures. We are looking at whether we need to … change that in order to raise levels of consistency and standards that are taken in terms of protective security at sites. That needs to be done through consultation because there will be a cost to the industry in that and … there will also be the need for us to put in place … processes that are efficient to do that, and we need first to explore whether we have used all the … levers and regulations that we already have for thinking about whether we need more in that space.*[274]

270. A further problem is that both public and private sector owners of public places must themselves pay for the installation of any protective security measures that are deemed necessary (there is no central funding). CTP admitted that, when owners are reluctant to fund measures that are deemed necessary, "*we have actually quite limited powers to force people*

[272] Oral evidence – OSCT, 1 May 2018.
[273] Oral evidence – CTP, 25 April 2018.
[274] Oral evidence – OSCT, 1 May 2018.

to do anything".[275] When asked whether there should be any legal obligation in relation to the installation of physical counter-terrorism measures, CTP said:

> *we have trialled with the Government … the notion that there should actually be on certain authorities a 'protect' … duty, but that is not something that seems likely at the moment in law. …*
>
> [Currently] *there is no legal clarity about who is responsible and therefore who will pay.*[276]

Vehicle attacks: Westminster, London Bridge and Finsbury Park

271. As noted in Section 6 (Vehicle hire), the use of vehicles by terrorists to attack groups of pedestrians – seen in the Westminster, London Bridge and Finsbury Park attacks – is a recent development, with the first such attack in Europe having taken place in France in December 2014. We have seen that such attacks can lead to high death tolls: the Nice lorry attack in 2016 killed 86 people.

272. The relative simplicity of the method means that such attacks can be carried out by lone actors, who can move from contemplation to action very quickly. ***. Protective security measures – such as bollards and barriers protecting crowded places – can therefore constitute an important means of protection.[277]

273. Nevertheless, it is not practical to install Hostile Vehicle Mitigation Barriers at every public place in the UK. Arguably, therefore, they are only a means of displacement: as certain sites are protected, attackers will switch targets to those which are not protected by bollards or barriers. The Finsbury Park attack demonstrates that vehicle-ramming attacks can take place in relatively low-profile locations, which are unlikely to have physical protective security measures installed. Attacks in such places may indeed be more damaging where armed police officers would be more thinly spread geographically ***.

274. When we raised the question of displacement with OSCT, it did not recognise it to be a problem:

> *I have* [not] *seen evidence … that somebody has consciously displaced their activity to another area; in fact, to the contrary … ***. So we have not seen evidence of that displacement.*[278]

275. CTP did recognise the potential issue but considered that in practice it did not arise: "*clearly there is a risk of displacement but … certain places are more attractive than others*".[279] MI5 agreed that the focus should remain on high-profile targets, explaining: "*making the more obvious and iconic and attractive targets for terrorism harder to attack makes terrorism less likely to happen*".[280]

---

[275] Oral evidence – CTP, 25 April 2018.
[276] Oral evidence – CTP, 25 April 2018.
[277] OSCT informed us that "*Further measures such as operational and procedural mitigations (e.g. suspicious activity reporting and site access control measures), deterrence communications, awareness and vigilance campaigns, and contingency planning, also all increased the likelihood of a vehicle as a weapon attack being deterred, detected or delayed.*" Written evidence – OSCT, 5 July 2018.
[278] Oral evidence – OSCT, 1 May 2018.
[279] Oral evidence – CTP, 25 April 2018.
[280] Oral evidence – MI5, 25 April 2018.

276. After the London Bridge attack, CTP installed Hostile Vehicle Mitigation Barriers to protect the pavement on eight central London bridges and at certain other vulnerable locations. Such barriers come with not just a financial cost, but also a practical cost to pedestrian movement and the wider public realm. We asked CTP what assessments went into the decision to install these barriers, given that some were installed within just 48 hours of the attack:

> *So Westminster Bridge, that was not considered an attack on a bridge … it was just one of the crowded places in an attack on Parliament. …* [I]*t was not considered specifically about bridges until London Bridge happened and then … it was very clearly a decision made by Protect and Prepare, so* [a Deputy Assistant Commissioner Specialist Operations] *and a COBRA recommendation on the day of that attack that we should look at bridges and I think within seven days protective security was put in place on eight bridges.*[281]

Suicide bombing of a crowded place: Manchester Arena

277. The Manchester Arena attack took place immediately outside the Arena itself, in an indoor public place adjacent to Manchester Victoria station, the freehold of which was owned by Network Rail. Although not formally within the curtilage of the Arena, this space effectively constituted the Arena's foyer and contained its box office.

278. SALMAN Abedi spent 15 minutes reconnoitring the site the day before his attack. It is not apparent that he was noted or challenged by staff on this visit. While there was no event taking place, it is nevertheless worth noting that it was a public area with other facilities, including a cashpoint and places to eat. On the day of the attack, SALMAN detonated his bomb inside the foyer while attendees were leaving, despite having not attended the concert himself. Again, he had not been noted or challenged by Arena or Victoria station staff. Numerous other people who had not attended the concert had also entered the foyer at this time – primarily parents who were picking up their children – so his presence was not necessarily suspicious *per se*. While he was wearing a large rucksack, this was in the vicinity of a railway station and therefore not unusual.

279. Nonetheless, we asked CTP whether staff could, or should, have identified SALMAN's reconnaissance of the site the day before as suspicious. They were non-committal:

> *It is difficult to say. I can't say without watching it as to whether it would have alerted* [me]. *It is interesting when you look* [in CCTV footage] *at Abedi walking through the streets of Manchester with the bomb itself that nobody picked that up and then I could take you to Victoria Coach Station on any single day of the week and show you many people doing exactly the same thing.*[282]

[281] Oral evidence – CTP, 25 April 2018.
[282] Oral evidence – CTP, 25 April 2018.

280. We also questioned whether the advice to operators of large venues had been changed following the bombing, and OSCT explained:

> *Yes, so we have improved the guidance to them, and … we would like to go further, in the sense that, you know, there is a very large security industry out there, so the Security Industry Authority has … 324,000 members. These are people who are licensed security guards.* [W]*e want to raise the level, standards, amongst that cohort, particularly around behaviours and behavioural science.*[283]

281. CTP echoed the view that counter-terrorism training should be provided to qualified stewards:

> [T]*he Security Industry* [Authority] *… doesn't currently have* [counter-terrorism] *as part of its curriculum, so we are giving them a curriculum that we are suggesting* [that it] *ought to be a standard part of their curriculum before people get accredited using the SIA.*[284]

282. We asked CTP and CPNI whether they had provided protective security advice (whether bespoke or generic) to either Manchester Arena or Manchester Victoria station prior to SALMAN's attack. CPNI had not, but CTP had.[285] CTP told us:

> *Police CTSAs* [Counter Terrorism Security Advisers] *had engaged with both Manchester Arena and Victoria Station prior to the attacks (but not in relation to the Ariana Grande concert) and delivered protective security advice … CTSA support to Manchester Arena between November 2015 and March 2017 included a specific vulnerability assessment, accompanied by use of the Protective Security Improvement Activity (PSIA) and associated action plan. The PSIA is an innovative assessment tool developed by CT Policing NaCTSO* [National Counter Terrorism Security Office]*, for companies and sites to use to review and improve their security arrangements against terrorist attacks.*
>
> *In addition to this, staff training was provided to the operator (SMG Europe) and the security and crowd management provider (Showsec International). SMG Europe managers attended the regional launch of 'ARGUS Stadia'; a targeted strategic level protective security exercise focused on stadiums. Showsec International had 176 staff on duty on the evening of the attack, of which 174 had completed the CT eLearning training module. Thirteen staff had participated in the CTSA delivered Project GRIFFIN in 2012 (CT awareness training) and the CTSAs were involved in training Showsec to accredit them for Project GRIFFIN self-delivery in February 2017.*[286]

[283] Oral evidence – OSCT, 1 May 2018.
[284] Oral evidence – CTP, 25 April 2018.
[285] CPNI has an ongoing relationship with Network Rail and provides advice in relation to rail assets.
[286] Written evidence – MI5 and CTP, 16 May 2018.

CONTEST 2018 and the Counter-Terrorism and Border Security Bill

283. CONTEST 2018 states that Government will need to engage more with the owners of crowded places in relation to protective security measures, and hints at possible new legislation:

> *We will need to do more* [to reduce the risk of vehicle-ramming attacks]*, in the light of the shift in terrorist methodology and the very large number of sites where people congregate in the UK. We are currently considering the development of more and better communication to crowded places owners, operators and responsible authorities, how we can better engage these stakeholders to achieve effective security outcomes, and if required, potential legislative measures.*[287]

284. The new CONTEST Strategy also includes a case study describing how the police have worked with the Pool Reinsurance Company, in order to incentivise the owners of public places to implement protective security measures through lowering their insurance premiums if they do so. Given the problems we have identified above in ensuring that owners of public places do implement such measures, this is an interesting scheme which – in the absence of mandatory protective security measures – may provide owners with some incentive to take action.

285. The Counter-Terrorism and Border Security Bill contains some modifications to the Anti-Terrorism Traffic Regulation Order (ATTRO) regime. ATTROs were introduced in 1984, and they enable the police – working with local authorities – to restrict vehicle or pedestrian traffic for counter-terrorism reasons. This can include the installation of protective security measures in place on or near roads. In particular, these changes will enable a local authority to charge the beneficiary of an ATTRO (e.g. an event organiser) for the costs associated with it, and clarify the powers of the police to deploy bollards and barriers in relation to permanent or temporary restrictions – however, we note that they will have no relevance where the measures required are not either on or abutting a road.

LL. Although we are encouraged by OSCT's reports of positive engagement on counter-terrorism issues by the owners of public places, we remain concerned that there appears to be no way of mandating owners of public places to install necessary protective security measures where they do not do so voluntarily. This issue becomes yet more difficult where sites have multiple owners. The Government should consider clarifying the legal responsibilities of both site owners and relevant public authorities in this regard.

MM. We understand that well-known places are particularly attractive targets for terrorists, and that making them harder targets therefore makes sense. Nonetheless, we recommend that Government remains cognisant of the displacement risk, and in each case carefully considers whether or not to install barriers: it is neither practical nor desirable to install such measures at every potentially crowded place in the UK.

NN. Even with the most comprehensive training available, it is not clear that Manchester Arena staff could have been expected to identify SALMAN Abedi's behaviour on either of his two visits to the attack site as suspicious. Nonetheless, we support Government's efforts to ensure that those working at major venues are trained to spot suspicious activity.

---

[287] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.

SECTION 15: DATA AND INFORMATION

286. Data is fundamental to the work of the Security and Intelligence Agencies and law enforcement. It is at the centre of their investigations and all that they do. The issue the Agencies face is two-fold: the quantity of data produced has increased significantly over the past decade, whilst the technological environment has become increasingly complex through advances in encryption – meaning that accessing the content of data has become increasingly difficult.

287. The Internal Reviews focus on changes and improvements across the intelligence community in how data is managed, shared and analysed.[288] This does not flow directly from a particular aspect of any of the attacks: it is a more general issue arising from the considerable increase in the number of Subjects of Interest (SOIs) and the amount of data about them that could potentially be analysed.

Data management

288. The Committee has highlighted deficiencies in the Agencies' record keeping in numerous contexts over the years. To take one example, the Committee's Woolwich Report 2016 made the following recommendations regarding MI5, SIS and police record keeping:

> *The Committee is concerned that SIS and CTP 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 CTP 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.*[289]
>
> *We recognise the pressures that investigative teams are under. Nevertheless, MI5 must maintain comprehensive records and ensure that there is a complete audit trail.*[290]

289. It is noteworthy, therefore, that the Internal Reviews contain an entire chapter on 'Information Management', with recommendations including the updating of systems, the introduction of new training and guidance for staff, and better use of information to inform strategy and prioritisation. Record keeping is an area that is, necessarily, subject to continuous improvement – especially when new technology creates new types of information – but it does appear that the attacks have given impetus to further work in this regard. The Committee challenged MI5, who responded:

> *On the record-keeping theme and information management, can I say to you it is now fixed and you will not come back to it? No, I will tell you the reverse, I guarantee in big reviews like this in the future it will continue to be a theme because it is a vital continuous improvement area central to our work, and it is not something where, you know, "Oh we just thought of the information management, we will throw the switch and fix it"; it*

[288] MI5 and CTP, *Operational Improvement Review*, October 2017.
[289] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.
[290] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795.

> *is something you will want to keep holding us to account for, making it stronger and better and acting on the things that we find in each worked instance of ways in which it can be made better but there is no getting there with information management. That is true I think in general for any organisation. It is certainly true for us. There is no "It is now done."*[291]

Data sharing: a multi-agency approach

290. The Internal Reviews, Anderson Report and updated CONTEST Strategy all focus on the importance of going beyond existing relationships and established processes to allow the widest possible range of partners to play a role. In practical terms, this means a new commitment by MI5 to allow knowledge derived from their intelligence to be shared beyond their existing intelligence circles. Data-sharing agreements already exist between MI5 and the other Intelligence Agencies, CTP and liaison partners. However, a broader model of intelligence, involving more partners from outside the traditional security community, which have never received information like this before, represents a challenge for all concerned.[292] MI5 will need to declassify material and share information about their targets with organisations that they do not currently have a relationship with. The Internal Reviews note that MI5 are currently exploring the legal and policy implications of wider data sharing, and the related risks.

291. The suggestion is that a new 'multi-agency approach' is developed, to manage SOIs who are no longer under active investigation through the sharing of MI5 information with a wider range of partners at national and local level. This will allow for an improved understanding of the threat, and enable a joint approach to managing the risk and a more effective local intervention, with involvement by neighbourhood policing, local authorities and other public agencies such as the Charity Commission.[293]

292. The 2018 CONTEST Strategy announced the establishment of Multi-Agency Centre pilots in London, Manchester and the West Midlands. These trials will focus on different ways of sharing information with a broader range of partners to improve the overall understanding of the risks faced. The strategy says that the pilots will also provide an improved understanding of the local threat picture, which will be of benefit to local emergency responses.[294]

293. CTP explained that the current counter-terrorism model already draws on intelligence provided from outside the central intelligence-gathering organisations − predominantly by local policing:

> *the whole point of having a local to global system, is that community information … probably about *** of our intelligence comes from that source, which is much higher than most people would think.*[295]

[291] Oral evidence – MI5, 25 April 2018.
[292] Oral evidence – CTP, 15 March 2018.
[293] MI5 and CTP, *Operational Improvement Review*, October 2017.
[294] *CONTEST – The United Kingdom's Strategy for Countering Terrorism*, June 2018.
[295] Oral evidence – CTP, 15 March 2018.

294. Given that this new approach will involve a two-way flow of information, the Committee questioned both organisations on the potential barriers to the success of the new model. CTP responded:

> *the barriers will be information sharing, the confidence of partners, and the ethics of doing this. There is a debate outside of the security community that really needs to go on … a large part of this was a discussion about the public acceptance of what we might be about to do, so the ethical considerations are foremost and then of course − and I am afraid we are back to the resources question − we are asking partners who have spent the last decade, effectively have been cutting some of these services, to potentially take on risk and the really important point is this is not spread evenly out across the UK.*
>
> *there will be a lot of pressure, where our biggest counter-terrorism units are there, they are there for a reason, they are resourced there for a reason and that will then play out in this. So some regions of the country of which some of you will be very interested in could end up with a risk–resource imbalance which is quite dangerous.*

295. There is a question as to whether, had this new model been in place previously, it might have made a difference but CTP noted:

> *There is no silver bullet here. There never has been in managing that enormous sort of, you know, wicked problem that lies beneath the very acute threat. This is our latest iteration of a long evolution … this is the next generation and these are being piloted.*[296]

MI5 commented:

> *none of us really in truth know, but these improvements represent our collective best judgement as to the changes we can make that slightly stack the odds in our favour.*
>
> *I think given the degree to which the threat has got worse and has changed and 2017, you know, is a year in which the threat markedly got worse, not a year in which MI5 and the police, you know, took our eye off the ball. It is a thing, the thing has developed and developed and grown and we have got to change the ecosystem in response to that, and that is why we are using this language of CT step up …*[297]

296. In addition to this closer working with partners at a local level, the Internal Reviews also address potential changes in data sharing with industry. MI5 and CTP have previously shared information relating to SOIs and processes with Communications Service Providers (CSPs) and financial institutions on a secure basis. According to the Internal Reviews, discussions have begun around the expansion of the scale and scope of data exchanged between MI5, CTP and the financial sector. The Internal Reviews note that this is the first step in the potential

[296] Oral evidence – CTP, 15 March 2018.
[297] Oral evidence – MI5, 15 March 2018.

development of strategic data-sharing relationships with industry; however, it is still very much in the development stage.[298]

OO. The Committee welcomes the new initiative to share intelligence beyond the traditional boundaries in order to strengthen the ability to connect information. This will nevertheless place an additional burden on frontline services already under pressure. We encourage the Government to ensure that this change is sufficiently resourced.

Data analytics

297. In addition to wider data sharing, the Internal Reviews and the CONTEST Strategy suggest working alongside industry and academia to ensure the Agencies are able to keep pace with the increase in available data and – crucially – advances in data analytics. MI5 explained:

> *it is absolutely the case that we believe the current state of data science does offer the potential for us to shift our approach and gain greater capability, and therefore counter terrorism strengths from the use of … the pots of data we have and can get access to and the way in which we can operate a distributed model of analytics …*

298. The Committee questioned what the practical outcomes of utilising data more efficiently would be. MI5 responded:

> *Now, will it be predictive about who is going to do what next? Not so much, but what it will do, and what we can realistically expect it to do, is … spot things that actually deserve more intense deliberate examination by the human being applying the judgement? Yes, we do expect it to do that, including through those upper tiers of the closed cases that get no human attention at the moment because it is not imaginable we would ever be big enough to be able to resource that.*

This is an ambitious proposal that will significantly change the manner in which the Agencies use their data. MI5 highlighted the risks and limitations of the proposed changes:

> *There are some limitations for us … we cannot do it all in Google Cloud space because obviously this is secret stuff and we have to find ways that have proportionate security around it, ***, so you would never expect us to be at the leading edge of this, but what is being developed in the commercial world has application for us … big data, analytics and machine learning, AI* [Artificial Intelligence] *applied, ***.*
>
> ***.[299]

[298] MI5 and CTP, *Operational Improvement Review*, October 2017.
[299] Oral evidence – MI5, 25 April 2018.

299. MI5 explained to the Committee that they are drawing on expertise from industry and academia to help them achieve this:

> *we are testing now ways of doing it and talking to commercial partners about approaches … I have already been in discussion with CEOs and *** they are basically willing to volunteer to help in this and ***.*[300]

300. This change in approach raises a number of privacy concerns around data sharing with industry. The Committee questioned MI5 as to their proposed safeguards:

> ***
>
> *So we want that back, but that involves the risk of us telling people in a non-vetted, although we can do a bit of that, but a largely non-vetted private sector environment, who our targets are.*
>
> *But in counter-terrorism, what is the worst that can happen? So we will take some risk with that in order to get better results.*[301]

PP. The Committee welcomes the Agencies' proposals to use data in a more innovative way. We are encouraged by MI5's commitment to work with industry and academia to help in the design and delivery of this and believe this partnership has the potential for significant skill and capability transfer. These changes are very much in the initial design stages, however, and we will wish to see how they develop.

301. These changes will mean a substantive shift in how MI5 work. MI5 are therefore considering whether they need staff with different skill sets, and what this might mean for the overall configuration of the organisation − for example, how analysts can best work with investigators, collectors and partners in order to get the best out of the large amounts of data available. The Internal Reviews note that MI5 are also investing in a more structured career offer for analysts, improving training and development. This approach is shared across the Agencies:

> *MI5, GCHQ and SIS are working more closely than ever on data analysis, including on training analysts across the different datasets and systems available to each. This is delivering a cadre of staff who are able to operate in each agency regardless of their parent organisation. The Agencies have also developed new tools which increasingly pool data together and allow queries to be run by analysts in different* [agencies].[302]

The Internal Reviews note that, whilst there is senior-level commitment across the organisations, these new ways of working will need to be embedded "*over the coming years*".[303]

QQ. The Committee notes the increased pressure that the changes in the Agencies' use of data will have on existing capabilities and fully supports the proposed sharing of analytical expertise across the organisations. It is encouraged by the Agencies' commitment to the establishment of a more defined Analyst career path and hopes that this will encourage greater retention of staff.

---

[300] Oral evidence – MI5, 25 April 2018.
[301] Oral evidence – MI5, 25 April 2018.
[302] MI5 and CTP, *Operational Improvement Review*, October 2017.
[303] MI5 and CTP, *Operational Improvement Review*, October 2017.

ANNEX A: RECOMMENDATIONS AND CONCLUSIONS

A. This Committee was the first to identify – in its Report into the murder of Fusilier Lee Rigby – the problem of Communications Service Providers (CSPs) failing to remove extremist material from their platforms. In 2014, we urged Government to engage with the CSPs to get them to take action. Progress has been slow but we welcome the steps now being made by CSPs to automate the removal of extremist material.

B. Systems that the CSPs do put in place must ensure that law enforcement agencies are notified of any material that may have a national security threat element. Failure to do so will prevent early detection of potential threats.

C. In return, Government should ensure that it takes a co-ordinated approach to the CSPs: rather than confronting them with competing messages, single points of contact will ensure consistency and simplify the relationship for the CSP.

D. We particularly note the impact that recent action from advertisers such as Unilever has had in encouraging the CSPs to take action. Where reputational levers have failed to produce action, financial levers could provide the solution. We commend these companies and would encourage other major companies to follow their lead.

E. Government should now seek to lobby the business community to take action, following the Unilever example. This is a matter on which we expect a full report from the Government on what action has been taken with the business community within the next six months.

F. The ISC recommended in its 2014 Report into the murder of Fusilier Lee Rigby that more should be done to prosecute those accessing extremist material online. We are disappointed to note that the last four years have seen no progress on this issue. The Government must ensure that the Counter-Terrorism and Border Security Bill, when passed, tackles those who view extremist material online, as well as those who disseminate it.

G. We support the intention expressed in the Internal Reviews to improve the Approved Visitor Scheme in relation to Category A prisoners – although clearly this is dependent on the detail of any measures to be implemented. We expect this detail to be provided by the Government within the next 12 months.

H. The monitoring of visitors to extremist prisoners below Category A is haphazard. This is concerning: it allows known extremist prisoners to potentially maintain links with those vulnerable to extremism. The Government should consider expanding the Approved Visitor Scheme to include all extremist prisoners.

I. It would be wholly inappropriate for prisoners who convert to Islam to be subject to routine monitoring. Nonetheless, prison officers must be trained to identify instances where someone has converted following association with extremists, to assess whether that conversion is therefore part of a positive journey or a negative one for an individual, and to be able to take action in the latter case.

J. While the Committee recognises the sound intention behind segregating extremist prisoners, we are concerned that the new Separation Centres may also provide a networking opportunity for extremists. We urge Government to keep this risk under review, and take what steps it can to minimise it. We expect to see the results of this review in 12 months' time.

K. We are encouraged by witnesses' evidence that those organisations involved in managing, and gathering intelligence on, extremist prisoners are working well together. Nonetheless, we remain concerned that the number of organisations and teams working in this area makes it a crowded space. The Government should keep this matter under review and we expect a report on whether it is still working well in the next 12 months.

L. Whilst there may be some merit in increasing ***, the Committee is conscious of the limitations of this capability. We query whether resources may be better served in seeking alternative solutions.

M. Given the propensity for vehicles to be used as weapons, monitoring vehicle hire must be a significant element of counter-terrorism work. The Committee is encouraged that the Department for Transport and the Home Office are working on a new system to improve the information provided by vehicle hire companies. However, we are concerned that the *** of the proposed scheme significantly reduces the likelihood of its success.

N. The previous system for regulating and reporting purchases of the ingredients used to make explosives such as TATP (triacetone triperoxide) and PETN (pentaerythritol tetranitrate) was out of date in dealing with the threat at the time. The Manchester Arena bombing showed this to devastating effect. We therefore welcome the updates to the current system of regulating and reporting explosives precursor purchases.

O. The Committee notes that the proposed changes to the system will result in a considerable increase in the volume of data generated. We are concerned that there must be sufficient resources to deal with this increase in data. The Home Office must ensure that proper support is in place ***: we expect to see an analysis of what is required within the next six months.

P. We are pleased to hear that progress is being made to develop relationships between retailers and the counter-terrorism network: again, this is overdue.

Q. Whilst there are changes that can – and should – be made to the current arrangements around the regulation of chemicals used in explosives, it is not possible to prevent all purchases: at a certain point the benefits that can be gained from successive tightening of the system will become marginal.

R. ***

S. ***

T. ***

U. The Committee has raised concerns about the need for improved joint working between MI5 and CTP for over ten years. Improvements have been made but we note that this is an area that requires continuous improvement.

V. Further issues that MI5 and the police might consider are: how to ensure comprehensive dissemination of information from MI5 to CTP; cultural change to support the new structures in place to facilitate closer working; and a renewed impetus to resolve the problems caused by incompatible IT systems.

W. The Committee welcomes the number of initiatives focused on improving the flow of information between MI5 and CTP; however, it is important that this results in real, practical change. The Committee expects a report on how this is working and what tangible benefits have been seen in six months' time.

X. The Committee considers that the Government failed to tackle the leaking of information about the Manchester Arena attack sufficiently robustly. Leaking our information – and potentially causing distress to the victims and families in so doing – will not be tolerated. The US administration recognised the seriousness of the situation and we welcome the thorough investigation they undertook.

Y. The Emerging and Residual Threats system, CLEMATIS and DAFFODIL all clearly represent major steps forward in MI5's management of Closed Subjects of Interest (SOIs). We support improving these operations yet further, including progressing the Science Advisory Council's recommendation that CLEMATIS should be run ***. We also support MI5's current work to categorise its entire pool of Closed SOIs into risk bands and to treat the higher-risk individuals accordingly, although we were surprised to learn that they had not already been subject to such categorisation.

Z. From the date of his phone number first appearing on the periphery of an investigation, it took MI5 over six years to identify Khalid MASOOD. This is despite email addresses and phone numbers, which we now know to have belonged to him, being in contact with known extremists on numerous occasions, and his being mentioned in reporting. Whilst we recognise that 'joining the dots' between thereto-unconnected pieces of information and identifiers is a highly complex task, we nonetheless urge MI5 to consider what more can be done to connect those seen on the peripheries of investigations.

AA. We are encouraged that the CLEMATIS process correctly identified SALMAN Abedi as being of concern. However, there is clearly a problem in terms of timescales: in this case, the activity which had triggered the concern ***. Had he been flagged and considered for referral sooner, then SALMAN might have been subject to investigation under DAFFODIL before he committed an attack.

BB. Overall, it is clear that MI5 are now taking serious steps to improve their management of Closed SOIs, and we welcome this. It is disappointing, however, that previous recommendations of this Committee have clearly not been taken on board until now.

CC. SALMAN Abedi should have been subject to travel monitoring and/or travel restrictions. ***, MI5 should have put alternative measures in place to alert them to SALMAN Abedi's movements.

DD. The Committee notes MI5's assessment that had SALMAN Abedi been placed under travel restrictions, there still may not have been sufficient time to identify or act on his attack planning. It would, nevertheless, have provided more of an opportunity.

EE. The Committee supports the policy change being implemented by MI5 and CTP in respect of the use of travel monitoring for Closed SOIs. We note, however, the impact that these changes will have on day-to-day resourcing: both organisations will need to assess these during the implementation phase.

FF. Regardless of operational demands, an eight-week delay between the receipt of a trace request from a partner agency and onward dissemination is far too long. Delays of this nature could have a very significant impact on an operation, not just here in the UK but in other countries too.

GG. The Committee acknowledges the difficulties of working with partners with different organisational structures and ways of working. We welcome the progress made during the UK's Presidency of the Counter Terrorism Group on national security collaboration: the UK's exit from the EU must not impact on the information-sharing relationships and powers currently available to the UK intelligence community.

HH. The Committee is reassured to see the Agencies have taken on board our previous recommendation that the Behavioural Science Unit be better integrated into the investigative process. We expect to be kept updated on progress, with a full report on this matter in 12 months' time.

II. SALMAN Abedi should have been considered for a Prevent referral after his closure as an SOI in July 2014. It is concerning that there is no evidence of a discussion between CTP and MI5 as to a potential referral.

JJ. The Committee is surprised that at no point were any members of the Abedi family referred to the Prevent programme – ***. It is highly disappointing that Prevent was, once again, not applied to SOIs who later went on to instigate an attack – an issue this Committee has previously criticised.

KK. The Committee considers the Home Office's failure to provide evidence relating to Ahmed HASSAN's case such that the Committee could consider it as part of this Inquiry as unacceptable. There are a number of fundamental failings in the handling of HASSAN's case: the Committee hopes that the Home Affairs Select Committee will instigate a thorough review of the Prevent programme in relation to this case.

LL. Although we are encouraged by OSCT's reports of positive engagement on counter-terrorism issues by the owners of public places, we remain concerned that there appears to be no way of mandating owners of public places to install necessary protective security measures where they do not do so voluntarily. This issue becomes yet more difficult where sites have multiple owners. The Government should consider clarifying the legal responsibilities of both site owners and relevant public authorities in this regard.

MM. We understand that well-known places are particularly attractive targets for terrorists, and that making them harder targets therefore makes sense. Nonetheless, we recommend that Government remains cognisant of the displacement risk, and in each case carefully considers whether or not to install barriers: it is neither practical nor desirable to install such measures at every potentially crowded place in the UK.

NN. Even with the most comprehensive training available, it is not clear that Manchester Arena staff could have been expected to identify SALMAN Abedi's behaviour on either of his two visits to the attack site as suspicious. Nonetheless, we support Government's efforts to ensure that those working at major venues are trained to spot suspicious activity.

OO. The Committee welcomes the new initiative to share intelligence beyond the traditional boundaries in order to strengthen the ability to connect information. This will nevertheless place an additional burden on frontline services already under pressure. We encourage the Government to ensure that this change is sufficiently resourced.

PP. The Committee welcomes the Agencies' proposals to use data in a more innovative way. We are encouraged by MI5's commitment to work with industry and academia to help in the design and delivery of this and believe this partnership has the potential for significant skill and capability transfer. These changes are very much in the initial design stages, however, and we will wish to see how they develop.

QQ. The Committee notes the increased pressure that the changes in the Agencies' use of data will have on existing capabilities and fully supports the proposed sharing of analytical expertise across the organisations. It is encouraged by the Agencies' commitment to the establishment of a more defined Analyst career path and hopes that this will encourage greater retention of staff.

ANNEX B: PARSONS GREEN LETTER

Home Office

Sir Philip Rutnam KCB
Permanent Secretary

2 Marsham Street
London SW1P 4DF
www.homeoffice.gov.uk

Rt Hon. Dominic Grieve QC MP
Chair, Intelligence and Security Committee

By email

18 June 2018

Dear Dominic,

PARSONS GREEN

On 28 March the Home Secretary's predecessor committed to write to the Home Affairs Select Committee to provide further information on Ahmed Hassan's interaction with the police and Home Office prior to him detonating an explosive device on the London Underground at Parsons Green on 15 September 2017.

This letter sets out a timeline of key events of AH's case (agreed by the Home Office, police and Surrey County Council) and a summary of key recommendations and action taken on those recommendations coming out of an internal review into the case commissioned by the police and Surrey County Council (SCC).

The Home Secretary is confident that the measures outlined here, along with efforts already in train, will help to ensure that Channel panels around the country are equipped to address vulnerabilities and manage risk linked to the evolving terrorist threat.

Timeline of events

In October 2015 Ahmed Hassan (AH), an Iraqi national, was identified by Surrey Police in Egham, Surrey as having entered the UK illegally. As he claimed to be 16 years old he was treated as an Unaccompanied Asylum Seeking Child (UASC) and taken into the care of SCC Social Services, who contacted the Home Office Asylum Intake Unit to request an appointment to register his claim. Although AH had previously travelled through Italy on his journey to the UK it was not possible to take Third Country action (through the Dublin Treaty) as he was a minor.

He failed to attend an initial screening interview in November 2015. In his rescheduled screening interview (18th January 2016), AH stated that he was taken by force by ISIS but that he was not told at any point to do anything in Europe in their name. Following this interview, the details were provided to SCC who, on assessing the risk, referred to local Police Prevent Officers from Counter-Terrorism Policing South East (CTPSE).

CTPSE conducted a gateway discussion including known intelligence and an assessment of the risks and vulnerability. This concluded that AH was suitable for Prevent support and in February 2016 AH was discussed at a Channel meeting following which a vulnerability assessment (using a standard tool known as the Vulnerability Assessment Framework, or VAF) was conducted.

In a statement in support of his application for asylum (dated 7th March 2016), AH stated that he was taken by ISIS who talked to him about his duty to fight against the non-believers, and that he was forced to watch executions. In his second asylum Interview (June 2016), AH claimed he had been subjected to intimidation in Iraq by way of threats towards his family. He also described exposure to acts of violence and murder, and disclosed details of ongoing mental health issues.

The first formal Channel Panel for AH took place in June 2016. Existing support / protective factors included stable foster care provision in Sunbury, mental health support and commencement on a Head Start Education Programme at college. The Channel Panel decided that these existing protective factors were likely to be sufficient, and agreed to monitor his progress.

Consent for AH to take part in the Channel process was given by Surrey County Council. This is usual practice for minors without a legal parent or guardian. Social workers made AH aware that he was in the Channel process.

There were a total of nine formal Channel Panel discussions of AH at varying intervals between June 2016 and September 2017, although no Channel Panel meeting took place between January 2017 and June 2017.

There were episodes of AH going missing from home in April, August and December 2016. 'Missing from home debriefs' were conducted to a professional standard. However, the police Prevent officers, and therefore the Channel Panel, did not fully consider these absences further in the context of AH's vulnerabilities.

The Channel Panel also did not clearly resolve questions they had over AH's mental health treatment / support plan, or the outstanding matter of whether all his suspected mental health conditions had been diagnosed. As such, the relationship between AH's mental health and other vulnerabilities was not clear to the Channel Panel.

There was positive support via SCC Children's Services and through the foster care provided; however, the Channel Panel was unable to establish routine Children's Services attendance and reporting to a satisfactory level at the Channel Panel in order to adequately understand any risks from this important aspect of his care.

There was positive support and involvement at Channel Panel meetings from key workers involved in his education and academic development.

Throughout this time there was an ongoing asylum process. The Channel Panel did not have full visibility of the asylum process, and did not directly contact the Home Office regarding their concerns about perceived delays in assessing his claim.

The VAF was updated in August 2016 with little increase in his vulnerability or potential risk.

Police Channel practitioners spoke with AH on two occasions, in August and November 2016. These meetings did not raise any additional concerns about AH's risk of becoming involved in terrorism. Police left the November meeting with the impression that AH was making positive progress. However, concerns were raised by a Channel Panel member in January 2017 based on AH's demeanour and behaviour.

There was an apparent lack of a formal, documented plan to manage and mitigate AH's vulnerabilities and associated risks. At no stage did the panel request support from a Home Office approved Intervention Provider (who exist to provide specialised mentoring to address the issues around an individual's radicalisation), as there was a greater emphasis on other forms of support, including provision of constructive activities.

AH's positive progress at college was the main focus of the Channel Panel, and was considered a significant protective factor. Other concerning events and behaviour involving AH (such as AH going missing from home, and ongoing mental health issues) in some instances were not clearly shared or picked up on by the wider Channel Panel members for further exploration, challenge or intervention. There was a consensus that the case should remain in Channel. However, no violent ideology was confirmed. The Channel Panel were unable to establish a holistic overview taking into account the entirety of AH's turbulent background, mental health concerns, and ongoing behaviour and remarks.

The final Channel Panel took place on the 5th September 2017. Considering the ongoing vulnerability assessment and intelligence update, the Channel Panel was in the process of considering closure of AH's case.

Recommendations

The internal review commissioned by police and SCC identified a number of learning points and recommendations. Additional work, and information that came to light during the trial, has helped to develop some of the review findings and recommendations. A summary of the consolidated recommendations is provided below, grouped into themes, and with action taken in response. Following completion of the review at the end of December 2017, police, SCC, and the Home Office have followed up at local and national level to take forward recommendations alongside policy changes which were already in train. Taken together, these are designed to ensure that vulnerabilities and risks surrounding individuals such as AH are fully addressed in future.

Recommendations around immigration and asylum cases within Channel

Recommendations: Relevant immigration staff should have appropriate understanding, skills and training around intelligence collection, security, and reporting protocols; and timelines for processing asylum applications in relation to UASCs who are engaged in Channel should be reviewed.

In addition, learning and understanding in relation to the particular issues of dealing with UASCs in Channel should be shared with all Channel Panel Chairs. This should cover, among other things: the role and remit of immigration interviews, intelligence sharing and timescales; an understanding of the asylum application process; the assessment of age; and the sharing of

common or emerging 'back stories' or themes in the accounts of UASCs, including learning around 'disguised compliance'.

Action taken: A review of existing CT and Prevent training provision to staff in Asylum & Intake and casework (including the National Asylum Intake Unit) will take place to improve awareness of factors to identify in relation to radicalisation, and will emphasise the need for prompt referrals to CT police. Improved processes are being developed to support the identification of the immigration status of individuals referred to Channel. This will help identify where an immigration presence on the Channel Panel could help identify vulnerabilities, including mental health issues. This is particularly pertinent for Channel Panels seeking advice on managing the vulnerabilities of UASCs.

It is reasonable to observe in hindsight that uncertainty around AH's immigration status, combined with other events and developments, was not given due regard at several points along the Channel process. Part of the solution is the creation of a single point of contact for Prevent practitioners and immigration officials to contact Home Office Immigration teams regarding CT related enquires. This has been done and Channel Panel Chairs have been informed so they are able to access the immigration system directly, should an immigration issue arise.

Recommendations around mental health representation at Channel Panels

Recommendations: A relevant mental health practitioner should attend all Channel Panels where mental health concerns have been identified, and steps should be taken to raise awareness of Prevent and Channel among mental health professionals (which should include guidance on what information can be shared whilst respecting the needs of patient confidentiality).

Action taken: Mental Health Guidance, published in November 2017, makes it clear that there is an expectation of mental health representation at Channel Panels either in a standing role or a care advisory role. It sets out processes to ensure timely access to mental health support where a suspected mental health need is identified by Channel Panels or Prevent police. Regional NHS Prevent Coordinators are working with local services to implement this. The Home Office funds regional health coordinators to provide support and facilitate engagement.

NHS England published an Information Governance policy in September 2017 for Prevent which includes up to date information sharing protocols and an agreed Prevent referral process.

The Office for Security & Counter Terrorism (OSCT), working with NHS England, has also produced specific e-learning for mental health practitioners. This was published in November 2017.

Recommendations around using Multi-Agency Safeguarding Hubs, and quality assurance of Prevent and Channel delivery

Recommendations: Where Multi-Agency Safeguarding Hubs (MASH) exist, they should lead delivery of Channel across all local stakeholders. There should be quality assurance of how the Prevent duty and Channel are being delivered, and sharing of good practice. Quality assurance could include dip sampling or peer reviews. Exit interviews for subjects completing the Channel process should be considered.

Action taken: While SCC's positive experience of transferring responsibility for Channel to its MASH will be shared with other Channel Panel Chairs, we note that not all MASHs operate in the same way, and we will continue to allow individual local authorities flexibility to determine the most appropriate governance structure for Channel in their area. OSCT is currently considering, alongside its partners in the police, options for quality assurance of Channel processes to support the improvement of Channel delivery, in addition to the current programme of peer reviews.

Recommendations around police management of risks within Channel cases

Recommendations: All risks and vulnerabilities relating to a live Channel case must be properly assessed, with outcomes clearly recorded on the Channel case management information system. Guidance and training should reflect, in particular, the need for awareness of how CT risks can escalate within Channel cases. CTPSE should review its processes around handling Prevent Case Management information, and their staff should have the highest collective understanding of the vulnerability and risk information which Prevent staff managing cases need to be aware of. VAFs should be regularly updated and Channel Panel members updated with changes in CT risk. National guidance should be refreshed to ensure that key areas are understood, particularly in relation to: the timeliness of meetings; the roles of police Channel practitioner, supervisors and line managers, intelligence management, assessment and review; information sharing; proactive management of actions, enquiries and interventions; and completion of VAFs.

Action taken: Police play a vital role in identifying changes to terrorism-related risk posed by individuals and advising Channel stakeholders where risk has escalated. Additional measures to support police in this role are being delivered this year. As part of a wider effort to standardise Prevent Case Management (incorporating learning from this case), the police have introduced new information handling and case management processes, as well as training for the entire police network. Additional training on vulnerability assessments will be given to all police officers with responsibility for managing Channel cases. New case management guidance and training reflect all the learning points coming out of this case. Within CTPSE, a regional learning review workshop will help to develop standard operating procedures in CTPSE regarding the referral, assessment and information sharing process as identified within the learning review.

Recommendations around awareness and training of social workers in Surrey

Recommendations: All social care staff and managers should fully understand their role in relation to the Prevent statutory duty (under the Counter-Terrorism and Security Act 2015); the purpose and remit of Channel; and the need for full support and involvement at Channel Panels. Training should include the signs of radicalisation, issues around UASCs, and should increase confidence to make constructive challenge at Panels.

Action taken: Surrey County Council have implemented changes to manage Channel cases within the existing MASH structure, which includes social services.

Recommendations around training for Channel Panel Chairs

Recommendations: Tailored induction and training for Channel Panel Chairs should include minimum standards for Panel meetings, with templates for agendas, and sharing of successful case studies. The roles of Intervention Providers should be clarified and chairs should gain a greater understanding of the usefulness of interventions even where a clear ideological theme may not always be entirely clear. Good practice and experience should be shared, including in dealing with suspected 'disguised compliance'.

Action taken: National Channel Practitioners Guidance was not fully followed in this case with regard to record keeping, frequency of vulnerability assessments and intelligence developments along with the regular Channel Panel meetings. Channel Panels will be reminded of the need for structured support plans in each case, and the need to regularly review progress in open cases. The Home Office has issued templates for Channel Panel meeting agendas and minutes to assist in more consistent record keeping. A new e-learning package has been designed to enhance training on offer for Channel Panels. This includes detail around support required from partners, and expectations of sharing of information around the vulnerable individual in question to ensure they receive appropriate support. An ongoing programme of work to pass some Channel functions from police to local authorities will incorporate this training.

This case emphasises the need to manage Channel cases in a timely fashion. Statutory Channel guidance suggests that good practice is for:

- Statutory partners to provide relevant information to police within ten working days of receiving a request;
- Channel Panels to discuss ongoing cases on a monthly basis;
- Cases to be reassessed at least every three months.

Additional police guidance recommends that the first Channel Panel to discuss a case should take place within 20 working days from receipt by the relevant police team.

OSCT are considering whether a checklist could be developed to assist Channel Panel Chairs manage the exit process and ensure that identified vulnerabilities have been addressed successfully.

OSCT will make clear to Channel Panel Chairs that mentoring from approved Intervention Providers can have clear benefits even when it is difficult to identify a distinctive ideological theme, and that they should err on the side of caution when deciding whether or not to appoint one.

Yours sincerely,

Sir Philip Rutnam Permanent Secretary

ANNEX C: LIST OF WITNESSES

Ministers

HOME OFFICE

The Rt Hon. Sajid Javid MP – Secretary of State for the Home Department

Other officials

Officials

SECURITY SERVICE

Mr Andrew Parker − Director General, MI5

Other officials

METROPOLITAN POLICE SERVICE

Commissioner Cressida Dick

Other officials

ANNEX D: CODE WORDS

In some instances in this Report we have substituted a code word where it has been necessary to refer to the name of an operation, in order to protect classified information. No significance is intended by, nor should be inferred from, the matching of code words to the real operation names they have been substituted for.

AGAPANTHUS ..... ***

BEGONIA ..... ***

CLEMATIS ..... ***

DAFFODIL ..... ***

ECHINACEA ..... ***

FREESIA ..... ***

Operation E ..... ***

CCS0818342688
978-1-5286-0861-9