2017 TERRORIST ATTACKS
MI5 AND CTP REVIEWS

IMPLEMENTATION STOCK-TAKE

UNCLASSIFIED SUMMARY OF CONCLUSIONS

by

DAVID ANDERSON

(LORD ANDERSON OF IPSWICH K.B.E. Q.C.)

11 JUNE 2019

EXECUTIVE SUMMARY

- This is the unclassified summary of a stock-take of the progress made by MI5 and Counter-Terrorism Policing (CTP) in implementing the recommendations arrived at in the Operational Improvement Review and Post-Attack Reviews of 2017. It summarises progress to 31st January 2019 and looks in greater depth in some key areas: use of data, management of closed subjects of interest (CSOIs), multi-agency centre (MAC) pilots, and non-Islamist extremism.

- Both MI5 and CTP were conscientious and frank in providing me with the documents and briefings required. I was able to meet and question several dozen security officials, police officers and others, including the senior management of each organisation.

- Implementation has been tackled with energy and commitment. As of 24 January 2019, 85% of the 104 recommendations were complete (63%) or on track for delivery (22%). With possible very limited exceptions the recommendations were forecast to be complete on schedule, by Q4 2019.

- Good progress has been made for example on data discovery projects, CSOI management and non-Islamist terrorism. Positive results have been noted from some of the reforms, but it has not yet been possible to make an authoritative assessment of their overall benefits or of any opportunity cost.

- Obstacles to delivery remain, notably in the fields of data, information management and multi-agency interventions. Progress on Prevent data-sharing has been delayed while officials across government work up a proposal for ministerial approval. The most serious deficiencies, where daunting challenges persist, relate to CTP's data capabilities. The MAC pilots have required much effort for (so far) limited reward, but their extension to Q1 2020 should enable an informed judgement to be reached as to how the MAC principles can best be deployed.

- MI5 and CTP are committed to operating in a legal and ethical manner. Both the Home Office and external oversight bodies (notably the ISC and IPCO) should however continue to check that their activities remain within legal and ethical bounds as technology develops, particularly as regards the use of data.

- Though it will never be possible to prevent every attack, the measures being taken will, in my opinion, strengthen the existing ability of MI5 and CTP to stop most of them.

CONTENTS

1. INTRODUCTION

1.1 This stock-take assesses the position as of 31st January 2019 and was effectively finalised in mid-February 2019. It does not take account of any later developments.

Background to this report

1.2 In the months after the 2017 terrorist attacks in London and Manchester, the Security Service **[MI5]** and Counter-Terrorism Policing **[CTP]** made a series of detailed and in some respects radical recommendations for operational improvement. Summarised in a capping document and presented to the Home Secretary in November 2017:

a) seven post-attack reviews **[PARs]** exhaustively examined and drew lessons from the way in which intelligence was handled prior to the Westminster, Manchester Arena, London Bridge and Finsbury Park attacks of March-June 2017; and

b) an operational improvement review **[OIR]** identified operational changes to improve the future performance of MI5 and CTP.

1.3 Highly classified and extending to some 1150 pages, the nine reports constitute:

a) one of the most detailed examinations ever conducted of the UK's counter-terrorism machine; and

b) a blueprint for its operational reform.

1.4 I was closely involved in the preparation of those reports, having been asked by the then Home Secretary (Amber Rudd MP) to provide independent assurance that the right questions had been addressed and the appropriate conclusions drawn.[1] To that end:

> "I embedded myself for part of every week in Thames House and New Scotland Yard, where I attended internal meetings, reviewed drafts, teased out detail, challenged assumptions, called out complacency,

[1] I was at that time (and remain) a barrister in independent practice, with developed vetting security clearance originally granted for my work as Independent Reviewer of Terrorism Legislation from 2011 to February 2017. In July 2018 I was introduced to the House of Lords as a cross-bench "People's Peer", on the recommendation of the independent House of Lords Appointment Commission.

> drew attention to omissions, arbitrated differences and occasionally counselled greater boldness."[2]

1.5 My assessment of the MI5 and CTP reviews was conveyed to the Home Secretary in November 2017, supplemented by a classified letter, and published in December. I concluded that "*the recommendations of the internal reviews appear well-founded and are likely to contribute positively to the UK's counter-terrorism effort*",[3] but added, on a cautionary note:

> "It has been known for large institutions to react to reviews by going through the motions, or digging defensive redoubts. Even when a window is opened to change, it can close again before long. … The lasting impact of the OIR, and the other recommendations for future change, will depend on their effective implementation."[4]

It remained to be seen, therefore, whether good intentions forged after the terrorist atrocities of 2017 would translate into future action.

1.6 With such considerations no doubt in mind, the then Home Secretary asked me by letter of 30 January 2018 (Annex 1) to provide an independent stock-take of progress in implementing the recommendations of the OIR and the PARs, to be copied to the Prime Minister and to the Intelligence and Security Committee of Parliament **[ISC]**. That stock-take, covering progress to the end of January 2019, was completed in February and provided to the current Home Secretary, Sajid Javid MP, in March 2019.

1.7 I was also invited to prepare an unclassified summary of my conclusions for public use, containing no information that could prejudice national security or any criminal prosecutions or inquests relating to the 2017 terrorist attacks. That summary is contained in this document.

The limits of transparency

1.8 Parliament and the public have a strong and legitimate interest in understanding why counter-terrorism powers are said to be necessary,

[2] D. Anderson, *Attacks in London and Manchester, March – June 2017: Independent assessment of MI5 and Police internal reviews* **[Anderson I]**, December 2017, Foreword. The nature of the exercise, for which I had a degree of expert assistance, is further explained in chapter 4 of Anderson I.

[3] Anderson I, 5.19.

[4] Anderson I, 5.3-5.4.

how they are interpreted, and in broad terms how they are used. Such knowledge is a prerequisite for informed, democratic consent to the laws that govern covert activity, and is particularly important when new laws are being introduced or debated.[5] No-holds-barred scrutiny by security-cleared oversight bodies is an essential supplement to such knowledge, but not a substitute for it.

1.9 Where operational matters are concerned, however, transparency has its limits. Any published information is liable to be carefully read, not just by the interested public but by terrorists and hostile state actors who will seek to exploit any knowledge they can glean from it of the operational strengths and weaknesses of their opponents. Oversight bodies must continue to see everything, and to make their conclusions available to the public so far as considerations of national security allow. But to disclose information from which sensitive tradecraft can be inferred risks hindering the security services in doing their vital job, and should be contemplated only where there is a sufficiently compelling reason in the public interest.

1.10 The purpose of the OIR and the PARs was not to bring about change in the law but rather to build on the lessons of 2017 by improving the operational effectiveness of MI5 and CTP. Such were the national security concerns surrounding these internal reviews that I was not permitted even to set out their recommendations (save in broad summary) in my report of December 2017. The ISC in its own published report of November 2018 similarly made very limited reference to the detailed content of the OIR and PARs, despite having been provided with them in their entirety.[6]

1.11 I have therefore been constrained by considerations of national security in finalising this public summary of my stock-take. One of the areas of implementation on which I particularly focused was (though it is governed by clear laws) considered so sensitive that it could not be referred to at all in a public document.[7] Others can be referred to only

[5] This was a theme of a number of my previous reports, including *A Question of Trust* (2015) and *Report of Bulk Powers Review* (2016).

[6] ISC, *The 2017 Attacks: What needs to change?* HC 1694, November 2018 **[ISC 2018 Report]**. The ISC did however commend MI5 and CTP "*for taking the initiative in conducting their own, very thorough, reviews*": para 2.

[7] Cf. section 8 of the ISC 2018 Report, which consists only of a series of asterisks.

in outline. However, aware of the dangers of excessive self-censorship, I submitted a relatively full version of this unclassified report and have left it to others – as I am obliged to do by my letter of instruction – to make such further redactions as have been judged necessary in the interests of national security.

1.12 I hope that this summary may give the reader a sense for the scale and significance of the changes that have followed the 2017 attacks, and of what I have found to be the commitment of MI5 and CTP to seeing them through.

Terminology

1.13 I have sought to ensure that the key terms and processes used in intelligence and counter-terrorism work are sufficiently explained for the purposes of this summary: but Annex 2 elucidates the various acronyms used in the report, and further assistance may be found in my report of December 2017.[8]

[8] See in particular the definitions of key terms used by MI5 in Anderson I, 1.18-1.27, and the explanation of MI5 investigative processes, updated from a similar account in a 2014 report of the ISC, at Annex 5 to Anderson I.

2. THE RECOMMENDATIONS

2.1 The OIR and PARs produced not only 650 pages of text and 500 pages of annexes but a total of 126 recommendations, later consolidated into 104.

2.2 The 66 recommendations in the OIR are grouped in 10 chapters as follows:

a) Triage, leads and prioritisation

b) Information management

c) Management of closed subjects of interest **[CSOIs]**

d) Lone actor casework

e) PREVENT

f) Multi-agency interventions

g) Data

h) Research, innovation and international engagement

i) Domestic extremism

j) Resourcing.

2.3 The remainder of the 104 recommendations come from the PARs. They were made by MI5 on an attack-specific basis and by CT Policing on a cross-review basis.

2.4 The PAR recommendations related to subjects ranging from a variety of process improvements to the use of police powers for border interventions, the exploitation of intelligence opportunities in prisons and police engagement with communities.[9]

2.5 Previous terrorist attacks have been the spur for major systemic change: notably the digitisation of information after 9/11, and the creation of the

[9] Twelve strategic themes extracted from the PARs and set out in the capping document are reproduced in Anderson I, 3.23.

regional counter-terrorism **[CT]** network after 7/7. The 2017 attacks have in turn given urgency and operational direction to further strategic developments. Of these, three stand out as major step changes:

a) an enhanced role for big data across the full spectrum of risk, from initial leads through priority investigations to closed subjects of interest;

b) an intensification of partnerships across the UK Intelligence Community **[UKIC]** and between MI5 and CTP, coupled with the wider sharing of intelligence with neighbourhood policing, local authorities and others; and

c) an application to other forms of terrorism, notably extreme right-wing **[XRW]** terrorism, of the threat assessment and operational tools developed to counter the threats from Northern Ireland-related terrorism **[NIRT]** and Islamist terrorism.

2.6 As explained below, it is those step changes on which my stock-take was particularly focused.

3. CONDUCT OF THE STOCK-TAKE

3.1 A comprehensive audit of progress against each of these recommendations would have required a great deal of time and a range of specialised expertise not available to me, notably in data science and in the management and evaluation of public sector projects. Internal governmental mechanisms exist in order to verify that resources are being wisely spent.[10] The view was however taken that there could be value in an external stock-take of general scope, aimed at verifying whether the good intentions of 2017 were being translated into sensible action. I was not offered a team to assist with that task, and did not request one.

3.2 In performing the stock-take, my objectives were to:

a) examine whether MI5 and CTP have approached the task of implementation in the right spirit (i.e. without digging the defensive redoubts or closing the windows referred to 1.5 above);

b) record the nature and quantity of the work that has been done, and continues to be done, in order both to implement the recommendations and to evaluate progress; and

c) comment, to the extent possible, on the quality of that work and on any lessons that it may be possible to draw from it.

3.3 As part of that work, I kept an eye on progress across the whole range of the recommendations, in particular (from April 2018) via the six-weekly meetings of the OIR Oversight Board **[OIROB]** and a regularly updated tracker spreadsheet on which progress on each recommendation was recorded. In addition, and with the consent of the Home Secretary, I decided to apply more intense scrutiny to certain priority areas. Those that can be publicly discussed are use of data, management of closed subjects of interest, multi-agency centre pilots and domestic extremist terrorism.

3.4 I chose those topics because of their central importance:

[10] In particular, UKIC has a federated internal audit team and CTP is audited by HMICFRS

a) Between them, they cover the three aspects of the OIR described as step changes: exploiting data, multi-agency engagement and domestic extremism **[DE]**.[11]

b) The first three topics are of direct relevance to the recurring issues identified in the ISC 2018 Report, referred to at 1.10 above.

3.5 Whilst there was some coverage of those topics (save for domestic extremism) in the ISC 2018 Report, the ISC also devoted attention to a number of other topics, which I did not seek to replicate in detail.[12] The ISC has requested quarterly updates on progress, and will continue to provide oversight across the range of security and intelligence and agency activity as, within its remit, will the Office of the Investigatory Powers Commissioner **[IPCO]**.

3.6 Both MI5 and CTP were conscientious in providing me with briefings and documents relevant to my task. They were understandably anxious to ensure that I saw their work at the most advanced stage possible; and for that reason, the in-depth briefings or "*deep dives*" that were provided for me in each of my priority areas – intensive sessions with a total of several dozen security officials, police officers and others – took place for the most part in the second part of November and in December 2018. These were supplemented by a range of further documents and by interviews in January 2019 with the Director General of MI5 (Andrew Parker) and his Deputy and with the Metropolitan Police Commissioner (Cressida Dick QPM) and National Coordinator for Counter-Terrorism (ACC Neil Basu QPM).

3.7 My classified report was addressed to the Home Secretary and copied to the Prime Minister and to the ISC as noted in my letter of instruction. I also requested that it be copied to the Investigatory Powers Commissioner so as to ensure that the various bodies entrusted with oversight have the fullest possible view of current and proposed changes.

[11] Anderson I, 3.38-3.46.

[12] E.g. extremist material online (section 4), extremism in prisons (section 5), vehicle hire (section 6), chemicals and explosives (section 7), travel (section 11), disruptive powers (section 12), families and Prevent (section 13) and protective security (section 14).

4. OVERALL PROGRESS

Other initiatives

4.1 Implementation of the OIR and PARs is not an isolated exercise. Largely tactical rather than organisational in nature, and due to be completed by November 2019, the OIR is being given effect in the context of a number of wider-ranging and longer-lasting initiatives. As well as the CONTEST 3.0 counter-terrorism strategy, relaunched in June 2018, these initiatives are:

a) ***CT Step Up***, an ambitious and in some respects experimental strategy, based on continuous learning and innovation to unlock the value of data for threat discovery,[13] knowledge-sharing and intervention, which will run at least until 2021 and probably until 2023;

b) ***A Shared Corporate Services Organisation*** hosted by MI5 for UKIC, aimed at more integrated corporate services to support stronger joint missions between MI5, MI6 and GCHQ; and

c) The proposed co-location of London-based elements of CTP and MI5 by 2023.

4.2 Expectations for each of those initiatives are high. As MI5 told the ISC:

> "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".[14]

Non-integrated systems, causing difficulties in exchanging and processing each other's data, are indeed the weak spot in what is otherwise an exceptionally (by international standards) close and harmonious working relationship between MI5 and CTP. Closer integration between CT partners, coupled with a step change in the use of data (where it is acknowledged that there are lessons to be learned from the private sector), are seen as the key to future success in disrupting not just terrorism but hostile state activity. Integrated systems are the ideal, but coverage is only partial and progress can be slow (as

[13] "*Discovery*" in this context means the work that is done to detect and better understand threats, whether from persons not currently on MI5's radar, live SOIs or closed SOIs.

[14] ISC 2018 Report, para 139.

in the case of a major CTP database, which after many years of development is scheduled to complete its roll-out in March 2019). The proposed co-location (4.1(c) above) would bring compensating synergies, as already seen in regional Counter Terrorism Units **[CTUs]** and Counter-Terrorism Intelligence Units **[CTIUs]** where CTP and MI5 work alongside each other.

Tracking implementation

4.3 Each of the 104 agreed actions has an owner who is responsible for its completion, at the latest, by November 2019. Delivery owners (MI5, CTP, the Home Office or a combination) report progress to the OIROB via the OIR secretariat. They provide a narrative comment on progress, the current red – amber – green – blue status of each recommendation,[15] and the anticipated status in the next cycle. A tracker in spreadsheet form records current and previous status so that progress can be monitored. Traceability of decision-making and approach is provided by the records of the OIROB, which comprise the agenda, the minutes and the version of the tracker provided for the meeting.

4.4 At the granular level of verifying whether action has been taken to implement the recommendations, the tracker is useful. Each recommendation is listed, its "*owner*" identified, a colour (blue, green, amber, red) assigned to its progress and a short delivery narrative given. As of 24 January 2019:

a) 85% of all recommendations were complete (blue, 63%) or on track for delivery (green, 22%).

b) The great majority of MI5-owned recommendations were blue; CTP-owned recommendations were blue and green in equal number.

c) There were obstacles to delivery (amber) in the OIR fields of data, information management and multi-agency interventions, and in relation to a few post-attack review points.

d) The only two recommendations marked red (5.6 and 5.7) related to Prevent data-sharing. Since officials are currently working on a

[15] Blue = delivery is complete; Green = delivery is on track; Amber = some obstacles to delivery exist; Red = significant obstacles to delivery exist.

proposal on which they will seek Home Secretary approval, I say no more about the issue in this report.

e) It was forecast that all recommendations would be blue on schedule, i.e. by Q4 2019. However, of the 15% not currently on track, some continue to present significant challenges.

The picture is thus a generally positive one in the mechanical terms of translating recommendations into action. In many cases, however, the nature of the recommendations is not such as to guarantee that their implementation will make the UK safer. Accordingly, I encouraged MI5 and CTP to keep under review the benefits and any possible drawbacks of their recommendations, and to show me their evaluations of whether such benefits were still expected to materialise.

Internal evaluation of progress

4.5 I was told that the standard against which the OIR was held to account was "*whether the UK will be safer as a result of the implementation of the 104 recommendations*".

4.6 Completed terrorist attacks are fortunately so uncommon, in the UK and across the western world, that the impact of new policies and techniques on the frequency of attacks is impossible to measure with confidence. Yet some evaluation of progress is plainly essential. The OIR recommendations were arrived at under very significant time pressure, in the immediate aftermath of serious attacks and at a time of enhanced threat. Effective implementation requires not just the ticking of boxes but some sort of evidence-based assessment that the direction chosen in 2017 remains a sensible way forward into the 2020s and beyond.

4.7 For this reason, and because I did not myself have the necessary tools or capabilities fully to evaluate the impacts and cost-effectiveness of what is being done, I impressed on CTP and on MI5 my interest in seeing robust internal mechanisms for evaluation.

4.8 I saw the agenda and minutes of OIROB meetings from April 2018 to January 2019, and attended a number of those meetings. I asked whether further relevant material was presented to the MI5 Board, and was given material relating to use data that had been prepared for this purpose. Had time permitted I would have liked to speak to a non-executive director of MI5, but it did not prove possible to arrange this in the couple of weeks between my suggesting it and the submission of this report.

4.9 I was also presented:

a) in November 2018 with a written summary of progress, which I was able to interrogate and discuss with its author; and

b) in February 2019 with slides on OIR Delivery Progress and the final versions of a series of Benefit Statements which set out in relation to each chapter of the OIR and some aspects of the PARs a summary assessment of progress against the recommendations and of the benefit or anticipated benefit from their implementation.

4.10 The Benefit Statements are useful summaries of progress but do not amount to an authoritative assessment of the benefits, and any possible drawbacks, of the far-reaching reforms on which MI5 and CTP have embarked, partly in response to the recommendations of 2017. Still less do they seek to assess the opportunity cost of reform, in terms of identifying benefits foregone as a consequence of resources tied up in implementing recommendations.[16]

4.11 It may be that it is too early for such an exercise, or that the necessary methodologies are lacking. Many of the OIR and PAR recommendations are so self-evidently sensible that there can be little doubt as to their worth, even if it cannot be precisely measured. Nonetheless, particularly in areas where high ambition is matched with high cost, the bodies entrusted with regular oversight of CTP and MI5 (e.g. the ISC, Home Affairs Select Committee, Investigatory Powers Commissioner and National Audit Office), will need to remain vigilant.

4.12 No less important is the need for legal and ethical vigilance. Some aspects of the recommendations – for example, increased data-sharing and the improved analysis of bulk personal datasets in order to identify

[16] See, e.g., Anderson I at 5.18, raising but not answering the question of whether the resource necessary to investigate the increased number of *leads* generated by better use of data, multi-agency engagement and research and innovation might be more usefully devoted to *priority investigations*.

and enhance the understanding of threats from individuals – touch on areas of some potential public sensitivity.

4.13 The Independent Digital Ethics Panel for Policing **[IDEPP]** provides a useful sounding-board for discussion with outside experts about ethical issues arising out of the exercise of police powers. In my Bulk Powers Review of 2016, I decided against recommending an equivalent body to be constituted for the security and intelligence agencies, noting as I did so that the Investigatory Powers Commissioner, assisted by the Judicial Commissioners at IPCO, is well equipped to provide his own leadership in this area.[17]

4.14 It is of course not for me to suggest how IPCO – or indeed the ISC, which has asked for quarterly updates on progress on implementation – should perform their functions. I hope however that the Home Secretary will choose to supply my report to the IPCO as well as to the ISC, and anticipate that both bodies, with the full cooperation of Government and of the Agencies themselves, will take such steps as they consider necessary to ensure the continuation of effective legal and ethical oversight as the nature of UKIC work evolves.

[17] D. Anderson, *Report of Bulk Powers Review* (Cm 9326, 2016), 9.27.

5. USE OF DATA

Summary of recommendations

5.1 These recommendations seek to improve the ability of MI5 and CTP to exploit data to detect activity of concern, particularly on the part of closed SOIs but also in relation to active subjects of interest **[SOIs]** and previously unknown individuals. This was described in Anderson I as the first of the three step changes to come out of the OIR. The two strands of this work were, as summarised there:

a) a ***better strategy for acquiring, analysing and sharing data across intelligence and policing***, for example through wider use of bulk personal datasets **[BPDs]** and by enhancement of existing tools; and

b) ***increasing cooperation with the private sector***, for example to improve the detectability and even the preventability of purchases of potential explosives precursors by would-be terrorists.

5.2 Many of the OIR recommendations on data are far-reaching, for example:

a) the development of an MI5 data strategy for the acquisition, sharing and analysis of data across GCHQ, MI6 and CTP, supported by Head of Data and Analysis at MI5;

b) consideration of how data can become a more central part of MI5's investigative process, so far as possible on a tri-agency and CTP basis;

c) a full information-gathering exercise by CT Policing across all police systems and databases;

d) the better understanding of capability gaps across the UK CT community for data analysis;

e) examining the possibility of CTP mirroring MI5 analytical structures;

f) the identification of capabilities and data needed to develop relevant behavioural triggers;

g) a process to ensure that leads generated from discovery work can be acted on in a coherent manner across the three agencies and CTP;

h) the speedy development of an improved "*SOI Radar*"; and

i) a strategic step change in the approach to data sharing.

5.3 More specific recommendations include the acceleration of a major CTP data sharing programme, work by the Home Office with MI5 to identify and investigate suspicious transactions relating to explosive precursors and initiatives for preventing the future use of hire vehicles as weapons including by use of financial data.

5.4 The 2017 attacks strengthened existing incentives for MI5 to make use of machine learning, artificial intelligence and behavioural analytics; to manage data outside its own systems; and to share data with others to maximise its benefit. For CTP, the most pressing problems are more basic ones: streamlining disparate systems; extracting the maximum value from their own data; and acquiring the capacity to act as a data bridge between UKIC and the law enforcement community.

Progress against recommendations

5.5 As of 24 January 2019, the RAG tracker (4.3 above) revealed a mixed picture. Of the 15 recommendations, eight were blue, and three were green. The remaining four were amber. The amber recommendations were owned by CTP or, in one case, by the Home Office and Department for Transport. Overall, MI5 is finding it easier than CTP to comply with the recommendations on data. MI5 considered however that the current level of investment would make it impossible for UKIC to achieve some of the milestones outlined in its 5-year vision and strategy.

Observations: MI5

Central objectives

5.6 As set out in the Recommendations and Benefit Statements, the blizzard of initiatives can seem difficult to comprehend, let alone to evaluate. Their key objectives are however coherent:

a) "***stepped-up radar***": using data to warn MI5 and CTP of emerging threats across the leads, live and closed spaces,[18] and to set "***tripwires***" that will notify a re-emerging threat;

b) increasing co-operation with the ***private-sector on data analysis;*** and

c) the ***sharing / federating of data*** across the CT community, for use across all their areas of work.

5.7 Central to the first two of those objectives is private sector partnership.[19] Commercial operators, including but not limited to the tech giants, are well ahead of UKIC in their capacity to acquire and analyse data in bulk. The hiring of a heavy vehicle or the booking of a flight may, in the light of other available intelligence, be useful and even potentially life-saving tripwires.

5.8 Private sector cooperation in intelligence work is not new: the law already requires financial institutions to provide suspicious activity reports, and airlines to provide passenger name records. What is now envisaged however is cooperation:

a) with a ***wider range of partners***;

b) ***using external technologies and capabilities*** (including cloud-based capabilities) as the default; and

c) based on state-of-the-art ***data science techniques***, including artificial intelligence, machine learning and predictive analytics.

Institutional change

5.9 Institutionally, the chief developments have been:

a) the launch of the ***Data and Analysis Strategy*** in January 2018 (MI5) and across UKIC (August 2018), and its principal elements;

b) the appointment of a ***Head of Data and Analysis***; and

[18] This convenient shorthand is explained in Anderson I at 1.19 (leads), 1.22 (live or priority investigations) and 1.26 (closed SOIs).

[19] Partnership with Government departments may also be important.

c) the launch of the ***MI5 Data Hub*** in March 2018 to identify the top strategic requirements for data, drive its collection or acquisition, and provide for its onboarding (i.e. ingesting: the stage between acquisition and analysis).

Other developments

5.10 In the classified version of this document I reported on:

a) the state of the various ***strategic relationships*** which MI5 enjoys with private-sector and Government partners;

b) progress on the joint MI5/Home Office plan to address the challenge of ***explosive precursor purchases***;

c) the experimental ***discovery projects***, based on the application of artificial intelligence and behavioural analytics, which sit at the core of the "*stepped-up radar*" which it is sought to apply to leads, SOIs and closed SOIs; and

d) developments in relation to ***data sharing*** with private sector, public sector and overseas partners.

Observations: CTP

5.11 On the policing side, the data picture is characterised by a number of major challenges, which are at various stages of being addressed. These relate to capabilities (particularly collection capabilities), technology (particularly around network connectivity), vision (particularly regarding strategic coordination with UKIC), disparate and sub-optimal systems, over-reliance on manual analysis of data and governance within CTP. Further problems highlighted to me during the presentation included recruiting data scientists and poor data standards.

5.12 On a more positive note:

a) There was news of progress on two long-term data consolidation projects which are considered to be basic building blocks for cooperation between CTP and UKIC: a major data-sharing programme (directed to task of consolidating police databases already held and standardising processes nationally) and a major database (which aims to create a national intelligence platform enable the sharing of intelligence across geographical areas and with UKIC).

b) A project aimed at enabling the sharing of data between the police National Secure Network **[NSN]** and UKIC was said to be on track for completion by late spring 2019.

c) CTP were appointing a Head of Data and Analysis to give clear leadership and resolve some of their governance issues.

d) It was hoped that physical colocation of MI5 and CTP would help compensate for the many practical difficulties in data-sharing.

Legal and ethical issues

5.13 Both MI5 and CTP are committed to operating within the law, and should have no incentive to stray into grey areas where costly litigation could place officers at legal risk and distract their organisations from their necessary work.

5.14 It is obvious however that developments in data-sharing and in discovery techniques (notably the increasingly sophisticated use of artificial intelligence and behavioural analytics to extract information from bulk datasets, alone and in combination) will require continuing legal and ethical review.

5.15 The most sophisticated deployments of such techniques are not practised by intelligence agencies or police but by private sector operators including tech companies and major retailers. The world depicted in the film *Minority Report* remains strictly fictional. However, UKIC aspires to learn from the private sector, and if possible to catch up.

5.16 Behavioural analytics is here to stay, and its techniques may be effective not just in refining the assessment of risk from existing leads and SOIs but in discovering new leads who would not otherwise have come to the attention of the authorities. Some indicators are geared to identifying immediate pre-attack behaviour, such as attempts to obtain firearms or researching attack methodologies. More general indicators – for example, personal frustrations or changes in baseline behaviour – may also have their place when applied to persons who are already under suspicion.

5.17 More controversial, however, should increasing automation render it cost-effective, would be the use of such general indicators across the population as a whole, or significant portions of it, with a view to identifying possible future threats. As UKIC came to acknowledge in the wake of the Snowden affair, strongly-held public concerns have the potential to damage the perceived legitimacy of vital bulk capabilities. Apart from a strong internal compliance and ethics culture, the best response to public concern is maximum possible transparency, consultation and strong ethical oversight.[20] I hope that the Home Office, drawing on the positive example of the Investigatory Powers Act 2016, will keep this well in mind – as, no doubt, will the ISC and the Investigatory Powers Commissioner.

[20] These were themes not only of my earlier reports *A Question of Trust* (2015) and *Report of Bulk Powers Review* (2016), but of the Investigatory Powers Act 2016 which followed.

6. MANAGEMENT OF CLOSED SUBJECTS OF INTEREST

Summary of recommendations

6.1 Perhaps the most intractable problem faced by MI5 in its recent counter-terrorism work is the SOI whose file is closed after a period of inactivity, but who then re-emerges as an active and potentially lethal threat.[21] The Westminster Bridge and Manchester attackers, Khaled Masood and Salman Abedi, fell into that category, as before them had the 7/7 bomber Mohammed Siddique Khan and the killers of Private Lee Rigby, Michael Adebolajo and Michael Adebowale.

6.2 The problem is exacerbated by:

a) the large number of closed SOIs; and by

b) the risks inherent in shifting resources from the 3000 or so live SOIs, who by definition pose the most immediate threat to national security.

6.3 The various recommendations of the OIR relate, among other things, to:

a) improving ***CLEMATIS/DAFFODIL*** (as it was referred to by the ISC):[22] a process devised by MI5 to identify activity of renewed intelligence interest conducted by closed SOIs, using targeted data exploitation and other automated techniques;[23]

b) the formulation and implementation of a ***revised strategy*** for the management of closed SOIs.

c) ***procedural changes*** to include CTP involvement in closure decisions, a specific focus when closing leads on referrals to Prevent or multi-agency interventions and new information management standards; and

d) the giving of ***incoming intelligence*** on closed SOIs the same status as intelligence on new threats.

[21] ISC 2018 Report, section 10, paras 170-189.

[22] ISC 2018 Report, paras 153-156 and 165-166.

[23] Anderson I, 2.38.

6.4 These recommendations overlap to a substantial extent with matters reviewed elsewhere in this report: including the use of data (section 5 above) and multi-agency pilot centres (section 7 below). The reforms in each of those areas have been motivated partly by the need to improve visibility of closed SOIs, and to improve the "*tripwires*" that, if appropriately set, may announce their re-mobilisation.

Progress against recommendations

6.5 Progress on each of these recommendations was graded either green or blue.

6.6 In the classified version of this report, I addressed the principal developments which include:

a) the creation of a dedicated "*closed*" team in MI5, working closely with CTP, and of a new ***"closure gateway"*** process, which:

(i) sets thresholds for closure, to promote consistency of approach;

(ii) assesses SOIs against those thresholds at the point of closure, with CTP as well as MI5 involvement;

(iii) checks that all reasonable steps have been taken to mitigate threat in the active space (i.e. while active investigation continues), before the focus shifts to managing residual risk in the closed space and detecting re-engagement and mobilisation;

(iv) ensures that Key Information Store **[KIS]** records (the intelligence "*files*" kept on open and closed SOIs) meet the required standard; and

(v) passes SOI "*ownership*" from the investigative team that owned the relevant Priority operation to the Region where the SOI is based, where it sits with MI5 and CTP partners;

b) an intention to expand these processes to include the management of non-Islamist closed SOIs, with CTP's National Operating Centre **[CTP-NOC]** providing an equivalent closure gateway;

c) the introduction of a ***new categorisation system for closed SOI***, based on evidence and insights from MI5's Behavioural Science Unit **[BSU]**, to improve recording and hence understanding of the risk posed by an SOI at the point of closure;

d) in place of the old Emerging and Residual Threat **[ERT]** process, which focused on threat disruption among a small number of SOIs, a more consistent ***risk mitigation model*** will see somewhat larger number of SOIs subject to regular checks, both automatic and manual, on Police indexes and local criminal records;

e) use of ***enhanced discovery capabilities*** to strengthen the "*radar*" around closed SOIs generally, easing the identification of potential re-engagement or mobilisation from within the closed SOI stable and improving the quality of data feeds, reducing data errors and causing a number of investigations into closed SOIs to be re-opened;

f) a ***manual update of SOIs' KIS records***, using data from a range of bulk personal datasets, and the embedding of new processes to ensure a higher quality of KIS record-keeping in future;

g) building capability that enables ***more efficient updating of KIS records***;

h) the routing of all ***unsolicited intelligence*** received on closed SOIs to a triage point where it is assessed in line with the standard Intelligence Handling Model **[IHM]** and, where it potentially meets the threshold for further investigation, joint assessment by CTP and MI5[24]

i) the piloting of the ***Multi-Agency Centres*** **[MACs]** referred to in section 7 below; and

j) continued refinement of the ***CLEMATIS/DAFFODIL*** process (6.3 (a) above).

[24] The IHM is the process for lead identification, assessment, decision-making and resolution, jointly developed since 2011 by MI5 and CTP and described in Anderson I, 1.20.

Terminology

6.7 In the light of the new categorisation, and the improved procedures for ensuring that new intelligence on closed SOIs is taken into consideration, the term "*closed SOI*" (or CSOI) could be considered anachronistic. When individuals cease to be part of a priority investigation and pass through the "*closure gateway*", active intelligence-gathering on them ceases, but intelligence interest in them does not.

6.8 Though the issue is of presentational more than operational significance, I advised that it might be more accurate to refer to at least the higher categories not as closed SOIs but as non-investigated or non-priority SOIs.

Conclusions

6.9 I was satisfied that the new mechanisms for handling closed SOIs represent an improvement over what went before in at least the following respects:

a) fuller consideration of the intelligence before a SOI is closed;

b) an end to the automatic closure of SOIs when the priority investigation with which they were associated was closed;

c) logical categorisation of the potential threats from closed SOIs, based on updated KIS files;

d) enhanced mechanisms for "*mitigating*" the threat, targeted to appropriate categories of closed SOIs; and

e) evaluation of new intelligence on all closed SOIs under the IHM, departing from the previous position in which unsolicited intelligence on closed SOIs could go untriaged and unread.

6.10 The enhanced investment in closed SOIs required a degree of cultural change from both MI5 and CTP. There has in the past been an understandable tendency to react with relief to the closure of an investigation and the SOIs associated with it, leaving hard-pressed investigators free to concentrate on the remaining (and aptly-named) priority investigations.

6.11 Without doubt, the fact that a number of recent attackers have been closed SOIs speaks powerfully in favour of stepping up the radar on that very large group. However:

a) The rigorous requirements for closure will place additional burdens on those investigating priority operations, and mean that some SOIs (and some priority investigations) will remain live for longer than would previously have been the case.

b) The new data-driven discovery mechanisms (referred to at section 5 above) have the potential to generate large numbers of leads on closed SOIs.

c) The requirement to triage such leads manually via the IHM, and to triage unsolicited reporting on all CSOIs, will inevitably require more resource from both MI5 and CTP: resource that if occupied on triage will not be available for priority operations.

d) Regional ownership of closed SOIs will also have resource implications, which were described to me as difficult to predict, for MI5 Regional Stations and CTP Partners.

6.12 My previous description of this dilemma was in the following terms:

> "[A] number of the recommendations (relating for example to use of data, to multi-agency engagement and to research and innovation) are likely to have as their effect an increase in the volume of leads. While this may be desirable in principle, the processing of more leads will logically require the transfer of resources from other activities, including perhaps priority investigations. Whether the quality of the extra leads will be such as to justify removing those resources from other areas of MI5's work is something of an imponderable, at least for me."[25]

6.13 That was not intended as a criticism of decisions taken in the OIR, nor is it a criticism of the faithful implementation of those decisions that have been in train since 2017. It does however bear out the need to keep the

[25] Anderson I, 5.18.

results of these positive changes, and the categories to which various mitigations are applied, under constant evaluation.

7. MULTI-AGENCY CENTRE PILOTS

Summary of recommendations

7.1 The principal recommendation under this head was to develop:

> "a new multi-agency approach to managing Closed Subjects of Interest … (and potentially other SOIs where appropriate), by 'breaking out' more information to a wider range of partners at national and local level, and establishing mechanisms for a joint approach to managing risk – with pilots beginning in November 2017, to be rolled out more widely if successful".

7.2 As will be clear from 6.6 above, the multi-agency pilots are just one aspect of the multi-pronged strategy, already described, for managing closed SOIs. Nonetheless, the principle of multi-agency engagement was considered so important as to constitute one of the three step changes identified in the OIR (the others being exploiting data and domestic extremism).[26] For that reason, I decided to conduct a "*deep dive*" into the MAC pilots, which took place over two days in London and in Birmingham.

Progress against recommendations

The MAC Process

7.3 MAC pilots have been set up, as recommended, with the aim of reducing the risk of closed SOIs engaging or re-engaging in terrorism. Five phases of the MAC approach are currently being tested:

a) identification of newly-closed high risk SOIs by MI5 and the preparation of their cases;

b) sharing by MI5 and CTP of data on the SOIs with other agencies liable to have contact with them, such as local authorities and other government departments **[OGDs]**;

c) enrichment of that data from the databases of multi-agency partners, including local authorities, and proposals by them for intervention;

[26] Anderson I, 3.37-3.46.

d) collaborative development of an integrated profile on each subject, based on a behavioural baseline assessment, and preparation of a draft management plan to safeguard the subject and address any risk; and

e) the delivery of a management plan, coordinated by a police-chaired multi-agency panel and potentially resulting in a wide range of disposals

7.4 The most radical part of the current approach is sharing SOI data with local authorities and OGDs, which redeems the OIR commitment of MI5 and CTP to allow knowledge derived from intelligence to be shared more widely beyond intelligence circles. Their reward for this openness should come, in principle, from the data enrichment that is contributed by multi-agency partners, ensuring that the personal profile and management plan are informed by the full range and depth of knowledge available to public authorities.

7.5 A MAC behavioural assessment results in a grading of Level 1 (minimal changes to baseline behaviour), Level 2 (the category most likely to be suitable for a multi-agency intervention) and Level 3 (extreme or worrying traits, which may warrant reference back to the IHM). So far, to the surprise of those to whom I spoke, only 10-20% of those who have gone through the process have been assessed at Levels 2 or 3.

Implementation

7.6 The implementation measures to date may be summarised as follows:

a) Three MACs have been established, in London (National Multi-Agency Centre **[NMAC]**), West Midlands (Regional Multi-Agency Centre **[RMAC]**) and the North West (RMAC).

b) Plans are being developed to work in areas outside the three pilot regions. The significance of London's classification as NMAC is that it could in future take cases from anywhere in the country (the so-called "*MAC in a box*"), whereas RMACs, which are not likely to be reproduced elsewhere, take their cases only from the region where they are situated.

c) The aim is to process both Islamist and XRW cases, though as shown by experience in the Midlands, the pilot is not currently structured in a way that that renders this feasible. CTP and MI5 are currently discussing how MAC might take such referrals, as the processes for their closure are developed.

7.7 The classified version of this report detailed the cohorts referred into the pilots, which have been extended to March 2020, and the steps taken to produce preliminary assessments, both internal and external, of their advantages and drawbacks.

7.8 The teething troubles experienced with MAC pilots have been such that the principal recommendation under this head was graded amber on the tracker. No one suggested that the MAC pilots were pointless: the principle of pooling and making accessible the sum of information available to the public authorities about a potentially dangerous SOI is clearly a desirable one, and the local authorities to whom I spoke in both London and the West Midlands were strongly committed to the MAC concept. As the representative of one London Borough put it to me:

> "It's about safeguarding and managing risk, harm and threat. We need to develop partnerships with these people and to have trusted relationships with them."

The amber grading reflects however the considerable practical difficulties in the way of making the MAC system work, particularly at scale and at speed.

7.9 Those challenges were explained in the classified version of this report. They range from difficulties in securing clearance to share information through to delays in securing information-sharing agreements with local authorities and the need to train personnel in producing behavioural assessments.

7.10 As to the delivery of management plans, some local authority representatives cautioned against unrealistic expectations of services such as mental health and community safety. It is not difficult to see how intensive interventions could assist in the management of closed SOIs; but against, what was described to me as, a background of widespread recent degradation of local services, such interventions may not be generally available, and there was a degree of reluctance in local authorities to prioritise closed SOIs at the expense of other citizens, or to take on the risk of any failure to do so.

Conclusions

7.11 There has been no backsliding in the commitment of MI5 and CTP to the MAC pilots, or for that matter of the local authorities who continue to participate in them. Impressive amounts of energy have been invested over more than a year into improving the assessment and safeguarding of the highest-risk closed SOIs by making available to multi-agency panels the full range of information held by agencies, police, government departments and local authorities.

7.12 The objective of bringing other sources of public sector information to bear on the management of CT risk is an obviously sound one. The practical difficulties in realising that praiseworthy objective are however substantial and any cost-benefit analysis will inevitably be influenced by the fact that current pilots have demonstrated that interventions may be applicable in far fewer instances than originally envisaged.

7.13 I observed openness of mind among all stakeholders as to the future of the MAC process. The feasibility of more data sharing on live SOIs prior to closure, and allowing for the abbreviation of the lengthy MAC phases, were two ideas that it was suggested to me might be usefully considered as part of any future evaluation. Other issues for the future are governance; retention and deletion policies; the balance between central and regional control; and the relationship with Prevent.

7.14 I welcome the extension of the pilot, by which time I anticipate that some teething troubles will have passed and a reliable evaluation of effectiveness should be possible. That evaluation should consider not only the functioning of the MAC pilots themselves, but their relative cost and effectiveness compared to the other mechanisms for handling closed SOIs outlined in section 6 above.

8. NON-ISLAMIST TERRORISM

Summary of recommendations

8.1 The nine recommendations concerning what was referred to as "*domestic extremism*" had two central elements:

a) transfer to the Joint Terrorism Analysis Centre **[JTAC]** of responsibility for the production of national terrorist ***threat assessments*** arising from DE work, employing common language, methodology and approach to that already used for Islamist extremist threats; and

b) greater ***MI5 involvement*** in the assessment of leads, in higher priority investigations, and in decision-making and resource allocation in all investigations relating to proscribed organisations such as National Action.

Taken as a whole, the recommendations aspire to ensure the equivalence of processes in analysing and dealing with all kinds of terrorism, irrespective of the ideology that inspires them.[27]

Terminology

8.2 One recommendation committed the Home Office to considering whether the International Counter-Terrorism **[ICT]** and DE labels are still fit for purpose and if not, in consultation with the CT community, to developing new ones.

8.3 "DE" is an amorphous concept, stretching from groups which currently pose no more than occasional public order concerns (animal rights, anti-fracking) to attack-planning by associates of the proscribed XRW terrorist organisation National Action. In practice, the "DE" most likely to reach the terrorism threshold is that promoted by the XRW, whose ideology is of white supremacy or neo-Nazism and which is to be distinguished from (but recruits from) the racist or anti-Muslim Far Right **[FRW]**.

[27] Anderson I, 3.43.

8.4 Both the ICT and the DE labels seemed to me manifestly deficient, for the reasons given in Anderson I.[28] In summary:

a) Islamist terrorism is often home-grown, just as right-wing terrorism can be international.

b) To describe even the most threatening non-Islamist activity as "extremism" may be read as signalling that it is taken less seriously than Islamist "terrorism".

c) ICT stands for international *counter*-terrorism and should not be used to refer to a form of terrorism.

More fundamentally, the categorisation of terrorism by its governing ideology might be seen as unnecessary for many (though not all) purposes, given similarities in the backgrounds and psychological profiles of both types of terrorist and in their modus operandi: a point pressed upon me by MI5's Behavioural Analysis Unit.

8.5 The problem is not solved by using the phrase "*Domestic Extremist Terrorism*" **[DET]** to denote domestic extremism which reaches the threshold for terrorism. Though a convenient patch, it does not address the unsatisfactory nature of the term domestic extremism.

8.6 The Home Office has played a constructive role in this debate. This may be seen from the June 2018 iteration of the CONTEST strategy, which moved deliberately away from the DE/ICT terminology in favour of referring to terrorism either generically or, where necessary, by reference to its governing ideology (e.g. XRW). But though my criticisms of the status quo are widely understood and shared in MI5 and CTP, as well as within the Home Office, revised terminology proved more difficult to agree.

8.7 At a workshop in December 2018:

a) All departments agreed to stop using the terms "*Domestic Extremism*", "*Domestic Extremist Terrorism*" and "*International Counter-Terrorism*".

[28] Anderson I, 3.46 and fn 44.

b) All departments agreed to move to using "*terrorism*" with the motivating ideology as a prefix.

8.8 That seems straightforward and sensible. However, the status of this recommendation remains amber. In that connection it has been noted that:

a) further work is needed to identify how the new approach would fit with operational processes and the public reporting of statistics; and that

b) there is as yet no parity of approach around thresholds, the current approach being a pragmatic one that enabled the best current capabilities to be placed on the cases.

8.9 It is to be hoped that the agreed public-facing terminology will so far as possible be carried over for internal purposes. I would add only that while thresholds for intervention should of course be determined on an operational rather than a legalistic basis, it is helpful to remember that terrorism is clearly defined in law by s1 of the Terrorism Act 2000 and that this definition should inform operational practice, for example in relation to the borderline between terrorism and hate crime.

Progress against recommendations

8.10 Progress against the other, substantive recommendations is graded blue or green in each case. In brief:

a) Pilot investigations were undertaken from March 2018, initially with the police in the lead.

b) Joint panels were signed off in August 2018 to review the casework with a view to deciding whether the threshold for MI5 involvement had been reached and whether MI5 could add value.

c) MI5 took on primacy in October 2018 for high-threat "DET" investigations (in deciding those including those investigations linked to proscribed organisations), and in November 2018 for high-threat "DET" leads MI5 takes on cases only where they meet their national security and terrorism thresholds and it judges that it can add value, taking account of wider resourcing pressures, and prioritises such cases alongside its other casework. CT Police and mainstream policing retain the lead, as was always envisaged, for lower-priority "DET" and broader "DE" casework, and for the initial receipt and triage of new intelligence on such threats.

d) JTAC launched its capability to assess the threat from "DET" in November 2018, following the successful implementation of an intelligence ingest process and a baselining assessment paper. "DET" (in practice, very largely XRW terrorism) is now being considered across all relevant JTAC products including Methodology and Chemical, Biological, Radioactive and Nuclear **[CBRN]**.

Observations

8.11 On the ***threat assessment*** side, JTAC at the time of my visit had set up a small (but growing) team focused on XRW terrorism in the UK, together with two police analysts. This is tiny by comparison with the Islamist side, but still makes for an improvement on the police analysis which I assessed in 2017 to be of variable quality.[29] JTAC thematic expertise, e.g. in CBRN and attack methodologies, is additionally available to the "new team" and allows a more professional and holistic approach to be taken.

8.12 JTAC outputs to date have included a position paper on the comparisons between Islamist and XRW terrorism, which revealed more similarities than had been expected (e.g. as regards lone actors, radicalisation of the vulnerable and links to international groups) and examined the phenomenon of "*reciprocal radicalisation*".

8.13 JTAC has learned also by seeing the XRW threat in its international context. As it was put to me:

> "Had the OIR recommendations not been made, JTAC would look at the US and Eastern Europe, and have no evidence base for what to do in the UK. It has put us ahead."

8.14 The comparative element to the ***intelligence-handling model*** gave additional points of reference to those engaged in it, and enabled different approaches to be questioned (though not necessarily found

[29] Their task is also eased by the fact that nearly all relevant material is in English.

wanting). For example, the joint teams tasked with deciding the thresholds for investigation observed far greater interest in the XRW world than among Islamists in weaponry and military culture: CPT-NOC had been less likely than MI5 to see such interest as an indicator that the terrorism threshold had been reached.

8.15 On the ***operational*** side, I was taken in detail through two 2018 investigations.

8.16 Although the number of live XRW investigations is small by comparison to Islamist investigations the police appreciate the extra depth of capability that MI5 brings, in priority operations but particularly in the lead space, where MI5 is seen as having access to more tools and data and enjoying a far greater analytical capability.

Challenges

8.17 In keeping with the frank nature of my briefings, I was informed of a number of initial or continuing difficulties. Most of these were not however fundamental in nature, and there has been a healthy tendency to see teething troubles as learning points rather than obstacles. For example:

a) There was some initial police reluctance to share information around the CT network, which was resolved by negotiation.

b) It has been necessary to manage the inherent tension that exists between Police prioritisation of evidence-building in order to effect executive action and the intelligence agencies' desire to build as full an intelligence picture as possible, particularly in relation to SOIs intent on travelling overseas.

c) There was uncertainty, now resolved, as to who should conduct international liaison (e.g. with the FBI) and who should authorise or seek the authorisation of covert activity: as to the latter, it was concluded that MI5 would have primacy in the covert phase and the police in executive action.

8.18 A more lasting problem is that of making historic police records available from CTP-NOC to MI5: the familiar problem of incompatible systems is compounded by the fact that historic police records have not been compiled with a view to identifying whether a subject meets the terrorism threshold.

8.19 The changes have had a resource impact for MI5 (though not for CTP), particularly in terms of training. New growth funding has been made available to restore dedicated "DE" desks in the regions, which existed previously but were phased out a few years ago.

8.20 More fundamentally, MI5 identified to me two respects in which its still partial coverage of non-Islamist terrorism is liable to leave it at a disadvantage:

a) in the identification and stopping of attacks: having restricted itself to the most serious leads, MI5 will remain unsighted on the threat posed by those who register less prominently on the radar; and

b) in the post-incident phase, where a more limited intelligence base may reduce the speed and effectiveness of its response.

8.21 Finally, while MI5 would like its discovery tools to be "*threat-agnostic*" and UKIC-wide, the task of adapting GCHQ's techniques to the non-Islamist terrorist threat is for the future. The same is true as regards the use of MI6 liaison facilities with overseas agencies, though MI5 – while unable to act as the UK's sole interlocutor on non-Islamist terrorism – is starting to play a role in liaison with 5 Eyes and European counterparts.

Conclusion

8.22 Had the UK seen an event equivalent to Anders Breivik's slaughter in 2011 of 77 people in Norway, recommendations such as those in chapter 9 of the OIR would surely have been implemented years ago. I supported them strongly during the OIR, taking the view that the involvement of JTAC and MI5 in XRW terrorism had been rendered inevitable by the terrorist murder of Jo Cox MP and the proscription of National Action in 2016.

8.23 I was nonetheless apprehensive about two things in particular: that costly steps to build capacity in JTAC and MI5 might be seen as tokenistic within MI5; and that the police might resent the loss of their previous control in this area.

8.24 Neither of these fears was substantially borne out by events. The police attitude was well expressed by the officer who said to me:

> "There is no resentment. We thought MI5 were so busy with ICT that they wouldn't be interested in taking the work. It was extremely refreshing that what we saw as an equal threat did attract their attention. We thought it was a tough sell but in fact, the new challenges and types of work were interesting to MI5 teams."

8.25 It is still not possible to say definitively how the XRW terrorist threat ranks against its Islamist counterpart. It is unlikely that the similar numbers of individuals receiving Channel support, though much publicised, translate into an equivalent terrorist threat.[30] But as I was frequently reminded, "*what you look for is what you find*": volume increases in identified XRW threats may be a function not so much of rapid growth in the underlying problem as of early steps taken to establish dedicated desks and disciplined joint assessment. In the longer term, it should be possible to stand back and evaluate whether the resource devoted to different types of terrorism is commensurate with the threat or not – which will in itself be a significant advance.

8.26 For now, I am happy to report that implementation of these recommendations is well on track. Though JTAC and MI5 involvement in non-Islamist terrorism remains in its infancy, it is already bringing tangible benefits in both understanding and meeting the threat.

8.27 I hope that the future will bring standardised terminology, on the model of the June 2018 iteration of CONTEST; the completion of all necessary steps to ensure complete parity of assessment and response between the Islamist and XRW threats; and the extension of that parity to all other forms of terrorism.

[30] In 2017/18, right wing extremists accounted for 18% of those referred to Prevent, 32% of those discussed at Channel panels and 44% of those who voluntarily agreed to receive Channel support: *Individuals referred to and supported through the Prevent Programme, April 2017 to March 2018*, Home Office Statistical Bulletin 31/18, December 2018.

9. CONCLUSION

9.1 As stated in my letter of instruction (Annex 1), implementation of the recommendations in the 2017 OIR and PARs is a crucial priority.

9.2 At a time of heightened threat, both MI5 and CTP have gone about their task of implementation both conscientiously and energetically. As summarized in more detail at 4.4 above, 63% of recommendations were complete and a further 22% were on track at the end of January 2019.

9.3 Moving beyond the ticking of boxes, positive results have already been noted from some of the reforms. Some subject-specific external evaluations have also been commissioned, notably into the MAC pilots. Many of the reforms are self-evidently desirable, to the point where continued evaluation of their merits might be considered superfluous.

9.4 It is the case however that no authoritative assessment has yet been made of the overall benefits of the reforms, or of the possible opportunity cost in terms of benefits foregone as a consequence of resources tied up in the implementing them. While I make no criticism of the recommendations themselves or of the steps taken to implement them, legitimate questions may be asked as to whether the enhanced emphasis on generating leads and on closed SOIs that underlies many of the recommendations risks diverting resource from the priority investigations which, by definition, contain the greatest risk. It is doubtful whether such an evaluation will be possible for another year or so, but desirable that it should be performed in due course.

9.5 MI5/CTP's own progress tracker and my own "*deep dives*" have identified areas in which progress has proved slower or more difficult than might have been hoped.

9.6 The most serious deficiency, fully acknowledged as such by the police, is the delivery of CTP's data strategy. Here, daunting challenges persist, summarized at 5.11 above.

9.7 The progress of the MAC pilots (section 7) has required a huge amount of effort for (so far) limited reward, though I welcome the extension of the pilot to Q1 2020, by which stage it should be possible to judge in the light of experience how the MAC principles can best be deployed and whether it is cost-effective to persist with this approach for managing closed SOIs, given the advances that are being made in the use of data (section 5) and the availability of other approaches for the management of closed SOIs (section 6).

9.8 Progress towards parity of treatment between Islamist and other forms of terrorism has been ahead of target, though much work remains to be done.

9.9 MI5 and CTP are each committed to operate in accordance with the law and to ensure that any applicable ethical standards are respected. However, I have identified areas, particularly in relation to the sharing of data and the use of behavioural analytics and artificial intelligence, where it is important that the ISC and IPCO – which, unlike me, have a continuing oversight function – ensure that the activities of UKIC and CTP remain legally and ethically compliant as technology develops.

9.10 There are too many imponderables to say whether, if implemented at the time, the OIR and PAR recommendations would have prevented any of the 2017 attacks. It is certainly possible that some of them would have made a difference, particularly in relation to the Manchester attack which involved a closed SOI and the purchase of explosive precursors.

9.11 The true value of these recommendations will be seen, however, in the future. As I noted in December 2017:

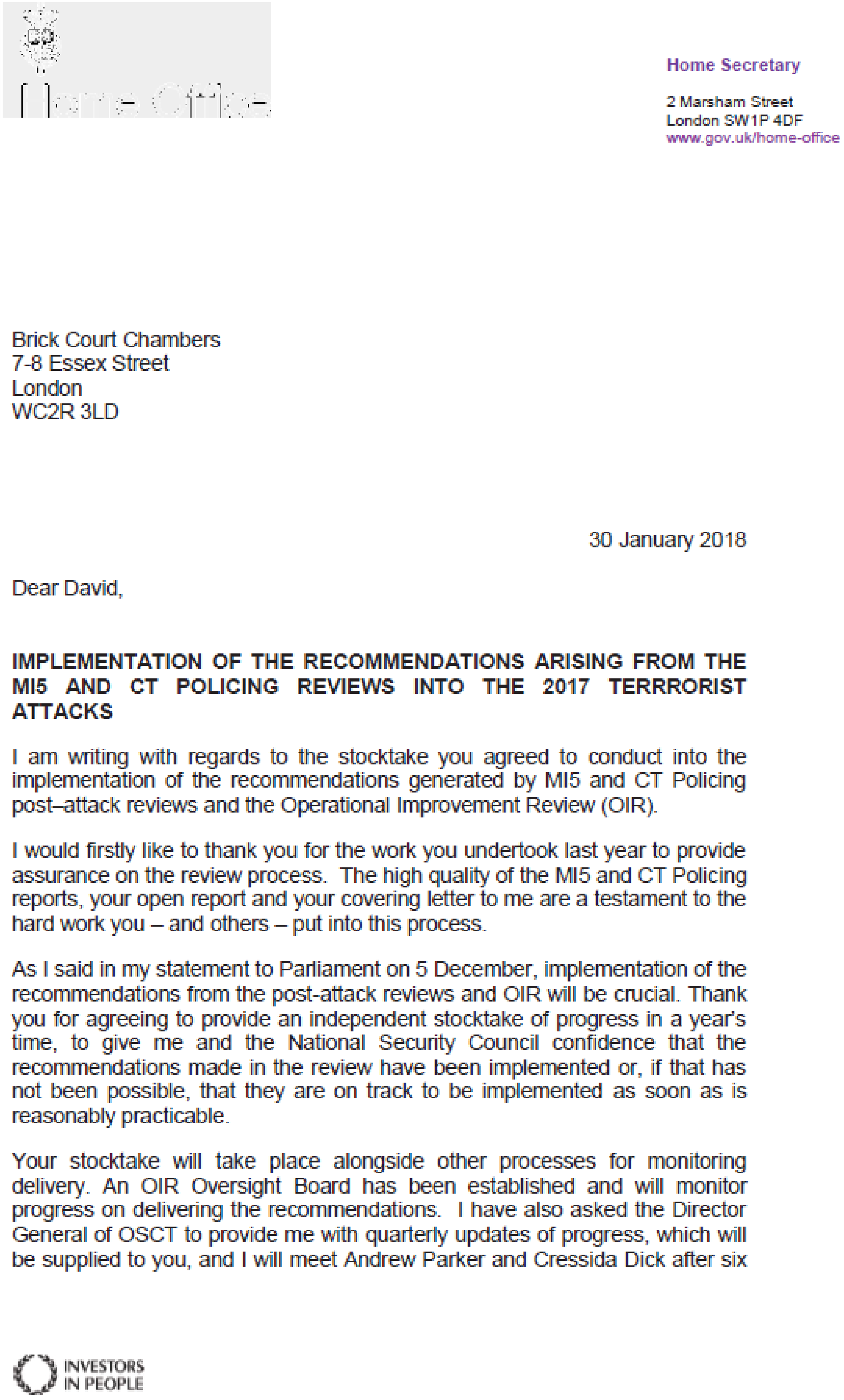
> "[I]n an increasingly high-volume business, whose success or failure depend on tiny margins, there will almost certainly be future cases in which these recommendations will tip the balance in favour of the security forces. MI5 and the police may not stop every attack, in other words, but will be strengthened in their existing ability to stop most of them."[31]

That remains my opinion. Though obstacles to delivery remained as of 31st January 2019, MI5 and CTP deserve credit for their considerable and for the most part productive efforts in implementing their recommendations to date.

[31] Anderson I, 5.28.

ANNEXES

ANNEX 1: LETTER OF INSTRUCTION



Home Office

Home Secretary

2 Marsham Street
London SW1P 4DF
www.gov.uk/home-office

Brick Court Chambers
7-8 Essex Street
London
WC2R 3LD

30 January 2018

Dear David,

IMPLEMENTATION OF THE RECOMMENDATIONS ARISING FROM THE MI5 AND CT POLICING REVIEWS INTO THE 2017 TERRRORIST ATTACKS

I am writing with regards to the stocktake you agreed to conduct into the implementation of the recommendations generated by MI5 and CT Policing post–attack reviews and the Operational Improvement Review (OIR).

I would firstly like to thank you for the work you undertook last year to provide assurance on the review process. The high quality of the MI5 and CT Policing reports, your open report and your covering letter to me are a testament to the hard work you – and others – put into this process.

As I said in my statement to Parliament on 5 December, implementation of the recommendations from the post-attack reviews and OIR will be crucial. Thank you for agreeing to provide an independent stocktake of progress in a year's time, to give me and the National Security Council confidence that the recommendations made in the review have been implemented or, if that has not been possible, that they are on track to be implemented as soon as is reasonably practicable.

Your stocktake will take place alongside other processes for monitoring delivery. An OIR Oversight Board has been established and will monitor progress on delivering the recommendations. I have also asked the Director General of OSCT to provide me with quarterly updates of progress, which will be supplied to you, and I will meet Andrew Parker and Cressida Dick after six months to discuss how implementation is going. As you know, the Intelligence and Security Committee of Parliament also intends to conduct some work in this area.

You should engage as you see necessary with lead officials and Ministers in MI5, CT Policing and the relevant Government departments who are responsible for delivering recommendations from the reviews. You will be able to discuss what progress has been made with these officials and Ministers and ask for any follow up information. You should also have access to any documentation you need as part of this work.

I would be grateful if you could complete your stocktake by the end of January 2019 and provide your conclusions to me, copied to the Prime Minister and the ISC.

Please also prepare an unclassified summary of your conclusions for public use, which, subject to discussions with the relevant information owners, I will place in the House Library. Those discussions are to ensure that nothing in the public facing document could prejudice national security.

While it seems unlikely that such a review could adversely affect criminal prosecutions or inquests relating to the 2017 terrorist attacks, please also ensure that any published version of your conclusions does not do so.

Thank you again for agreeing to undertake this further work.

Rt Hon Amber Rudd MP

ANNEX 2: LIST OF ACRONYMS

BPD	Bulk Personal Dataset
BSU	Behavioural Science Unit (MI5)
CBRN	Chemical, Biological, Radioactive and Nuclear
CSOI	Closed Subject of Interest
CT	Counter-Terrorism
CTIU	Counter-Terrorism Intelligence Unit
CTP	Counter-Terrorism Policing
CTP-NOC	Counter-Terrorism Policing National Operations Centre
CTU	Counter-Terrorism Unit
DE	Domestic Extremist
DET	Domestic Extremist Terrorism
ERT	Emerging and Residual Threat
FRW	Far Right Wing
GCHQ	Government Communications Headquarters: UK digital intelligence agency
ICT	International Counter-Terrorism
IDEPP	Independent Digital Ethics Panel for Policing
IHM	Intelligence Handling Model
IPCO	Investigatory Powers Commissioner’s Office
ISC	Intelligence and Security Committee of Parliament
JTAC	Joint Terrorism Analysis Centre
KIS	Key Information Store
MAC	Multi-Agency Centres

MI5	Security Service: UK domestic intelligence agency
MI6	Secret Intelligence Service or SIS: UK overseas intelligence agency
NIRT	Northern Ireland Related Terrorism
NMAC	National Multi-Agency Centre
NSN	National Secure Network
OGDs	Other Government Departments
OIR	Operational Improvement Review
OIROB	Operational Improvement Review Oversight Board
PAR	Post-Attack Review
RAG	Red – Amber – Green
RMAC	Regional Multi-Agency Centre
SOI	Subject of Interest
UKIC	United Kingdom Intelligence Community
XRW	Extreme Right Wing