Intelligence and Security Committee Annual Report 2016-17: Further Government Response

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

July 2018

Cm 9678

Intelligence and Security Committee Annual Report 2016-17: Further Government Response

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

July 2018

Cm 9678

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

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

ISBN 978-1-5286-0737-7

CCS0718140448 07/18

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

INTELLIGENCE AND SECURITY COMMITTEE ANNUAL REPORT 2016-17: FURTHER GOVERNMENT RESPONSE

The Government is grateful to the Intelligence and Security Committee for its continued independent oversight and scrutiny. On 20 December 2017, the Committee published its 2016-17 Annual Report, covering the period July 2016 to April 2017. The Prime Minister acknowledged and thanked the ISC for the report in a Written Ministerial Statement on the same day. The 2016-2017 Annual Report is thorough and comprehensive, and demonstrates the breadth and importance of the Committee's work. This document provides further detail on the Government's response to each of the ISC's recommendations and conclusions contained in that report.

The ISC's recommendations and conclusions are set out below in **bold**, followed immediately by the Government reply.

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

The Government notes the ISC's recommendation and recognises the importance of the challenge posed by those returning from Iraq and Syria. Security considerations are a key priority for the Government and the Home Office is ensuring that potential threats are properly assessed and dealt with appropriately. The Home Office is also continuing to make resources available, both centrally and at a local level, to ensure that support is provided to those who need it. The Government has issued advice to all local authorities in England, and worked with Devolved Administrations who are producing their own advice, setting out the importance of using multi-agency safeguarding processes to monitor and manage the risks around returning children. This advice also set out how local authorities could access national support programmes which have been established by the Home Office.

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

The Government acknowledges and accepts this conclusion. The Prevent programme counters terrorist ideologies specifically by tackling the causes of radicalisation, which is a complex process for individuals with no single factor at work. The purpose of Prevent is to safeguard and support vulnerable people to stop them from becoming terrorists or supporting terrorism. Government's Prevent work also extends to supporting the rehabilitation and disengagement of those already engaged in terrorism. Counter-radicalisation forms one part of a wider effort to counter broader extremist messages and behaviours. The Home Office has an effective Counter-Extremism Strategy to protect our communities from the wider social harms beyond terrorism caused by extremism.

The Government's new Counter Terrorism Strategy, published in June 2018, sets out the work being done under the Prevent strand to safeguard and support those vulnerable to radicalisation, to stop them from becoming terrorists or supporting terrorism. In CONTEST, the Government sets out that we will:

- Focus activity and resources in those locations where the threat from terrorism and radicalisation is highest.
- Expand the Desistance and Disengagement Programme with an immediate aim over the next 12 months to more than double the number of individuals receiving rehabilitative interventions.
- Develop a series of multi-agency pilots to trial methods to improve our understanding of those at risk of involvement in terrorism and enable earlier intervention.
- Focus 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.
- 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.

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

The Government welcomes this conclusion. The Agencies are working closer together than ever before, including on counter-terrorism, with even closer collaboration planned for the future.

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

The Government welcomes this conclusion. The ability to relocate TPIM subjects is an important element of the toolkit of disruptive measures available, and its use has been supported by the Courts.

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

The Government welcomes this conclusion.

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

The public-facing National Cyber Security Centre operates a variety of assurance schemes for products, services and people. It works with other industry standards-setting bodies to scale its advice, as well as with other government departments such as the Department for Digital, Culture, Media and Sport (DCMS) on the Internet of Things (IoT) code of practice, to ensure strong security is built into these products by design.

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

The Government weclomes this conclusion. This remains a top priority.

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

The Government welcomes this conclusion.

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

The Government welcomes this conclusion. NCSC's messaging about the importance of individuals taking responsibility for their own cyber security is continually reinforced through targeted communications.

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

The Government welcomes this conclusion.

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

The Government welcomes this conclusion, and GCHQ recognises the challenges of recruiting and retaining a technical workforce. They are responding to this by:

- Using all the levers offered around pay to improve the joining offer for some technical candidates;
- Increasing reach into diverse communities through initiatives such as Decoded in Campaign and Decoded Digital;
- Ensuring recruitment marketing is varied, and not only advertises current opportunities but increases GCHQ's recognition as a technical employer;
- Running specific technical campaigns, which aim to increase the speed of recruitment, supported by a wide range of innovative marketing;
- Improvements in external market review of specialist payments to better encourage skills growth and career planning; and building better understanding of the application of specialist payments and mission outcomes.

GCHQ also does a significant amount of outreach work, engaging with local schools and universities around the UK. An example of this includes the work on Cyber First which introduces 11-17 year olds to the world of cyber security.

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

The UK national cyber security strategy makes it clear that the UK's offensive cyber capability will be used in accordance with national and international law. The strategy sets out our commitment to safeguarding the long-term future of a free, open, peaceful and secure cyber space by:

- Strengthening a common understanding of responsible state behaviour in cyberspace;
- Building on agreement that existing international law applies in cyberspace – including the respect for human rights and fundamental freedoms;
- The application of international humanitarian law to cyber operations in armed conflict; and
- Continuing to promote the implementation of voluntary, non-binding, norms of responsible state-behaviour.

We recognise that an increasing number of states are developing operational cyber capabilities. We assert states' legitimate right to develop these capabilities, and continue to emphasise the obligation to ensure their use is governed in accordance with international law.

To this end, the UK remains committed to promoting international consensus on stability frameworks for cyberspace. We will continue to pursue this agenda bilaterally and through multilateral fora, including the EU, the UN, the Organization for Security and Co-operation in Europe (OSCE), Association of Southeast Asian Nations (ASEAN) and the Organization of American States (OAS), to ensure the cumulative reports of the UN Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) are implemented. The UK worked to ensure this approach was endorsed in EU Council Conclusions on the Joint Communication to the European Parliament in November 2017 and in OSCE Ministerial Council Decisions in Hamburg in 2016 and Vienna in December 2017.

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

Countering the threat from hostile state activity requires activity across a wide-range of Government departments and Agencies, both domestic and international-facing. It is central to the work of the intelligence agencies, the lead government departments for the security of critical national infrastructure, those Departments responsible for the UK's long-term prosperity and, critically, those responsible for foreign relations with our allies and our adversaries. Cabinet Office also has responsibility for oversight of the National Cyber Security Strategy, which is a crucial component of the Government's approach to this issue. Given this breadth, across both domestic and international issues, and with cyber security a central component of response, it is the Government's view that at this stage the National Security Secretariat is best placed to coordinate these strands of activity, but we will continue to keep it under review.

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

The Government notes this conclusion. As the ISC acknowledged in its report, the Agencies have been increasing their efforts to understand and mitigate the threats posed to our national security by Russia.

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

The UK keeps its policy on collaboration with other intelligence agencies under constant review. We will continue to explore cooperation on specific issues where appropriate.

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

It is important to draw on the full range of Government expertise when making such important decisions. The Agencies were involved in the Government's consideration of the national security risks arising from the Chinese investment in Hinkley Point C. The Centre for Protection of National Infrastructure (CPNI) and NCSC continue to provide advice to the relevant government departments, regulators and companies.

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

The UK Government closely monitors US policies for any changes that may impact on our Counter Terrorism (CT) cooperation with the US as a result of detainee treatment issues. Should a change in policy arise that would impact on our cooperation, swift action would be taken as part of our close CT cooperation and dialogue with the US to prevent British laws and values being compromised.

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

The Government acknowledges the recommendation and would highlight recent progress.

US Communications Service Providers have argued that US law prevents them from cooperating with lawful orders from the UK for access to the content of communications in serious crime and counter-terrorism investigations. Following extensive engagement by UK Ministers and officials with the US Government, Members of Congress, and relevant companies, the Clarifying Overseas Use of Data Act (CLOUD Act) was passed by Congress on 23 March 2018. The CLOUD Act enables the signature of bilateral agreements that, once signed and ratified, will permit targeted access to this data in serious crime and counter-terrorism investigations. The Government is now negotiating a bilateral UK/US Agreement as a priority. The Agreement will set out the circumstances in which data can be accessed; with strong privacy protections, and high standards of oversight.

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

The Prime Minister has made clear our unconditional commitment to European security. Andrew Parker and Jeremy Fleming have recently highlighted the strength of cooperation with European intelligence and security agencies and the mutual benefit that brings – including in disrupting four terrorist operations in European countries over the last year. Those relationships and our close cooperation will continue after we have left the EU.

The nature of the UK's relationship with the EU will have to change but this should not be at the expense of operational capability. The recently published White Paper sets out the UK's vision for how to maintain operational capabilities. The Government is confident that the proposal in the White Paper provides a firm basis for progressing the negotiations.

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

The Government will need to maintain cooperation between law enforcement organisations, and ensure the fast and efficient exchange of data. The UK's Data Protection Act applies the standards of the EU's General Data Protection Regulation and Law Enforcement Directive, post exit. The UK's data protection framework will be assessed by the EU as part of the adequacy process, including the circumstances in which public authorities access personal data for the purposes of national security. In this respect, the Data Protection Act provides a bespoke regime for the processing of data by UK intelligence agencies, and the UK's Investigatory Powers Act was described as introducing 'world-leading standards of transparency' in an independent review. The Government is working closely with the Security and Intelligence Agencies to ensure their interests are properly represented in this matter, and across wider Brexit negotiations.

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

The Government notes the ISC's recommendation. Where appropriate the Government endeavours to include funding within baselines, and we are aware of the challenges that arise from having several different hypothecated funding pots. We will ensure that this issue is carefully considered as part of the upcoming Spending Review, with a view to reducing the complexity of funding streams. However, a number of funding streams are part of wider Government programmes being managed by other Government Departments; any potential changes to the funding models could affect both the flexibility in how the programmes are delivered and how funding is prioritised in the delivery of programme objectives.

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

We note this recommendation and regularly monitor and scrutinise the delivery of efficiencies at Financial Steering Group meetings. The Agencies have now exceeded their Year 1 and 2 combined targets for efficiencies, as set out in the Spending Review settlement, and Government will continue to work with them as they refine their savings plans for future years. The Agencies' track record over the last two years, as well as the work done on bringing together corporate services and IT infrastructure, should provide confidence that these cashable efficiencies are on track. We will continue to work closely with the National Audit Office.

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

The Government notes the ISC's conclusion on whistleblowing, and has identified appropriate processes by which concerns at work can be shared with the ISC Chairman.

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

The Government notes the ISC's recommendation, and is working with the Agencies to closely monitor their need for 'time hire' contractors. We continue to seek opportunities to drive down costs across all areas, not just contractors and consultants, in order to achieve the best value for the tax payer.

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

The Government notes this conclusion. In November 2017, the ALFA programme delivered the new electronic documents and record management system for MI5. This marked the successful delivery of the most substantial technology-based change across the whole of MI5 in many years and marks a major milestone in strengthening information management in MI5. It is the culmination of a sustained change programme focused on improved Information Management that has been a top priority for MI5 over the last few years.

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

The Government acknowledges and welcomes this conclusion. GCHQ's strategy remains to decentralise, accessing a wider and more diverse talent pool. With the opening of the National Cyber Security Centre in London in late 2016, increased

recruitment in Scarborough in 2018 and with the announcement on 11 April 2018 of the planned Manchester office (to be open by summer 2019), GCHQ assess that they have made demonstrable progress towards addressing accommodation issues, whilst at the same time enabling access to a more diverse recruitment market. In addition we continue to implement a number of tactical solutions to make greater use of accommodation in the Cheltenham area in response to our short term accommodation pressures. We continue to pursue opportunities for tri-agency collaboration in managing the Estate.

CCS0718140448

978-1-5286-0737-7