Intelligence and Security Committee of Parliament

Annual Report 2018–2019

HC 633

Intelligence and Security Committee of Parliament

Annual Report 2018–2019

Presented to Parliament pursuant to sections 2 and 3 of the Justice and Security Act 2013

Ordered by the House of Commons to be printed on 21 July 2020

HC 633

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

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

ISBN 978-1-5286-2091-8

CCS 0620799228 07/20

Printed on paper containing 75% recycled fibre content minimum

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

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

The Rt Hon. Dr Julian Lewis MP (Chair)

The Rt Hon. Chris Grayling MP	*The Rt Hon. Kevan Jones MP*
The Rt Hon. Sir John Hayes CBE MP	*Mark Pritchard MP*
Stewart Hosie MP	*The Rt Hon. Theresa Villiers MP*
Dame Diana Johnson DBE MP	*The Rt Hon. Admiral Lord West of Spithead GCB DSC*

This Report covers the work of the previous Committee, which sat from November 2017 to November 2019:

The Rt Hon. Dominic Grieve QC MP (Chair)

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

The Intelligence and Security Committee of Parliament (ISC) is a statutory committee of Parliament that has responsibility for oversight of the UK Intelligence Community. The Committee was originally established by the Intelligence Services Act 1994 and was reformed, and its powers reinforced, by the Justice and Security Act 2013.

The Committee oversees the intelligence and security activities of the UK Intelligence Community, including the policies, expenditure, administration and operations of MI5 (the Security Service), MI6 (the Secret Intelligence Service or SIS) and GCHQ (the Government Communications Headquarters)* and the work of the Joint Intelligence Organisation (JIO) and the National Security Secretariat (NSS) in the Cabinet Office; Defence Intelligence (DI) in the Ministry of Defence; and the Office for Security and Counter-Terrorism (OSCT) in the Home Office.

The Committee consists of nine Members drawn from both Houses of Parliament. Members are appointed by the Houses of Parliament, having been nominated by the Prime Minister in consultation with the Leader of the Opposition. The Chair of the Committee is elected by its Members.

The Members of the Committee are subject to section 1(1)(b) of the Official Secrets Act 1989 and are routinely given access to highly classified material in carrying out their duties. The Committee sets its own agenda and work programme, taking evidence from Government Ministers, the Heads of the intelligence and security Agencies, senior officials, experts and academics as required. Its Inquiries tend to concentrate on current events and issues of concern, and therefore focus on operational and policy matters, while its annual reports address administration and finance.

The reports can contain highly classified material, which would damage the operational capabilities of the intelligence Agencies if it were published. There is therefore a well-established and lengthy process to prepare the Committee's reports ready for publication. The Report is checked to ensure that it is factually correct (i.e. that the facts and figures are up to date in what can be a fast-changing environment). The Intelligence Community may then, on behalf of the Prime Minister, request redaction of material in the report if they consider that its publication would damage their work, for example by revealing their targets, methods, sources or operational capabilities. The Committee requires the

Intelligence Community to demonstrate clearly how publication of the material in question would be damaging since the Committee aims to ensure that only the minimum of text is redacted from a report. Where the Committee rejects a request for material to be redacted, if the organisation considers that the material would cause serious damage to national security if published, then the Head of that organisation must appear before the Committee to argue the case. Once these stages have been completed the report is sent to the Prime Minister to consider. Under the Justice and Security Act 2013 the Committee can only lay its reports before Parliament once the Prime Minister has confirmed that there is no material in them which would prejudice the discharge of the functions of the Agencies or – where the Prime Minister considers that there is such material in the report – once the Prime Minister has consulted the Committee and they have then excluded the relevant material from the report.

The Committee believes that it is important that Parliament and the public should be able to see where information had to be redacted: redactions are clearly indicated in the report by ***. This means that the published report is the same as the classified version sent to the Prime Minister (albeit with redactions).

---

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

CONTENTS

THE WORK OF THE COMMITTEE

1. This Report summarises the work of the Intelligence and Security Committee of Parliament (ISC) for the period August 2018 to July 2019, in carrying out its oversight of the UK Intelligence Community.[1] It was written and sent to the Prime Minister before Parliament was dissolved on 6 November 2019, but could not be laid before Parliament until the Committee was re-constituted following the Election.

Membership during the period covered by this Report

2. On 19 March 2019, the Rt Hon. Ian Blackford MP notified the Chairman of his intent to step down from his role on the Committee. Following a consultation process, as set out in the Justice and Security Act 2013, Stewart Hosie MP was nominated for membership of the Committee by the Prime Minister, and was appointed as a Member of the Committee by the House of Commons on 30 April.

Work programme

3. During the period covered by this Annual Report, the Committee focused on a number of specific Inquiries. (The Committee sets its own work programme, which is inevitably influenced by national events and public and parliamentary concern.) The Committee considered it essential to consider the Government's actions in relation to the five serious terrorist attacks at Westminster Bridge, Manchester Arena, London Bridge, Finsbury Park and Parsons Green, in which thirty-six people lost their lives and many more were injured.[2] We also considered it necessary to investigate Russian hostile activity – an Inquiry given further impetus by the use of chemical weapons on British soil in the attempted murder of Sergei and Yulia Skripal and the subsequent death of Dawn Sturgess. We also began an Inquiry into the threat posed by China and, in particular, the role of Chinese companies in the UK's telecommunications infrastructure.

The 2017 Terrorist Attacks

4. Following the terrorist attacks which took place in the UK in 2017, the Committee considered it essential to establish whether mistakes were made and to ensure that all changes and improvements required had been identified. Our Inquiry focused primarily on the actions of MI5 and Counter Terrorism Policing (CTP). In addition to examining a substantial volume of written evidence from both organisations – including the Internal Reviews carried out by MI5 and CTP immediately following the attacks – the Committee held oral evidence sessions with the Home Secretary, the Director General of the Security Service, the Commissioner of the Metropolitan Police and other officials.[3]

5. The Committee published its Report, entitled '*The 2017 Attacks: What needs to change*', on 22 November 2018. The Report considered each attack in depth, with the exception of the Parsons Green attack because the Home Office failed to provide full evidence in sufficient time. From the information we did see on that attack, there were fundamental failings in the handling of this case by the Home Office, the police and Surrey County Council, and we recommended that a separate review should be undertaken into these errors. In relation to the four remaining attacks, we considered the actions of MI5 and CTP in relation to 12 cross-cutting issues: extremist material online; extremism

[1] Throughout this Report, the term 'Intelligence Community' is used to refer to the seven organisations that the Committee oversees.

[2] We do not include the perpetrators of the attacks.

[3] The Internal Reviews were subject to independent assurance by Lord Anderson of Ipswich. His Report was published in December 2017, and he has since published an implementation stock-take (11 June 2019).

in prisons; vehicle hire; chemicals and explosives; ***; joint working; low-level, peripheral and closed subjects of interest; travel; disruptive powers; families and Prevent; protective security; and data and information.

6. We concluded that both MI5 and CTP had been thorough in their desire to learn from mistakes. Nevertheless we made 43 recommendations where we found action needed to be taken. The Government provided an initial response in February 2019, and committed to provide updates at the 6- and 12-month points thereafter.[4] It is essential that the lessons of 2017 are learnt, and that the recommendations made by the Committee are implemented. Events around the world continue to demonstrate that Islamist and Right-Wing terrorism are a threat to us all.

Russia

7. On 23 November 2017, the Committee announced its intention to begin an Inquiry into Russia, following steadily increasing public and parliamentary concern about Russian activity – including the invasion of Ukraine, provision of military support to the Assad regime in Syria, and possible interference in Western political processes. Our Inquiry was given further priority in March 2018 by the attempted murder by the GRU of Sergei and Yulia Skripal, and the consequent death of Dawn Sturgess, which brought international condemnation because Russia used chemical weapons against civilians in direct contravention of international law.[5]

8. We received written evidence on Russia in June 2018, after some initial delay by the Intelligence Community, and were finally in a position to begin oral evidence sessions in October 2018. This was a major undertaking, spanning a number of evidence sessions with a broad range of witnesses over the course of eight months. Our Report was written, and the usual factual checks and redaction procedures completed, by 17 October 2019, at which point it was sent to the Prime Minister for confirmation – in accordance with the Justice and Security Act 2013 – that there was no material remaining which would prejudice the discharge of the functions of the Agencies. That confirmation was received on 13 December 2019, but the Report could not be published until the Committee was reconstituted following the General Election (under the Justice and Security Act it is the Committee which lays its reports before Parliament). The Report covers aspects of the Russian threat to the UK – from cyber attacks, to disinformation and influence campaigns, to Russian expatriates – and examines how the Government and, in particular, the Intelligence Community, has responded.[6]

9. Russia is a formidable adversary with the capability, capacity and – crucially – the intent to harm the national interests of the UK and its allies. It appears that Russia considers the UK one of its top Western intelligence targets: while we may not experience the level and type of threat that countries on Russia's borders suffer, witnesses have suggested that we would sit just behind the US and NATO in any priority list. This is likely to be related to the UK's close relationship with the US, and the fact that the UK is seen as central to the Western anti-Russian lobby. It will have been reinforced by the UK's firm stance recently in response to Russian aggression: following the UK-led international response to the Salisbury attack – which saw an unprecedented 153 Russian intelligence officers and diplomats expelled from 28 countries and NATO – it appears to the Committee that

[4] HMG, *Government Response to the Intelligence and Security Committee of Parliament Report 'The 2017 Attacks: What needs to change?'*, January 2019

[5] The GRU is the Main Intelligence Directorate of the General Staff of the Russian Armed Forces.

[6] The matters covered by the Inquiry are highly sensitive and therefore, given that the Russian Intelligence Services will analyse whatever we put in the public domain, the potential to damage the capabilities of the Intelligence Community was significant. Given this, we decided to produce a shorter Report than usual, which took the form of a summary of the most important points we noted during the Inquiry, at a high level, without revealing underlying detail. This was supplemented with a substantial Annex, which was not published, in view of the current Russian threat.

Putin considers the UK to be a key diplomatic adversary. Our Report considered what action is now being taken in response to the Russian threat – and whether the Government was too slow to respond to the increasing threat.

10. In some cases, we found that more, or different, effort is needed: we noted, in particular, the extent to which much of the work of the Intelligence Community is focused on *** and questioned whether a more comprehensive approach is required. This focus led us to question who is responsible for broader work against the Russian threat and whether those organisations are sufficiently empowered to tackle a hostile state threat such as Russia, and in some instances we recommended a shift in responsibilities. In other cases, we recommended a simplification: there are a number of complicated wiring diagrams that do not appear to provide the clear lines of accountability that are needed. The most immediate need for action is in relation to new legislation: the UK must have the tools to tackle this very capable adversary, and this means a new statutory framework to tackle espionage, the illicit financial dealings of the Russian elite and the 'enablers' who support this activity.

11. Whilst it is possible that an improved relationship between Russia and the UK may one day reduce the threat to the UK, it is unrealistic to think that might happen under the current Russian leadership. It would have to be dependent on Russia ceasing its acts of aggression towards the UK, such as the use of chemical weapons on UK soil. The UK, as a Western democracy, cannot allow Russia to flout the rules-based international order without there being commensurate consequences: any public move towards a more allied relationship with Russia at present would severely undermine the strength of the international response to Salisbury, and the UK's leadership and credibility within this movement. A continuing international consensus is essential against Russian aggressive action – the West is strongest when it acts collectively and that is the way in which we can best attach a cost to Putin's actions.

China

12. On 6 March 2019, the Committee announced that its next Inquiry would be into national security issues relating to China. There has been concern as to whether the Government has achieved the right balance between the economic imperatives of the so-called 'Golden Era' of UK-China relations on the one hand and national security considerations on the other. These apparent tensions in Government policy will form the context for much of the evidence the Committee is taking in relation to this Inquiry.

13. The Committee received written evidence in April 2019, heard from leading academic and industry experts in May and June, and began questioning the Intelligence Community in July. The Inquiry was still underway when Parliament was dissolved for the 2019 General Election.

Other areas of inquiry

14. In addition to these major Inquiries, the Committee examined a number of other issues concerning the Intelligence Community, including, in particular, the Government's current approach to addressing the threat from Northern Ireland-related terrorism (NIRT), and the procurement arrangements for the headquarters of the National Cyber Security Centre in Victoria, London.

15. As part of its broader oversight function, the Committee continued to monitor the expenditure, administration and policy of the seven organisations it oversees through the Quarterly Reports it receives from them and the end-year information covering the 2017/18 financial year. We were also kept updated by the Intelligence Community on key developments relating to their work. Given the Committee's focus on its specific Inquiries during the period covered by this Report, detailed scrutiny of each area is not included in this Annual Report; however, the current threat

assessment, together with the key facts and major developments for each organisation, are summarised in the Annexes.

16. In carrying out its work during the period covered by this Report, the Committee:

- held 28 full Committee meetings, including evidence sessions with Government Ministers, senior officials from across the Intelligence Community, and external experts;
- visited Intelligence Community organisations on three occasions;
- held bilateral discussions with the American and Canadian intelligence communities;
- hosted delegations from Germany, Romania and the US; and
- held 15 other meetings.

Since its establishment in 1994, the Committee has met annually with the Prime Minister to discuss its work, report on key issues, and raise any concerns. With the interruptions to the Committee's work in 2015 and again in 2017 whilst Parliament was not sitting, no such meeting took place and it is a matter of some frustration that the Committee was also unable to meet the Prime Minister in 2018 or 2019. As a result, the Committee has not met with a Prime Minister since December 2014. This is an extremely unsatisfactory situation, and one that the Committee expects to be rectified.

Whistleblowing

17. We reported in our 2016-2017 Annual Report that we had been informed that the ISC was to be an approved route by which staff from the three intelligence Agencies could raise concerns.[7] Since then, the ISC Chair has considered the Agencies' own policies in relation to staff raising concerns, and has been approached by a small number of Agency staff. We have set out the policy and processes for Agency staff wishing to approach the ISC Chair with concerns (including, crucially, the difference between matters which should be considered as 'whistleblowing' and those which are grievances).[8]

18. In this context, we raised the concern in our 2016-2017 Report that "*if the Agencies intend* [the ISC] *to be used* [as a route for whistleblowing] *then the current bar on Agency staff being able to communicate with the Committee directly via secure email will need to removed*." This has not happened. If the Agencies are serious about their staff being able to approach the ISC Chair, then the bar must be removed.

Tracking progress on the Committee's recommendations

19. The ISC's reports contain recommendations for the Government and, under the Memorandum of Understanding which underpins the Justice and Security Act 2013, the Government must respond to the Committee's reports within 60 days. In the Government's response, it sets out which of the

[7] The policy since agreed with the Agencies is that the route is to the ISC Chair.

[8] The ISC considers matters which raise the following concerns:

- that a criminal offence has been committed, is being committed or is likely to be committed;
- that a person has failed, is failing or is likely to fail to comply with any legal obligation to which s/he is subject;
- that a miscarriage of justice has occurred, is occurring or is likely to occur;
- that the health or safety of any individual has been, is being or is likely to be endangered;
- that the environment has been, is being or is likely to be damaged; or
- that information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be concealed.

Committee's recommendations it accepts, and which it does not, with an associated explanation of its reasoning. However, in recent Inquiries, we have noted that previous recommendations which were accepted have not always been implemented – for example, during our Inquiry into the 2017 terrorist attacks, it became clear that the Government had not implemented recommendations the Committee had previously made about the handling of Subjects of Interest in its 2006 and 2009 reports on the 7/7 terrorist attacks, and in its 2014 report on the murder of Fusilier Lee Rigby.

20. In July 2018, the Committee raised these concerns with the National Security Adviser and requested a stock-take on progress implementing its recommendations. The Government has now provided a helpful document tracking the implementation of all ISC recommendations which the Government has accepted since 2013, and the Cabinet Office has undertaken to provide regular updates on progress. This will assist the Committee in carrying out its statutory role to provide effective and robust scrutiny of the work of the Intelligence Community by enabling the identification of areas where the Government is failing to make progress, and we trust that it will also provide a means for Government to ensure that improvements are made and momentum maintained.

Committee Resources

21. The Committee was supported in its work by a team of staff (eight for the majority of the year, ten at the time of writing).[9] The Committee's budget for the 2018/19 financial year was £1,646,000. This incorporated the costs of the Committee and Secretariat's security, IT, telecoms, report publication, accommodation, utilities and centrally provided corporate services.

Sir Charles Farr CMG OBE

22. The Committee wishes to take this opportunity to express its gratitude to the late Sir Charles Farr. The Committee took evidence from him on a number of occasions over the years, first when he was Director General of the Office for Security and Counter-Terrorism (OSCT) and, from December 2015, as Chair of the Joint Intelligence Committee. The evidence he provided to the Committee, and his wider assistance in progressing Inquiries such as that into Russia, were of great help. The Committee wishes to pay tribute more broadly to Sir Charles's exceptional service to the Intelligence Community.

[9] The separate team provided by Government to work on the Committee's Detainee Inquiry was disbanded in August 2018 following the publication on 28 July 2018 of that report.

LIST OF WITNESSES

Ministers

The Rt Hon. Jeremy Hunt MP – then Secretary of State for Foreign and Commonwealth Affairs

The Rt Hon. Sajid Javid MP – then Secretary of State for the Home Department

The Rt Hon. Ben Wallace MP – then Minister of State for Security and Economic Crime

Officials

CABINET OFFICE

Sir Charles Farr CMG OBE – formerly Chair, Joint Intelligence Committee

Ms Madeleine Alessandri CMG – then Deputy National Security Adviser

Other officials

FOREIGN AND COMMONWEALTH OFFICE

Sir Philip Barton KCMG OBE – then Director General Consular and Security

Other officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Mr Jeremy Fleming – Director

Other officials

HOME OFFICE

Mr Tom Hurd OBE – Director General, Office for Security and Counter Terrorism

Other officials

MINISTRY OF DEFENCE

Lieutenant General Jim Hockenhull OBE – Chief of Defence Intelligence

Other officials

NATIONAL CRIME AGENCY

Ms Lynne Owens CBE QPM – Director General

SECRET INTELLIGENCE SERVICE

Sir Alex Younger KCMG – Chief

Other officials

SECURITY SERVICE

Sir Andrew Parker KCB – then Director General

Other officials

Expert external witnesses

Mr Patrick Binchy – Chief Technology Officer, Three UK

Mr Christopher Donnelly CMG TD – Head of the Institute for Statecraft

Mr John Gerson CMG – Visiting Professor, King's College London

Mr Edward Lucas – Writer and consultant specialising in European and Transatlantic security

Mr Neil McRae – Chief Network Architect, BT Group

Mr Brendan O'Reilly – Chief Technology Officer, Telefónica UK

Mr Raffaello Pantucci – Director of International Security Studies, RUSI

Mr Charles Parton OBE – Senior Associate Fellow, RUSI

The Rt Hon. Lord Patten of Barnes CH – Chancellor of the University of Oxford

Dr Tim Stevens, Lecturer in Global Security, King's College London

Professor Steve Tsang – Director, SOAS China Institute

The Committee is also grateful for those who provided written evidence, including, amongst others, Ms Anne Applebaum (Professor, LSE Institute of Global Affairs), Mr William Browder (Head of the Global Magnitsky Justice Movement) and Mr Christopher Steele (Orbis Business Intelligence).

ANNEX A: THREAT ASSESSMENT

The threat to the UK and its interests overseas comes from a number of different sources, as outlined in previous Annual Reports, and includes Islamist and Northern Ireland-related terrorism, Hostile State Activity and nuclear proliferation. The following is a summary of the threat assessment as at 1 November 2019.[10]

The Threat Picture

The threat to the UK from terrorism

The UK National Threat Level is currently set at SEVERE, meaning an attack in the UK is highly likely.[11] The Threat Level has been at this level almost consistently since August 2014, with the exception of increasing twice to CRITICAL in 2017. Throughout 2018 and 2019 so far, there has been a lower intensity of attack planning than there was in 2017. However, the overall scale of the Islamist threat has remained, with persistent fluctuations and developments. The nature of the threat continues to be unpredictable, is subject to change at short notice, and is reactive to global events.

The threat from Right-Wing terrorism in the UK is not at the same level as that of Islamist terrorism, but the threat is increasing. The terrorist threat in the UK therefore remains diverse. It is most likely that an Islamist or Right-Wing terrorist attack would emanate from lone actors, who plan attacks independently of a formal association with a wider terrorist group.

ISIL-Core (Daesh) has endured territorial collapse in Syria and Iraq, and successfully reverted back to a clandestine terrorist organisation. ISIL maintains the long-term intent to re-establish a Caliphate, and will focus on propagating the conditions to potentially make this possible. ISIL's global network has become increasingly important as the group attempts to maintain a narrative of continuing success. Whilst territorial collapse has had a significant impact on ISIL's ability to project an external threat, in relative terms the residual threat it continues to pose globally remains high. The co-ordinated attack in Sri Lanka in April 2019 is an example of the continuing high level of threat posed by extremists willing to act in ISIL's name.

Al-Qaeda takes a long-term approach to its ultimate aim of establishing a Caliphate. It seeks to embed itself in local conflicts to develop the support of the population. It has developed a strong network of global affiliates that are empowered to push forward this agenda. These affiliates pose a high threat to Western interests in their region. Al-Qaeda has become more cohesive, meaning the threat from the group is increasing, because it potentially allows for Al-Qaeda to co-ordinate activities and share resources.

ISIL and Al-Qaeda capabilities have ebbed and flowed in recent years as military pressure has been applied and relieved. For both groups, their global franchises and worldwide base of supporters mean the threat they pose is multi-faceted, and will potentially become more nebulous in the future.

[10] We note that the UK National Threat Level was reduced to SUBSTANTIAL on 4 November 2019, shortly after this Report was sent to the Prime Minister. Notwithstanding this, the information in the box is otherwise representative of the Agencies' assessment of the threat to the UK.

[11] The Joint Terrorism Analysis Centre (JTAC) assesses the threat from all forms of terrorism. There is a single national threat level describing the threat to the UK, which includes Islamist, Northern Ireland, Left-Wing and Right-Wing terrorism. MI5 is responsible for setting the threat levels from Irish and other domestic terrorism both in Northern Ireland and in Great Britain. There are five tiers to the threat level system: CRITICAL (an attack is highly likely in the near future); SEVERE (an attack is highly likely); SUBSTANTIAL (an attack is likely); MODERATE (an attack is possible but not likely); and LOW (an attack is unlikely).

From a UK-mainland perspective, Islamist and Right-Wing terrorism are highly likely to remain internationally connected, but are now rooted in the UK. It is a dynamic and unpredictable picture.

Northern Ireland-related terrorism

There is a persistent threat of terrorism in Northern Ireland (NI), emanating from a small number of dissident republican (DR) groups who are opposed to the political process and remain committed to violence. The new IRA is currently the most widespread and capable of the DR groups. It has carried out some of the most significant attacks in NI since it formed in 2012. The Continuity IRA continue to aspire to conduct attacks, whilst Arm na Poblachta present a more localised threat. Despite the declaration of a ceasefire in January 2018, Óglaigh na hÉireann remain in existence; however, a split led to the announcement of a new DR group, the Irish Republican Movement, in April 2018.

The threat level in NI remains at SEVERE (an attack is highly likely). DR groups continue to target and attack Police Service of Northern Ireland (PSNI) officers, prison officers and members of the armed forces. There has been a small increase in the number of attacks so far in 2019 although the overall trend continues to be moving downwards. Recent attacks include a vehicle-borne improvised explosive device (VBIED) attack in Londonderry against a court house, a shooting attack in Londonderry which led to the murder of journalist Lyra McKee, an attempted attack using an under-vehicle IED (UVIED) against an off duty member of PSNI in Belfast, and five postal IEDs (one of which functioned) which were sent to a range of targets in Great Britain. All these incidents were carried out by members of the new IRA. These attacks demonstrate continued intent and the potential lethality of the threat in NI.

Hostile State Activity

The threat to the UK from espionage is both extensive and enduring. The UK continues to be a high-priority target for a number of hostile foreign intelligence services. Foreign intelligence services continue to conduct espionage against a broad range of UK interests, seeking to obtain government and military secrets, intellectual property and economic information. Those with hostile intent and sufficient capability also conduct operations designed to influence UK policy and public opinion. They engage in a wide range of activity, encompassing the recruitment of human agents with the ability to acquire sensitive information (both protectively marked and unclassified), and an increasing use of cyber in order to target the British government, the UK's Critical National Infrastructure (CNI) and UK businesses. As was graphically demonstrated by the attempted murder of Sergei and Yulia Skripal in 2018 and the subsequent death of Dawn Sturgess, some hostile state actors also pose a physical threat, which can include state-sponsored assassination. Some states also engage in the abduction of dissidents, or those who have displeased the regime.

The cyber threat

The interconnectedness of modern society provides hostile actors with significant access and opportunity. Both state and non-state actors are able to reach victims across international boundaries, stealing money, data and information, and affecting real-world functions that people rely upon. The cyber threat to the UK is broad, with threats to citizens, government, defence, CNI, academia, business, and many more.

The threat to the UK is also global. Digital connectivity offers an avenue to attacking victims across the world, through often-deniable means. State actors are afforded excellent espionage opportunities and mechanisms to damage adversaries. Criminal actors, likewise, are afforded access to a global market of victims, and operate behind the legal and logistical protection of international boundaries.

Many of these threats begin with hostile actors gaining unauthorised access to computer networks. A variety of methods are used to gain access, from the use of complex electronic attacks to the use of real people – whether insiders, tricked or coerced. Gaining initial access can enable a wide variety of follow-on activity, from theft of information to disruption of service, or the destruction of data. Constant advances in technique mean that this activity is often difficult to detect and defend against.

Examples of these attacks are now ubiquitous around the world. In December 2018, the UK Government and allies held elements of the Chinese Ministry of State Security responsible for a global campaign of cyber espionage, when intellectual property was stolen from managed service providers and their clients. In May 2017, the WannaCry attack locked 200,000 NHS computers, forcing the service to cancel 19,000 appointments at a cost of £20m. In December 2017, the UK Government attributed the Wannacry attack to North Korean actors, who were also deemed responsible for the theft of $81m from the Bank of Bangladesh in February 2016. CNI has also been affected. In December 2015, the BlackEnergy attack on a power facility in Ukraine caused a six-hour power outage, with Russia regarded as responsible by private sector cyber security companies.

Attacks like these are beyond the capability of most terrorist actors, whose activities are usually confined to the disruption of websites and the targeting of specific individuals. Criminals, however, are increasingly effective at monetising cyber activity. This ranges from malign influence (such as convincing someone to make a payment to the wrong person), through to the development of sophisticated tools such as ransomware, which locks an organisation's computer systems until a ransom is paid.

The cyber threat towards the UK will persist as long as it remains an attractive target to hostile actors. The work of the National Cyber Security Centre is focused on making the UK a harder target for those who wish to attack the UK. HMG continues to monitor, defend and deter the threat wherever possible.

Proliferation of weapons of mass destruction

The UK continues to support international efforts to prevent the proliferation of weapons of mass destruction (WMD). Departments across Whitehall continue to work to counter the procurement of WMD-related equipment and materials from UK or international companies.

ANNEX B: EXPENDITURE, ADMINISTRATION AND POLICY

<table>
<tr><th colspan="2">Single Intelligence Account</th></tr>
<tr><td colspan="2">Expenditure in 2017/18</td></tr>
<tr><td>Total budget and outturn</td><td>
<table>
<tr><th>£'000</th><th>Resource spending</th><th>Capital spending</th><th>TOTAL</th></tr>
<tr><td>Budget</td><td>2,443,006</td><td>578,031</td><td>3,021,037</td></tr>
<tr><td>Outturn</td><td>2,407,313</td><td>576,195</td><td>2,983,508</td></tr>
</table>
</td></tr>
<tr><td>Expenditure by category</td><td>• Administration spending: £70m
• Staff pay: £998m
• Capital spending: £576m</td></tr>
</table>

The figures above represent the combined budgets of MI5, SIS, GCHQ, *** and NSS costs for managing the Single Intelligence Account (SIA), as already published in the SIA. The Resource and Capital figures above include Departmental Expenditure Limits and Annually Managed Expenditure, as published in the SIA Annual Resource Accounts.

The Committee has been provided with the individual figures for each Agency; however, these have been redacted in the subsequent pages because publishing them would allow the UK's adversaries to deduce the scale and focus of the Agencies' activities and effort more accurately. This would enable them to improve their targeting and coverage of the Agencies' personnel and capabilities, and seek more effective measures to counter the Agencies' operations against them.

MI5 (Security Service)

Expenditure in 2017/18[12]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	***	***	***
Outturn	***	***	***

Expenditure by category

- Staff costs: ***
- Other revenue costs (including professional services, accommodation, research and development, and IT systems): ***
- Capital costs: ***

Administration

Staff numbers[13]

	Total staff	SCS[14]	Non-SCS
31 March 2018	4,416	50	4,366
31 March 2017	4,210	50	4,160

Recruitment in 2017/18

- MI5 recruited 459 staff, against a target of 550 in 2017/18.
- This compares with 505 staff recruited in 2016/17.

Major projects in 2017/18

- To improve the exploitation and retrieval of MI5's information (in progress).
- To deliver the changes required for MI5 to operate compliantly and effectively under the Investigatory Powers Act 2016.
- To address essential repairs needed to the exterior of Thames House.

Diversity and inclusion

- Achieved fourth place in the Stonewall Top 100 LGBT inclusive employers list.

Policy

Allocation of effort at 31 March 2018[15]

- Islamist terrorism: 67%
- Northern Ireland-related terrorism: 20%
- Hostile State Activity: 13%

Major achievements reported to the Committee for the period 2018-19

- Disrupted two Islamist terrorist plots, bringing the total number of Islamist terrorist plots disrupted since the March 2017 Westminster Bridge attack to 15.
- Played a key role in cross-Government work to identify the Russian intelligence officers who perpetrated the Salisbury attack, resulting in a September 2018 public announcement that the officers in question worked for the GRU (Russia's military intelligence service).
- Assumed overall operational responsibility for tackling higher priority leads and investigations on Right- and Left-Wing terrorism, and the successful disruption of several Extreme Right-Wing terror plots.

[12] As reported to the Committee in MI5's end-year report for the 2017/18 financial year.

[13] These figures refer to the number of full-time equivalent (FTE) staff as at the end of the financial year. MI5 also employs a substantial number of contractors who are not included in these figures.

[14] Senior Civil Service.

[15] Operational allocation of effort (by spend, to the nearest percentage point).

Secret Intelligence Service (SIS)

Expenditure in 2017/18[16]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	***	***	***
Outturn	***	***	***

Expenditure by category

- Staff costs: ***
- Operational expenditure: ***
- Other programme costs: ***
- Capital costs: ***
- Other costs: ***

Administration

Staff numbers[17]

	Total staff	SCS	Non-SCS
31 March 2018	2,866	83	2,783
31 March 2017	2,700	80	2,620

Recruitment in 2017/18

- SIS recruited *** new full-time equivalent (FTE) staff against a target of *** in 2017/18.
- This compares with *** new staff against a target of *** in 2016/17.

Major projects in 2017/18

- To rationalise and increase the capacity of the London estate and, as part of the UK Intelligence Community strategy, to co-locate some capabilities.
- To enhance SIS's capability to draw operational insights from data sets.
- To deliver the changes necessary to ensure SIS compliance with the Investigatory Powers Act 2016.

Diversity and inclusion

- Recognised as a Stonewall Top 100 LGBT inclusive employer.

Policy

Allocation of effort at 31 March 2018

- Key specific geographical requirements and tasks in line with those set out in the National Security Strategy and the Strategic Defence and Security Review 2015, including Russia and Ukraine; Arab Nations; Iran; East Asia; South Asia; Africa, including North Africa; and Latin and South America – around a fifth
- Other operational activities including counter-terrorism; cyber and access generation; defence technology and counter proliferation; and prosperity and economic stability – around a fifth
- Operational support including global network enabling; covert operations; data exploitation; operational security; and operational technology – 24%
- Corporate services including legal and private offices; human resources; finance, estates and business change; IT infrastructure; security and compliance; science, research and innovation; and policy, requirements and communications – 40%

[16] As reported to the Committee in SIS's end-year report for the 2017/18 financial year.

[17] These figures refer to the number of FTE staff as at the end of the financial year. SIS also employs a substantial number of contractors who are not included in these figures.

Major achievements reported to the Committee for the period 2018-19	• Extensive work with GCHQ on a variety of cyber operations around the world. • Worked with partners to follow up leads to disrupt terrorist attack plans and counter Hostile State Activity in the UK and Europe. • Continued to engage in operations to counter and disrupt Islamic State and Al Qaeda, including in Syria and Afghanistan, and responded to emerging terrorist threats across the globe, providing key upstream support to MI5 counter-terrorism investigations. • Provided assurance and significant insights to HMG with relevance to the UK's international relations.

Government Communications Headquarters (GCHQ)

Expenditure in 2017/18[18]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	***	***	***
Outturn	***	***	***

Expenditure by category[19]

- Programme costs (including staff costs, military personnel, private finance initiative costs, the Technical Investment Programme, and non-cash and other programme costs): ***
- Administration costs: ***
- Capital costs ***

Administration

Staff numbers[20]

	Total staff	SCS	Non-SCS
31 March 2018	6,348	82	6,266
31 March 2017	5,922	68	5,854

Recruitment in 2017/18

- GCHQ recruited 686 full-time equivalent (FTE) staff against a target of 612 in 2017/18.
- This compares with 568 (FTE) new staff against a target of 550 in 2016/17.

Major projects in 2017/18

- The Computer Network Exploitation (CNE) Scaling programme, to move GCHQ towards a focus on operations that are conducted on the internet using computer network exploitation techniques.
- The High-End Data Centre Capability, involving the creation of a new high-end data centre (in progress).
- To rationalise and bring together – where appropriate – the provision of technology and services across the three Agencies, enabling enhanced operational performance and delivering efficiencies.

Diversity and inclusion

- Launched REACH – a new staff affinity network for race, ethnicity and cultural heritage.

Policy

Allocation of effort at 31 March 2018

- Mission-specific programmes including counter-terrorism; specific geographical coverage to reflect the threats in the Strategic Defence and Security Review 2015, which include the Middle East, South Asia and former Soviet Union; offensive cyber; serious organised crime; and counter proliferation – ***
- Capability Exploitation[21] – 18%
- Engineering – 19%

[18] As reported to the Committee in GCHQ's end-year report for the 2017/18 financial year.

[19] While the Committee's 2017-18 Annual Report included Annually Managed Expenditure (AME) as a category of expenditure for GCHQ, this has not been included here as AME is not included in the resource and capital spending figures provided in the table above.

[20] These figures refer to the number of FTE staff as at the end of the financial year. GCHQ also employ a substantial number of contractors who are not included in these figures.

[21] Capability Exploitation is the process of finding and exploiting both secret and open source information in support of intelligence and security missions, and ensuring that GCHQ remains at the cutting edge of tradecraft and technology.

	• IT services – 7% • Cyber security – *** • Corporate services (including human resources and finance) – 20%
Major achievements reported to the committee for the period 2018-19	• The public attribution of a large-scale malicious cyber campaign to a group working on behalf of the Chinese intelligence services. • Developed new ground-breaking CNE techniques to assist with investigations. • Launched a new Engineering Accelerator which will allow GCHQ engineers to work with – and learn from – start-ups working on areas such as artificial intelligence and machine learning. • Support to HMRC and the UK finance sector to counter financial crime – for example, by taking steps to prevent the sale of stolen credit card details – thereby preventing fraud and generating significant savings for the taxpayer and the finance sector.

Defence Intelligence (DI)

Expenditure in 2017/18[22]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	345,142	4,234	349,376
Outturn	373,571	-1,579[23]	371,992

Expenditure by category

- Personnel: £238.8m
- Equipment support: £63.2m
- Research and development: £48.2m
- Administration: £48.2m
- Against this, DI received income of £24.9m

Administration

Staff numbers

	Total staff	SCS and military equivalents	Non-SCS and military equivalents
31 March 2018	3,905	7/6	1,292/2,600
31 March 2017	3,878	7/11	1,294/2,564

Recruitment in 2017/18

- In 2017/18, 232 civilian personnel were recruited by external open competition – an increase from 198 in 2016/17.
- Military manning is conducted centrally and the DI military staff is subject to the posting policy of the three Armed Forces. DI does not recruit military staff.

Major projects in 2017/18

- To integrate the capabilities provided by the Defence Geographic Centre and No1 Aeronautical Information and Documentation Unit into the intelligence hub recently formed at RAF Wyton (PRIDE 2).

Diversity and inclusion

- Introduced inclusion training across DI.

Policy

Allocation of effort at 31 March 2018

- Total operational and analysis effort – 83%. This comprises:
  - all source analysis and assessment – 11%
  - collection and analysis – 72 %
- Operational support – 13%. This comprises:
  - Armed Forces security and intelligence training – 11%
  - Armed Forces intelligence policy and future capability development – 2%
- Central support – 4%

Major achievements reported to the Committee for 2018-19

- Continued to contribute to NATO tracking of Russian compliance with the Intermediate Nuclear Forces Treaty.
- Piloted foundation training for the Defence Cyber School.
- Developed new cyber career management structure for DI military personnel.

[22] As reported to the Committee in DI's end-year report for the 2017/18 financial year.

[23] DI's capital spending budget of £4.234m at the start of 2016/17 was reduced in year by the sum of approximately £2.3m, which was reallocated to the Defence Infrastructure Organisation for the delivery of capital works on behalf of DI. The budget was reduced further by approximately £3.5m because of accounting adjustments (including removal of accruals from earlier years, which either did not materialise or were less than previously forecast). In total, these capital spending budget reductions amounted to £5.813m and therefore a negative outturn.

National Security Secretariat (NSS)

Expenditure in 2017/18[24]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	12,403	0	12,403
Outturn	12,105	0	12,105

Due to restructuring within NSS and the Cabinet Office more widely, NSS were not able to provide expenditure figures for only those parts of NSS which the ISC oversees. The figures stated above therefore represent the budget for NSS as a whole (apart from the Civil Contingencies Secretariat) combined with additional Cabinet Office spending funded by the National Cyber Security Programme.

Expenditure by category

- National Cyber Security Programme: £4.0m
- Pay costs: £6.4m

Administration

Staff numbers

	Total staff[25]	SCS	Non-SCS
31 March 2018	121	17	104
31 March 2017	120	10	110

Recruitment in 2017/18

- NSS recruited 31 staff in 2017/18.
- This compares with 14 staff recruited in 2016/17.

Major projects in 2017/18

- None reported.

Diversity and inclusion

- None reported.

Policy

Allocation of effort at 31 March 2018

- Operational (policy teams and private offices) – 76%
- Corporate services – 24%

Major achievements reported to the Committee for the period 2018-19

- Supporting the Department for Digital, Culture, Media and Sport in the delivery of the Telecoms Supply Chain Review.
- Significant developments towards the signing of the UK-US Bilateral Data Access Agreement – a key national security priority – including the Royal Assent of the Crime (Overseas Production Orders) Act in February 2019.[26]

[24] As reported to the Committee in NSS's end-year report for the 2017/18 financial year.

[25] These numbers are in relation to all NSS staff, excluding the Civil Contingencies Secretariat. NSS told the Committee that the number of staff working on areas that the ISC oversees was "*in the region of 40 FTE*", but they were not able to provide more detailed information.

[26] The UK-US Bilateral Data Access Agreement was subsequently signed on 3 October 2019.

Joint Intelligence Organisation (JIO)

Expenditure in 2017/18[27]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	6,058	0[28]	6,058
Outturn	4,085	270	4,355

Expenditure by category

- Pay costs: £3.6m
- Travel: £0.2m
- The remaining outturn is accounted for primarily through refurbishment work to the JIO offices, staff training and other administrative costs.

Administration

Staff numbers

	Total staff	SCS	Non-SCS
31 March 2018	79	8	71
31 March 2017	76	7	69

Recruitment in 2017/18

- The JIO recruited 19 new staff in 2017/18 – the same number as in 2016/17.

Major projects in 2017/18

- The refurbishment of the JIO offices was completed in April 2017.

Diversity and inclusion

- Launched a dedicated Diversity and Inclusion Network.

Policy

Allocation of effort at 31 March 2018

- Total operational activity – 51%
- Corporate services (including central support and intelligence profession) – 49%

Major achievements reported to the Committee for the period 2018-19

- Gaining cross-Government agreement for the establishment of a new Academy of Intelligence Assessment and the introduction of a new Professional Development Framework for the Government assessment community.

[27] As reported to the Committee in the JIO's end-year report for the 2017/18 financial year.

[28] JIO's only capital spending was on the refurbishment of their offices. While their intention had been to complete all refurbishment work in FY16/17, due to delays, some costs were incurred in FY17/18.

Office for Security and Counter-Terrorism (OSCT)

Expenditure in 2017/18[29]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	891,700	105,300	997,000
Outturn	891,700	103,600	995,300

Expenditure by category

- Grants spending: £839.8m
- Staff pay: £45.4m
- Other costs: £110m
- Against this, OSCT received an income of £103.5m

Administration

Staff numbers[30]

	Total staff	SCS	Non-SCS
31 March 2018	724	29	695
31 March 2017	586	24	562

Recruitment in 2017/18

- OSCT recruited 158 staff against a target of 53 in 2017/18 (more staff were recruited than originally planned for, following the terrorist attacks in the summer of 2017).
- This compares with 85 new staff against a target of 88 in 2016/17.

Major projects in 2017/18

- The Communications Capability Development Programme, which was designed to maintain communications data and lawful intercept facilities for the police, wider law enforcement, and security and intelligence agencies. Concluded on 1 April 2018.

Diversity and inclusion

- Introduced a dedicated Diversity and Inclusion Strategy.

Policy

Allocation of effort at 31 March 2018

- National Security Directorate – 26%
- Prevent and Research and Information Communication Unit – 18%
- Protect, Prepare, CBRNE and science and technology – 15%
- Communications Capabilities Development Programme – 15%
- Strategic Centre for Organised Crime – 13%
- Strategy, Planning and International – 13%

Major achievements reported to the Committee for the period 2018-19

- The passage and Royal Assent of the Counter Terrorism and Border Security Act.
- The launch of a new Serious and Organised Crime Strategy.
- The launch of the updated CONTEST Strategy.
- The passage in Parliament of updated rules governing the Investigatory Powers Tribunal and the establishment of regulations which bring in an appeals process.

[29] As reported to the Committee in the OSCT end-year report for the 2017/18 financial year.

[30] Full-time equivalent figures provided.

CCS0620799228
978-1-5286-2091-8