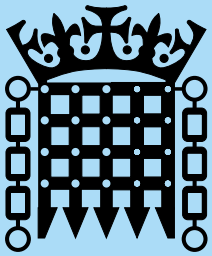

Intelligence and Security Committee of Parliament

International Partnerships

Chairman:
The Rt Hon. Sir Julian Lewis MP

HC 288

Intelligence and Security Committee of Parliament

International Partnerships

Chairman:
The Rt Hon. Sir Julian Lewis MP

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

Ordered by the House of Commons to be printed on
5 December 2023

HC 288

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 978-1-5286-4400-6

E02961539 12/23

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

The Rt Hon. Sir Julian Lewis MP (Chairman)

The Rt Hon. Maria Eagle MP
(from 9 February 2022 until 8 September 2023)

The Rt Hon. Sir John Hayes CBE MP

The Rt Hon. Stewart Hosie MP
(until 14 December 2022)

The Rt Hon. Dame Diana Johnson DBE MP
(until 14 January 2022)

The Rt Hon. Kevan Jones MP

Owen Thompson MP
(from 7 February 2023)

The Rt Hon. Mark Pritchard MP
(until 22 January 2022)

Colonel The Rt Hon. Bob Stewart DSO MP

The Rt Hon. Theresa Villiers MP

Admiral The Rt Hon. Lord West of Spithead GCB DSC PC

The Rt Hon. Sir Jeremy Wright KC MP
(from 9 February 2022)

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 Agencies,* 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). The Committee also scrutinises the work of other parts of the Intelligence Community, including the Joint Intelligence Organisation (JIO) and the National Security Secretariat (NSS) in the Cabinet Office; Defence Intelligence (DI) in the Ministry of Defence; and Homeland Security Group 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

* Throughout the Report, the term 'Intelligence Community' is used to refer to the seven organisations that the Committee oversees; the term 'Agencies' refers to MI5, SIS and GCHQ as a collective; and the term 'Departments' refers to the intelligence and security parts of the Ministry of Defence, Cabinet Office and the Home Office (DI, JIO, NSS and HSG) as a collective, unless specified otherwise.

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.

As part of this process, pursuant to section 3(4) of the Justice and Security Act 2013, following consultation between the Prime Minister and the ISC, the ISC has redacted content from this Report on the basis that the Prime Minister considers that the material will be prejudicial to the continued discharge of the functions of the Security Service, the Secret Intelligence Service, the Government Communications Headquarters or any person carrying out activities falling within the Memorandum of Understanding agreed with the Committee.

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 INQUIRY

1. Intelligence, in the words of one former Chief of SIS, is "*a team sport*".[1] While the UK retains important sovereign intelligence-collection capabilities and the ability to act alone when required, co-operation with international intelligence partners – from close allies to, in certain circumstances, governments and regimes with very different values – is at the heart of the UK's intelligence operating model. As the Heads of the intelligence Agencies and DI have repeatedly (and publicly) stated, such co-operation is firmly in the UK's national interest: we cannot work alone.

2. The gathering of intelligence is, almost by definition, fragmentary; if the whole picture were known, there would be no need for intelligence services to exist to identify the missing pieces of information. Diffuse and sometimes unreliable information must be pieced together to build a bigger picture in order to deliver whatever insight may be required by the Government – whether that is identifying a terrorist plot or uncovering the intentions of a hostile state.

3. The UK's security and intelligence Agencies – along with the other parts of the Intelligence Community, most notably DI – are in a constant battle to find those valuable fragments of information that can be the difference between success and failure – or even, in some cases, between life and death. While the Intelligence Community acting alone may collect some of the jigsaw pieces, the value of this information may only become clear when set against information obtained and shared by their international partners. Moreover, secret information is, by its very nature, difficult to obtain. Political, geographical, technological and cultural factors can limit the ability of any one country to find and extract secret intelligence; and thus it is often only by working in concert with allies that the UK's intelligence services can achieve success.

4. Strong international partnerships act as a vital 'force multiplier', enhancing the ability of the intelligence Agencies, the wider Intelligence Community and the Government to make sense of, and act in, an increasingly complex world. They allow the Intelligence Community to share with allies the burden of countering the most acute threats to our national interests, providing access to intelligence sources and capabilities beyond the UK's reach; and they enable the UK to exert a significant strategic influence on the world stage. Most importantly, they help keep UK citizens safe.

5. The UK's intelligence services have a long history of working closely with international partners. The Second World War ushered in a new era of uniquely close intelligence co-operation between the UK and the United States (US) and, later, with the other partners in what would become the Five Eyes alliance (Australia, Canada and New Zealand). Effective partnerships with western European intelligence services were forged in the shadow of the Iron Curtain. However, there is little doubt that the trend towards greater international working has accelerated since the end of the Cold War. As the old geopolitical certainties of the late twentieth century gave way to a more complex and diverse range of

[1] Oral evidence – SIS, 19 January 2010.

threats to UK interests, the need to work in closer co-operation with a broader range of partners became apparent.

6. This was heightened by the rise of an unprecedented range of international terrorist threats. Speaking in 2021, Sir Alex Younger, the former Chief of SIS, explained how the September 11 attacks in the US had been a catalyst for greater international working. He said that 9/11 had increased SIS's "*understanding of the premium on partnership. We realised that, by and large, we all had the same problem* [with terrorism] *and it was coming from similar places. The days where you could take a not-my-problem or, worse, beggar my neighbour approach to terrorism were well and truly over.*"[2]

7. The same can be said of state threats – particularly, in the UK context, from Russia[3] and China. The expulsion, in 2018, of 153 undeclared Russian intelligence officers by the UK's allies following the Salisbury attack clearly illustrated the power of international partnerships to extend and enhance the UK's security at home and its influence overseas. It remains to be seen whether the Salisbury expulsions represent the apogee of UK co-operation or simply another step towards greater collaboration in the future.

8. While there is no doubt that international co-operation is at the heart of the Intelligence Community's work, and offers many benefits to the UK, we cannot ignore the pitfalls. In many cases, the partners with whom the Agencies have to work do not necessarily share the UK's values, and even those who do may change their approach unexpectedly – a fact to which the Intelligence Community have not always been sufficiently alert (for example, in the way that they reacted to the US's change of detainee policy following 9/11). This Committee has produced a number of Reports that have been highly critical of the actions of the Intelligence Community in this respect, including the *Report on the intelligence relating to the murder of Fusilier Lee Rigby* and *Detainee Mistreatment and Rendition: 2001–2010*.[4] Yet it is inescapable that the Intelligence Community have, in the interests of national security, to work with regimes and organisations which may not be natural allies, and which may engage in practices that would be unacceptable in the UK: indeed, it runs through everything they do.

9. In the course of this Inquiry, therefore, the Committee took a particular interest in matters relating to legal compliance and UK values. Failings such as those identified in the past are unacceptable, and the public and Parliament expect the ISC to hold the Intelligence Community (and the Government more broadly) properly to account. From the evidence provided to this Inquiry there seems now to be a far greater understanding of the issues that must be taken into account, and a significant improvement in the processes and procedures for managing compliance risks since the Committee last examined this issue in detail.

---

[2] Combating Terrorism Center at West Point, 'Twenty Years After 9/11: Reflections from Alex Younger, Former Chief of the United Kingdom's Secret Intelligence Service (MI6)', *CTC Sentinel*, Volume 14, Issue 7 (September 2021).

[3] The Committee concluded taking evidence in this Inquiry in November 2021, before Russia's invasion of Ukraine in February 2022.

[4] The Intelligence Community's response to the change in US detainee policy was examined in the Committee's 2018 Report *Detainee Mistreatment and Rendition: 2001–2010*, HC 1113, June 2018; *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795, November 2014.

10. This was, necessarily, a wide-ranging Inquiry, examining many aspects of the Intelligence Community's work through the lens of international partnerships. The Committee held evidence sessions with the Heads of the three intelligence Agencies, the Chief of Defence Intelligence, and the then Foreign Secretary. It also considered a substantial quantity of written evidence from all of the organisations the Committee oversees. The breadth of the evidence taken reflects the reality of modern intelligence: almost every aspect of intelligence work relies upon, or benefits from, international co-operation.

11. However, this was not, from the Committee's perspective, a straightforward Inquiry. The initial scope of the Inquiry was decided by our predecessor Committee in October 2019, prior to the dissolution of Parliament for the general election. Written evidence was requested from the Intelligence Community in advance of the Committee being re-established following the election. At that point, the Government took the view that it would be inappropriate for it to provide that evidence until the appointment of the new Committee.

12. However, even following the reconstitution of the Committee in July 2020 (eight months after the election) and the reiteration of the Committee's request for evidence, we encountered significant resistance to this Inquiry. On 26 October 2020, the Heads of the intelligence Agencies wrote to the Chairman to request that the Committee reduce significantly the scope of its Inquiry. In the Committee's view, this amounted to an unacceptable attempt by the intelligence Agencies – and by one Agency in particular – to frustrate our ability to scrutinise this important area of their work. Only when the Chairman had again reiterated the Committee's request (on 3 November) did the Agencies provide the full written evidence required (on 23 November). The Agencies' approach resulted in counterproductive and entirely unnecessary delays to the Inquiry.

13. It is a matter of considerable regret that this unsatisfactory situation should have arisen at all. We hope that lessons have been learnt at senior levels in the Intelligence Community about the appropriate way in which to engage with the Committee. The provision of information to the ISC, properly requested under the terms of the Justice and Security Act 2013 and the associated Memorandum of Understanding between the Committee and the Prime Minister, is not a matter for negotiation; it is a statutory obligation on the intelligence Agencies and must be met if public and parliamentary confidence in the activities of the intelligence Agencies is to be maintained.

14. Given the focus of this Inquiry, much of the evidence examined by the Committee is inherently sensitive. It has therefore been necessary to redact certain details from the Report, particularly where these relate to international partnerships that have not been publicly avowed by the Intelligence Community (or by the partner(s) in question). It should therefore be noted that those partnerships named in this report do not represent the totality of those maintained by the Intelligence Community. As always, the Committee has only accepted requests for redaction from the Government where a robust case has been made that publication of the information in question would prejudice the Agencies' discharge of their functions. A short partner profile on one country and a case study on another have also been produced; these are not being published.

15. The Report examines the role international partnerships play, and the importance they have, for the Intelligence Community. It does so with particular reference to the strategy and

mechanisms underpinning the UK's approach to intelligence partnerships; the challenges involved in ensuring that the UK's law and values are not compromised in the course of intelligence co-operation; the vital Five Eyes intelligence partnership; and the Intelligence Community's partnerships with European counterparts, including a consideration of the impact of the UK's departure from the European Union on intelligence co-operation.

16. The Committee reached a number of conclusions, and has made several recommendations, as a result of its Inquiry. These are noted throughout the Report. Overall, we were satisfied with the evidence we received about how the Intelligence Community – and the Agencies and DI in particular – manage and develop their international partnerships. This is particularly the case given the often challenging legal compliance issues inherent in international intelligence co-operation. It was clear to the Committee that Ministers and senior officials recognise the value of these relationships and that appropriate efforts are made to make full use of them in the UK national interest.

HOW PARTNERSHIPS WORK

17. This chapter examines how international partnerships work in practice, including strategy, the role of Ministers, the 'mechanics' of how partnerships are conducted, and what the UK contributes to its various partnerships.

Strategy

18. The National Security Council (NSC), chaired by the Prime Minister and attended by senior Ministers, the National Security Adviser, and the Heads of the security and intelligence Agencies, is the main forum for cross-Government deliberation on matters of national security.

19. In March 2021, the Government published its *Integrated Review of Security, Defence, Development and Foreign Policy* (the 'IR').[5] Responsibility for the implementation of the IR falls to a series of 'priority sub-strategies', each led by a senior official acting as a cross-government Senior Responsible Owner. These sub-strategies are reflected, in turn, in the cross-government Intelligence Outcomes Prioritisation (IOP) process through which SIS and GCHQ (but not MI5 or DI) are formally tasked. Thus, strategies endorsed by Ministers at the highest level of government (the NSC) should have a direct effect on the strategy and priorities of SIS and GCHQ – including international partnerships – albeit via a rather elaborate system of bureaucracy.

20. For all parts of the Intelligence Community, international engagement is driven principally by operational priorities and requirements. This means that the Agencies and DI have sometimes to work with a broader range of partners, or place different emphases on partnerships, than other parts of the Government do. The then Foreign Secretary explained to the Committee:

> *what the Agencies do doesn't just follow the strategic lens that we're pursuing diplomatically or under the* [Integrated Review]*, but, because of the imperatives operationally, they will have relationships which supplement them*.[6]

21. In general, the Agencies and DI manage their own distinct relationships with their liaison partners, developing these as they see fit to ensure their operational and strategic outcomes are met. This arrangement is partly a consequence of the natural development of partnerships over the years, and partly a reflection of the different remit, focus and operational needs of each organisation.

22. Without exception, the partnership with the other Five Eyes countries is – and will remain – the most important element of the Intelligence Community's international engagement. Differences of strategy between the different Agencies and DI are therefore

---

[5] *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy* (the 'Integrated Review') was published on 16 March 2021 and sets out the Government's vision of the UK's role in the world. It contains a number of actions which the Government commits to taking in support of that view. A refresh of the Integrated Review was later published on 13 March 2023 (after evidence-taking for this Inquiry had concluded).

[6] Oral evidence – Foreign Secretary, 22 July 2021.

principally about which other non-Five Eyes partners they engage with; for what reasons (given their different operational requirements and objectives); and to what extent.

SIS

23. Given its foreign intelligence remit and global presence, international partnerships are at the heart of SIS's 'operating model' – more so than the other members of the Intelligence Community. The Chief of SIS explained to the Committee the importance of partnerships to SIS's work:

> *our foreign liaison partnerships are a critical part of our armoury in taking on … threats and meeting them. We have a very clear strategy *** focusing on partners who can help the UK, who can help us to keep our citizens safe and promote UK interests and values overseas, and we tend to look at our partnerships overseas in terms of their ability to work with us* [in terms of willingness, capability and legal compliance].[7]

24. However, there is no one overarching SIS strategy: in written evidence to the Committee, SIS explained that "*strategies for* [international] *engagement are embedded in operational objectives*".[8] As noted above, the IOP process is the means by which SIS is formally tasked, and this feeds through into its international presence and posture.

GCHQ

25. GCHQ describes its approach to international partnerships as being about "*creating a set of relationships that makes GCHQ more operationally capable and strategically influential*".[9] International partnerships are seen as a "*critical enabler*" that allows GCHQ to be "*a globally-capable intelligence and security agency*"; to "*reach data*"; and to access "*a level of technical capability far beyond what the UK could afford alone*".[10]

26. In addition to the Five Eyes, with which GCHQ enjoys an unparalleled level of co-operation, GCHQ's International Relations Strategy sets out an ambition to *** and *** – with a range of 'strategic partnerships' identified as key to achieving this (***).[11]

27. The National Cyber Security Centre (NCSC), while part of GCHQ, maintains its own set of international partnerships in order to assist with the delivery of its operational objectives, such as improving the global response to cyber incidents, and wider Government priorities like shaping the international debate on strategically critical matters such as cyber policy (including, crucially, discussions with US technology companies).[12] Sometimes the department or agency with which NCSC engages in a given country will be different from that with which GCHQ works; however, the Committee was assured that the NCSC's activity is aligned with broader HMG objectives.

---

7 Oral evidence – SIS, 27 May 2021.
8 Written evidence – SIS, 15 January 2021.
9 Written evidence – GCHQ, 2 November 2020.
10 Written evidence – GCHQ, 2 November 2020.
11 Written evidence – GCHQ, 23 November 2020.
12 Written evidence – GCHQ, 2 November 2020.

MI5

28. In evidence to the Committee, MI5 summarised its overall strategy regarding international partnerships as follows:

> *MI5's international partnerships are driven by our core mission to protect UK national security. MI5 will consider engagement with a foreign liaison service if we identify a requirement to do so, and where we judge that such engagement is necessary, proportionate, and in the interests of UK national security*.[13]

29. The Director General explained to the Committee the main recent operational imperatives that have led to a change in MI5's approach to partnerships:

> [MI5's] *partnerships have evolved organically over the last few years in some interesting and deep ways, in particular the twin drivers: one the effect of Syria on deepening European collaboration, and alongside that the resurgence in state threats, most prominently through the Salisbury attack.*[14]

30. In 2018, MI5 reviewed its approach to working with international liaison partners to "*bring greater structure to, and governance over, our relationships and to underpin our ambition to engage beyond our core investigative work on the development of new operational technology and capability*".[15] A key recommendation of the strategy review was to apply greater rigour and energy to the management of *** key 'strategic' international partnerships for MI5 ***; this has since been done, with *** posts supporting these partnerships.[16]

31. MI5 has a team responsible for managing its international partnerships and overall strategy. However, day-to-day engagement is typically led by the relevant operational team rather than being controlled centrally.[17]

Defence Intelligence

32. DI's recently updated international engagement strategy notes that "*the evolving global security context, BREXIT, HMG's* Global Britain *initiative and the need to deliver modernisation at a fast enough pace means DI will continue to work closely with international partners*".[18]

33. In evidence to the Committee, DI summarised its core purposes for maintaining international partnerships as follows:

> *Firstly,* [DI] *obtains intelligence and insights from its international partners to illuminate understanding of issues and events that DI's customers have identified as intelligence requirements … There is an expectation in these relationships that DI will give and receive intelligence about common interests.*

---

13 Written evidence – MI5, 23 November 2020.
14 Oral evidence – MI5, 17 June 2021.
15 Written evidence – MI5, 2 November 2020.
16 Written evidence – MI5, 15 January 2021; Written evidence – MI5, 3 June 2021.
17 Written evidence – MI5, 2 November 2020.
18 Written evidence – DI, 14 May 2021.

> *Second, international intelligence co-operation led by DI assists in furthering a range of broader strategic outcomes for the Department ***. Such intelligence co-operation may, for example, be for the purpose of *** promoting peace and stability agendas.*[19]

34. DI's highest priority partners are the Five Eyes, ***.[20] In line with broader Government strategy, DI is looking to bolster its ties with the Indo-Pacific region, particularly ***; however, Five Eyes and NATO allies will remain the priority.[21]

35. Unlike the Agencies, DI has no independent statutory basis and is an integral part of the Ministry of Defence (MoD). Therefore, while its activity is 'informed' by the IOP process, its priorities are driven by wider MoD requirements.[22] This is as true of its international engagement work as it is for its intelligence collection efforts, and means that DI's international engagement priorities will not always align directly with those of the Agencies. Where there are differences with the Agencies, these are likely to be a matter of emphasis on a given partnership, as opposed to a substantially different approach to intelligence sharing. The overlap between the UK's strategic defence, security and diplomatic objectives is such that, broadly speaking, DI will maintain similar partnerships to the Agencies.

A. Even within a well-integrated intelligence community such as that in the UK, varying operational imperatives mean it is inevitable that there will be differences of strategy between organisations when it comes to their international partnerships. This should not be problematic provided there is effective co-ordination between the different organisations engaging with foreign partners.

B. In the Committee's view, MI5, GCHQ and DI each have overarching strategies appropriate to their distinct functions and operational priorities. While we recognise that SIS's tasking via the Intelligence Outcomes Prioritisation helps give focus and direction to its many important international partnerships, we were surprised that SIS does not have a single overarching strategy for managing these, even at a high level. The Committee recommends that SIS follow the lead of GCHQ – which receives its tasking via the same process – and develop a standalone international partnerships strategy.

C. It is important that co-ordination between all three Agencies and DI remains strong. In particular, care should be taken that MI5 and DI, which are not tasked through the Intelligence Outcomes Prioritisation process, are nonetheless aligned with SIS and GCHQ where this is appropriate, and that the Agencies take care to read across to DI's strategy, which is derived from the Ministry of Defence's broader strategies and plans.

---

[19] Written evidence – DI, 3 November 2020.

[20] The Defence Geographic Centre, a part of DI which is responsible for meeting the Armed Forces' mapping needs, also maintains a very wide range of relationships with international counterparts, which often do not align neatly with other partnerships maintained by DI; Written evidence – DI, 17 September 2021.

[21] Written evidence – DI, 17 September 2021.

[22] Written evidence – DI, 4 May 2020.

D. The introduction of the Fusion Doctrine in 2018 saw policy departments across the Government brought into national security work. There is therefore also a need for the three Agencies and DI now to co-ordinate their engagement with foreign partners with policy departments' own international strategies.

The role of Ministers

36. Ministerial involvement in the Intelligence Community's international partnerships falls into three broad categories:

(i) setting high-level strategy, at both a whole-of-government and departmental level;

(ii) providing formal ministerial direction and legal authorisation for international activity, usually through the approval of warrants, authorisations and submissions; and

(iii) direct engagement with counterparts – an extension, broadly speaking, of traditional diplomacy.

37. As noted above, the NSC is the main forum for Ministers to set national security strategy at a whole-of-government level; strategies developed at this level feed into the IOP process. Most direct ministerial engagement in international intelligence partnerships takes place at the departmental level.

38. Of senior Cabinet Ministers it is the Foreign Secretary, under whose authority SIS and GCHQ operate, who plays the most significant role in the Intelligence Community's international work. The Foreign Secretary is consulted by SIS and GCHQ in relation to international partnerships when intelligence sharing or joint operations would involve political or legal risk; such submissions may also encompass MI5 work overseas when it is done in collaboration with SIS. This responsibility for approving submissions relating to international work is – along with approving warrants and authorisations for the use of intrusive powers or activity which would otherwise break UK law – one of the most important aspects of the Foreign Secretary's role. It is explored in further detail later in this Report.

39. Through their working relationship with the Chief of SIS and Director GCHQ, and their own engagement with foreign leaders, the Foreign Secretary also plays an informal, but nonetheless important, role in shaping international partnership priorities. The then Foreign Secretary explained to the Committee that he regularly discussed SIS's international engagement priorities with the Chief of SIS:

> *then typically for example 'C'* [the Chief of SIS] *will say to me "I'm thinking of engaging with X or Y" and, you know, normally I'll say it's a very good idea. Sometimes I've gone to him proactively on my own initiative and said "quite how much are we doing with A or B".*[23]

[23] Oral evidence – Foreign Secretary, 22 July 2021.

The Committee asked about the extent to which the then Foreign Secretary personally engaged with foreign counterparts on intelligence matters. He told us:

> *my time is spread across a whole range of competing priorities but, yes – absolutely. I think the truth is what you'd want me to be doing is strategically agreeing what the parameters are* [of the issue at hand] *with my opposite numbers and then we've got a clear steer that the Agencies … go and deliver*.[24]

40. Given that MI5 does not routinely carry out operations overseas (and some MI5 international work is carried out in conjunction with SIS and is therefore approved by the Foreign Secretary) there is a lesser requirement for the Home Secretary – under whose authority MI5 works – to take an active role in the international aspects of MI5's work. MI5 told the Committee:

> *in instances where MI5 relies on an SIS Ministerial submission …* [MI5 will] *forward these to the Home Office …* [and] *the Home Office will also be provided with a summary of MI5's specific use of the submission. The Home Office then take responsibility for ensuring that Ministers are appropriately informed.*[25]

41. Ministerial oversight of MI5's international partnership work is also maintained through annual reports to the Home Secretary and Prime Minister, and through the recently developed Ministerial Assurance Group (a forum for the Home Office to exercise its executive oversight of MI5's work – including its international partnerships).[26] Director General MI5 told the Committee that, through these mechanisms, the Home Secretary "*… has a good feel for quite a wide range … of international engagement that we're doing the whole time*".[27] He added that, if the Home Secretary is meeting foreign ministerial counterparts, MI5 might provide an update on operational priorities relevant to the policy-level conversations, to help inform discussions.[28]

42. DI's international partnerships typically do not require ministerial authorisation. The Chief of Defence Intelligence (CDI) told the Committee that ministerial submissions to the Defence Secretary on international matters are "*a relatively rare phenomenon*" and are generally only required when an issue is "*novel and contentious*" – for instance, certain aspects of DI's intelligence sharing with ***.[29] However, the CDI explained to the Committee that he will consult ministers when required to help advance DI's international work:

> *it may be that sometimes I would submit to ministers … to make sure* [they] *are aware of what I'm doing in order that it can shape their own activity in their own* [international] *relationships*.[30]

---

24 Oral evidence – Foreign Secretary, 22 July 2021.
25 Written evidence – MI5, 15 January 2021.
26 Written evidence – MI5, 15 January 2021.
27 Oral evidence – MI5, 17 June 2021.
28 Oral evidence – MI5, 17 June 2021.
29 Oral evidence – DI, 10 June 2021.
30 Oral evidence – DI, 10 June 2021.

Use of instant messaging applications

43. Speaking to the Committee about his interactions with foreign counterparts, the then Foreign Secretary noted that the instant messaging application WhatsApp is now frequently used as a means of making quick contact – for instance, in order to make sure a foreign counterpart is aware of a particular urgent issue, without the need to wait for the message to be passed through the respective countries' bureaucracies:

> *If* [the issue at hand] *is time sensitive,* [WhatsApp] *stops you having to go through embassies, ambassadors, and take a long time to do it*.[31]

44. The use of WhatsApp (and other similar instant messaging applications) in relation to the conduct of government business, and the maintenance of appropriate audit trails, is a wider security and propriety issue and is not the subject of this Inquiry. Nonetheless, given the context of discussions regarding sensitive international intelligence partnerships, the Committee felt it appropriate to seek assurances that messaging applications are not used to exchange any classified information with foreign counterparts. Writing to the Committee, the then Foreign Secretary said:

> *WhatsApp is not used for correspondence above the security classification OFFICIAL, and so is never used for the development of foreign policy decisions, all of which are at a higher security classification. For the avoidance of doubt, I do not use WhatsApp for any issues relating to intelligence, or to the organisations which the Committee oversees.*[32]

45. The Committee also requested, and was provided with, the Foreign, Commonwealth and Development Office guidance on the use of messaging applications for official business, including the retention of records.

E. The Committee is satisfied that arrangements for ministerial engagement with the Intelligence Community's international partnerships are mature and proportionate.

F. While most interaction with foreign liaison partners is best carried out between intelligence professionals, the Intelligence Community should continue to be alive to opportunities for Ministers to engage with foreign counterparts on intelligence matters where this is appropriate. In addition, it may be beneficial for the Home Secretary to receive submissions on MI5 and SIS/GCHQ joint activity with foreign partners in parallel with the Foreign Secretary rather than simply receiving a copy for information afterwards.

G. The Committee was satisfied that instant messaging applications are not used for the exchange of classified information with foreign counterparts. Nonetheless, it is essential that audit trails are maintained of diplomatic exchanges that are made using these means – not least so that retrospective oversight can be applied by Parliament should this be required.

---

[31] Oral evidence – Foreign Secretary, 22 July 2021.

[32] Written evidence – Foreign Secretary, 3 August 2021.

Mechanics

(i) The SIS global network

46. Fundamental to the work of SIS, and the Intelligence Community more broadly, is a network of intelligence officers posted overseas to conduct operations and maintain liaison relationships with international partners. Given its foreign intelligence remit, SIS takes the lead on this network for the Intelligence Community and manages the overseas offices (usually known as 'stations').

47. SIS is responsible for building, maintaining and securing stations, and providing a platform from which SIS officers can meet and recruit agents and conduct other operations, and for Intelligence Community personnel to meet with their counterparts in the host country. Almost all stations are ***. Likewise, a *** becoming widely known.[33]

48. There are currently *** personnel from the Agencies and other government departments posted overseas in *** countries as part of the global network, maintaining partnerships with *** counterpart organisations.[34] Of these, *** are SIS officers, with the remainder comprising personnel from MI5, GCHQ, *** Counter Terrorism Policing.[35]

49. By international standards, SIS has an extensive overseas network, and the Agency considers itself to be one of the few intelligence agencies with a global reach. The Chief told the Committee: "*my ambition basically is that we are a global service and we should be represented as broadly across the globe as we possibly can be*".[36] However, budgetary constraints mean that, inevitably, tough prioritisation decisions need to be made about how resources are distributed and where new stations should be opened and closed. In addition, the potential intelligence gains from opening a new station, as well as the physical risk and counter-intelligence threat to staff, are taken into account.

50. Opening a new station is not a straightforward business. SIS explained that it is "*a significant investment because of the* [security] *apparatus we have to put in around it … It's not an easy thing to do*."[37] However, although opening an SIS station requires a substantial lead time due to the infrastructure and security requirements, investments in new technology have allowed SIS ***.[38] Furthermore, SIS told the Committee that, where they make a decision not to have a station in a given country, they can often rely on partners ***.[39] (For example, ***.[40])

51. In addition to practical considerations around budgets, productivity and security, opening and closing stations can have serious implications for the partnership in question. The Chief of SIS told the Committee:

---

33 Written evidence – SIS, 23 November 2020.
34 Written evidence – SIS, 2 November 2020.
35 Written evidence – SIS, 15 January 2021.
36 Oral evidence – SIS, 27 May 2021.
37 Oral evidence – SIS, 27 May 2021.
38 Written evidence – SIS, 16 October 2020.
39 Oral evidence – SIS, 27 May 2021.
40 Oral evidence – SIS, 27 May 2021.

> *at one level we would be prepared to fold our tent and move on if we just weren't getting anywhere, but … it's not a decision you take lightly. Not surprisingly, countries and* [partner] *services are not particularly enamoured of us if we're there for a short period, then we close, then we want to come back … they notice and it's not a good policy.*
>
> *So, ultimately you can't keep somebody there where there's no benefit but we'll try quite hard to get the benefit and I certainly would be very focused on making sure that we don't go in and out like some sort of a concertina … because you need to look after the relationships there.*[41]

However, on occasion, the threat to personnel is such that stations have to be closed at short notice – ***.[42]

52. Although SIS leads the global network and has by far the largest overseas representation of the Agencies, SIS station heads are expected to represent the whole Intelligence Community, particularly in countries in which MI5 and GCHQ do not have any officers present. Asked how effectively this system worked, MI5 told the Committee that SIS station heads "*faithfully and professionally – and often excellently – represent the overall UK* [Intelligence Community] *need and not, as it were, the narrower institutional interests of SIS*".[43]

H. The SIS global network of stations overseas is a vital enabler for the work of the Intelligence Community, including the maintenance of international partnerships. While the Committee recognises that financial pressures will always require decisions to be made on the value for money provided by each station, SIS should maintain a general ambition to grow, rather than consolidate, its global footprint.

(ii) Broader Intelligence Community overseas presence

53. In addition to the SIS-led global network, MI5, GCHQ and DI all have an overseas presence, albeit on a more limited scale:

- MI5 has a network of around *** officers posted overseas carrying out a range of *** duties. These include *** attachments to SIS or GCHQ overseas.[44] MI5 also deploys staff overseas on temporary duty assignments.
- MI5 also has ***[45]
- GCHQ has around *** staff based overseas, ***.[46] Many of these personnel are ***.
- ***[47]

[41] Oral evidence – SIS, 27 May 2021.
[42] Written evidence – SIS, 20 October 2021.
[43] Oral evidence – MI5, 17 June 2021.
[44] Written evidence – MI5, 2 November 2020.
[45] Written evidence – MI5, 3 June 2021.
[46] Written evidence – GCHQ, 3 August 2021.
[47] Written evidence – GCHQ, 3 August 2021.

- DI has around *** liaison *** staff posted to the Five Eyes countries; a small number of personnel are also posted to NATO, ***. More broadly, DI relies on the Defence Attaché network to support its global intelligence network. Following the IR, DI intends to expand this overseas network.[48]
- ***
- ***[49]

(iii) Intelligence sharing

54. The exchange of information is at the heart of international partnerships; it is the foundation on which further co-operation is built. Indeed, for some partnerships maintained by the Intelligence Community, ad hoc intelligence sharing based on mutual interest will be the only substantive co-operation that takes place.

55. Nevertheless, intelligence sharing still requires trust, and the level of trust between partners generally determines the nature and scale of the intelligence sharing between partners (alongside an understanding of compliance regimes, appropriate safeguards and the level of mutual benefit). *** the Intelligence Community might share *** (with appropriate safeguards in place); ***, are likely to be shared.

56. The 'control principle' is essential in maintaining that trust between partners. Intelligence Agencies share information on the basis that they retain ownership of it: neither the information itself, nor the fact that it has been shared, will be disclosed directly or indirectly by the receiving state without explicit permission to do so being granted by the originating Agency.[50] The purposes of this are to protect the information and also to avoid 'circular reporting' of intelligence, whereby (in SIS's explanation) "*information could mistakenly be taken as corroborating a version of the same information already received directly by the second party from the same third party*".[51] This latter point is of critical importance in evaluating intelligence and demonstrates the importance of all parties rigorously observing the control principle.

57. A violation (real or perceived) of the control principle would likely result in further intelligence being withheld due to protection concerns, or otherwise extreme political turbulence in the relationship. In evidence to the Iraq Inquiry, one SIS officer explained the central importance of trust when it comes to intelligence sharing:

> *I think there's a sort of protocol. There has to be a protocol, about preserving the integrity and security of reporting you get from one liaison service. They are a source. If you compromise that ... you damage the trust that is the basis of that exchange.*[52]

58. A 2010 Court of Appeal decision requiring that certain intelligence originating from the US be published in an open court judgment is a case in point: the publication of this

[48] Written evidence – DI, 14 May 2021.
[49] Written evidence – MI5, 3 June 2021.
[50] In this context we note also the importance of the 'third party rule', which is used in the UK to refer to the convention that material provided by one third party cannot be shared with another.
[51] Written evidence – SIS, 23 November 2020.
[52] The Iraq Inquiry, *Transcript of oral evidence from SIS*, 2010.

material was a clear breach of the control principle, and caused strain in the UK–US intelligence-sharing partnership.[53] This example is explored in further detail later in this Report.

59. The nature of intelligence shared and received by the Intelligence Community can take many forms, for example:

- intelligence reports (i.e. it has been analysed and summarised);
- information identified in an intelligence agency's databases in response to a 'trace request' from another agency (e.g. information relating to a particular terrorist Subject of Interest);
- bulk datasets; and
- raw intelligence (i.e. in its original form).

60. Such information may be automatically or routinely shared as part of some bilateral and multilateral partnerships (most notably the Five Eyes alliance); it may be shared in response to the specific operational requirements of the requesting agency (i.e. an ongoing operation); or it may be unsolicited intelligence which, though it can vary greatly in subject matter, reliability and usefulness, is nonetheless often crucial to the Intelligence Community's work.

61. Due to the varied nature of information exchanged with partners it is difficult meaningfully to quantify the scale of intelligence sharing in which the Intelligence Community engage. However, by way of example, the Committee was told that MI5 alone received over *** intelligence reports from Five Eyes partners in the year to November 2020.[54]

(iv) Joint operations

62. Joint operations – the use of shared intelligence and capabilities in order to achieve a real-world effect – are one way in which intelligence partners might co-operate. Joint operations vary widely in nature, scale and objective. For example, in the case of MI5, joint operations might take the form of a joint investigation into a shared security threat, potentially including the subsequent disruption of that threat; while in the case of SIS it could involve the joint ***.

63. As with intelligence sharing, and generally to a significantly greater degree, joint operations require trust on all sides due to the inherent risks of sharing information on tradecraft, methodology and investigative priorities. SIS explained to the Committee that building up this trust is a slow but necessary element of its work:

> *if you're up against a pretty ferocious counter-intelligence threat in* [a country being targeted in a joint operation]*, you've got to be pretty sure that the people you're working*

[53] *R (on the application of Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2010] EWCA Civ 65. The case in question concerned the mistreatment, in US custody, of Binyam Mohamed, an Ethiopian national and UK resident.

[54] Written evidence – MI5, 15 January 2021.

> *with are not penetrated by that other country … so you take it pretty slow and you make sure you're pretty sure of your partner*.[55]

64. Legal and compliance issues are central to the decision-making process in relation to joint operations. The intelligence Agencies do not ask international partners to undertake operations that would be unlawful in the country of those partners.[56]

Case study: Disruption of *** terrorist plot

***[57]

(v) Joint capability development and operation

65. With some partners the Intelligence Community engage in joint development of new capabilities – to increase the ability to collect intelligence, enable new forms of 'effects' operations (i.e. delivering a real-world effect on the basis of intelligence) and overcome adversaries' ***.

66. This, too, requires deep levels of trust. In order to share sensitive information on capabilities, the Agencies need to be sure that, for political, legal and ethical reasons, the technology or expertise in question will not be misused – ***. As such, the most systematic collaboration on capability development and operation takes place with the Five Eyes partners, with much of the Agencies' work led by a jointly run team.[58]

Case study: *

***[59]

(vi) Capacity building

67. As with many other parts of government, the Intelligence Community engage in capacity building with some allies – training them in certain skills or capabilities. Amongst the Agencies, this work is generally led by SIS, with the other Agencies providing support as necessary. SIS told the Committee:

> *We train a whole range of different skills with partners, *** … increasingly our work on capacity building has grown out from counterterrorism into things like ***, for example*.[60]

68. Capacity building by the intelligence Agencies is strategically aligned with broader cross-government capacity-building efforts, and seeks to tackle the drivers of conflict and

55 Oral evidence – SIS, 27 May 2021.
56 Written evidence – SIS, 23 November 2020.
57 Written evidence – GCHQ, 9 June 2021.
58 ***
59 ***
60 Oral evidence – SIS, 27 May 2021.

instability overseas. It is also an investment in a particular partnership with the aim of supporting the partner in question to develop in a specific area that can better help the UK Intelligence Community meet their own operational objectives. SIS explained that there are political, ethical and legal reasons why there may be limits placed on the capabilities they will seek to provide or develop as part of capacity-building initiatives.[61]

69. A significant proportion of the Agencies' capacity-building work is ***.[62] The Foreign Secretary has ministerial accountability for the Agencies' capacity-building expenditure, which must adhere to the same rules and guidelines as all other capacity-building spending across government ***.[63] Questioned by the Committee on the Agencies' capacity-building expenditure, the then Foreign Secretary was strongly supportive:

> *I think it's good value for money. I can think of stuff we've funded in *** and other areas, in ***, where it has been good value for money. The truth is there's a lot of pressure on* [spending] *right now, so we have to make sure that it is really delivering bang for our buck. But I don't think that there's any misuse of* [capacity-building funds] *in the Agency space. If anything, I'd love to put more into it, but we've got to cut our cloak according to our cloth*.[64]

Case study: *

In evidence to the Committee ***, SIS cited a capacity-building project to provide *** as an example of an effective project financed through a combination of *** tri-Agency funding.

The capability helped disrupt numerous terrorist attacks and made a significant contribution to the security of UK ***.[65]

I. The Committee is supportive of the Intelligence Community's capacity-building efforts. However, working with some partners carries inherent risk, and the Agencies must continue to take great care about what capabilities they choose to share with which countries and to ensure robust safeguards are put in place (including the ability to withdraw if this becomes necessary).

(vii) Joint units

70. In addition to capacity building, the Agencies (primarily SIS) engage in 'joint units' with the intelligence services of certain international partners: these are generally partners with *** than the UK Intelligence Community, but which are recognised as being of current or potential intelligence value. SIS explained to the Committee that, unlike straightforward capacity building which promotes the security and stability of the host nation, joint units –

[61] Oral evidence – SIS, 27 May 2021.
[62] Written evidence – SIS, 16 October 2020.
[63] Written evidence – SIS, 2 July 2021.
[64] Oral evidence – Foreign Secretary, 22 July 2021.
[65] Written evidence – SIS, 2 July 2021.

which may be trained, funded and/or tasked by HMG – also support the Agencies' intelligence requirements and, as the Chief of SIS explained, "***".[66]

71. SIS is currently engaged in over *** joint units – which may be trained, funded and/or tasked by HMG – with a range of international partners. Most of the units ***.[67] The nature of the activity undertaken by such units varies widely, from ***.[68] Given that many of these units are not under the exclusive control of HMG (most will also be working to requirements set by their own government) ***.[69]

72. Joint units provide many operational benefits to SIS in the country in question, *** and enable SIS to generate trusted and capable partnerships that, over time, are likely to pay operational dividends. There can, however, be compliance risks attendant with some such units when HMG initiates, tasks or engages in operations, since HMG may then be legally and morally responsible for the actions of the unit. We return to this issue in the chapter on Law and values.

73. The Chief of SIS cited *** as an example of an effective joint working approach that is mutually beneficial for both parties:

> *of the *** have captured over the last ten years, *** of that has come out of *** and built the capacity of ... So it has a real impact in the real world on their ability to do things which are supportive of our interests*.[70]

(viii) Liaison with UK-based foreign intelligence officers

74. The Agencies, with support from the wider Intelligence Community, are responsible for liaising with UK-based foreign intelligence officers who have been 'declared' to the UK authorities (i.e. intelligence officers whose presence in the UK has been admitted – and accepted by the UK – for intelligence liaison purposes, as opposed to 'non-declared' intelligence officers working clandestinely under diplomatic cover). London is host to declared foreign intelligence officers from both close allies and strategic adversaries, and as such the relative risk posed by these individuals varies widely.

75. MI5 requests that UK-based liaison officers comply with a set of guidelines regarding their activities in the UK. The guidelines include ***.[71] MI5 states that "*all liaison services must comply with the terms set out in these guidelines* ***".[72]

76. MI5 can also deliver an official reprimand or warning to foreign liaison officers in response to unacceptable activity carried out by their country or intelligence service. For example, ***.[73]

---

66 Oral evidence – SIS, 27 May 2021.
67 Written evidence – SIS, 2 July 2021.
68 Written evidence – SIS, 2 July 2021.
69 Oral evidence – SIS, 27 May 2021.
70 Oral evidence – SIS, 27 May 2021.
71 Written evidence – MI5, 15 January 2021.
72 Written evidence – MI5, 15 January 2021.
73 Written evidence – MI5, 3 February 2021.

77. The Committee questioned MI5 as to how effective their 'guideline' regime was for foreign intelligence officers. The Director General told us:

> *we … have absolutely no objection to investigating intelligence service officers in this country who are doing things which are contrary to the UK's national interest* ***.[74]

78. Although MI5 *** investigating the activities of Russian, Chinese and Iranian intelligence officers in the UK, MI5 also provided the Committee with *** case studies involving malicious activity carried out by intelligence officers from countries that would not generally be considered to pose an acute threat to the UK's national security ***.[75]

(ix) Intelligence diplomacy

79. A further important aspect of international partnerships work is 'intelligence diplomacy', which HMG defines as "*the use of intelligence information and relationships to influence international action*".[76] This activity sits at the nexus between traditional intelligence work and diplomacy, and ranges from using intelligence partnerships to build alliances or encourage action on a particular issue, to the maintenance of alternative diplomatic channels with governments or non-state actors with which it is considered impolitic to have overt diplomatic relations. Even though this work is not considered to be 'covert', it nonetheless remains secret (and indeed secrecy is often fundamental to its continued success).

80. The most notable recent example ***.

81. An immediate ***, even in cases where relying on the broader diplomatic relationship alone might have resulted in a less supportive outcome.

82. Alternative channels can also allow HMG to play a role in facilitating diplomatic and military compromises and agreements in situations where the relevant parties cannot, ***, be seen publicly to be negotiating. An example of this type of work was provided to the Committee in evidence ***.[77]

83. At other times, alternative channels can allow HMG to communicate covertly with a foreign government with which overt political and diplomatic relations are considered – for whatever reason and for however long – sensitive. For example, in evidence to the Committee, it was explained that the main purpose of HMG's limited engagement and co-operation ***.[78] The Committee acknowledged and supported this limited engagement ***.

84. More broadly, by virtue of their often strong personal relationships with key figures in the security and intelligence establishments of many countries (particularly in less democratic regimes), as well as their relatively high profile and name recognition in the world of intelligence, the Agencies can sometimes 'open doors' for Ministers and senior officials to meet senior figures to whom access may be difficult to arrange through diplomatic channels.

---

74 Oral evidence – MI5, 17 June 2021.
75 Written evidence – MI5, 20 July 2021.
76 Written evidence – SIS, 15 January 2021.
77 Written evidence – SIS, 15 January 2021.
78 Written evidence – SIS, 23 November 2020.

The then Foreign Secretary noted the "*Heineken effect*" that the Chief of SIS and the Heads of the other intelligence Agencies have: "*the 'brand' of SIS and the other Agencies is particularly strong and you can see that with the access we get to people*".[79] In addition, SIS told the Committee: "*sometimes we are able to address sensitive issues more frankly than our diplomatic colleagues*".[80]

85. However, SIS is wary of allowing political considerations to feature strongly in an intelligence partnership – both because to do so could put the partnership at risk should the political relationship deteriorate, and because it may convey the impression that intelligence discussions have a primarily political motivation: "*if you start introducing political arguments and pressure into an intelligence exchange, you run the risk of undermining your credibility*".[81]

J. Intelligence diplomacy is an important aspect of modern international intelligence partnerships. * partnerships can be utilised in the national interest when co-ordinated with the Government's other levers of international influence. Ministers and policy departments should continue to be alive to the Intelligence Community's ability to have a tangible influence on broader diplomatic objectives.**

The UK's contribution to its partnerships

86. As noted above, the UK benefits greatly from its international partnerships – they provide the UK with access to intelligence that would otherwise be very difficult, or impossible, to obtain by other means. The question is what the UK Intelligence Community can offer their international counterparts – what capabilities and characteristics they have with which to reciprocate and which, in combination, might make the UK a valuable and sought-after intelligence partner.

(i) ***

87. Some of the UK's influence in intelligence matters is a result of ***, in combination with strategic capability investments over the years. ***. This makes a very significant contribution to GCHQ's ability to meet its operational requirements, ***.

88. ***[82]

K. The UK's overseas collection facilities are indispensable in terms of the contribution they make to the UK's national security, and the Intelligence Community should continue to exploit them for intelligence gain. Ministers should also ensure that broader government policy – * – fully takes into account such intelligence considerations.**

[79] Oral evidence – Foreign Secretary, 22 July 2021.
[80] Written evidence – SIS, 2 July 2021.
[81] Oral evidence – SIS, 27 May 2021.
[82] ***

(ii) Niche capabilities and expertise

89. In addition to ***, the UK Intelligence Community bring, in the words of Director General MI5, "*quite a bit of capability, intellectual capital, experience and expertise*" to their partnerships – attributes highly valued by their intelligence partners.

90. The UK's partners, ***, prize highly GCHQ's mathematical capabilities – where GCHQ "*punch*[es] *way above* [its] *weight*" – and technical expertise, for example on ***. The NCSC, which GCHQ describes as a "*global leader on cyber security*" and a "*crown jewel*" in the UK's capability, is also recognised as being world-leading and a model that several other countries are now seeking to emulate.[83]

91. The UK Intelligence Community are also recognised by Five Eyes and European partners as having significant expertise on the threat posed by the *** – as evidenced by the ***. Other *** are also areas of relative strength: for instance, the CDI described DI's experts on the *** as "*absolutely world-leading*" and recognised as such by allies.[84]

92. In addition, close *** with certain countries *** – for instance *** – afford the UK intangible and hard-to-replicate *** their leaderships and security establishments. These ties are ***.

L. It is clear to the Committee that the UK's relative strength across a broad range of intelligence disciplines and subject matters makes it a partner of choice for many countries. The Intelligence Community should continue to foster this reputation – which, like all reputations, is hard won and easily lost.

(iii) 'Forward leaning' approach to co-operation

93. In the evidence the Committee considered throughout the course of this Inquiry, it was clear that the Intelligence Community take a 'forward leaning' approach to international partnerships, in the sense of seeking actively to develop them beyond the merely transactional.

94. Among like-minded countries the UK may at times contribute more to a relationship than it receives in return. ***.[85] However, it is important to note that all such relationships ebb and flow, with circumstances and relative strengths and expertise dictating which party is taking the leading role.

95. Being a 'net contributor' to an intelligence partnership is not, in the Intelligence Community's case, an act of altruism. By moving the relationship beyond the transactional, they help build a reputation of reliability and a store of trust between the parties, which is likely to be reciprocated further down the line – thereby helping keep British people safe at times of acute threat. The CDI explained to the Committee how important it is to invest in relationship-building in this way: "*... if you haven't built that trust relationship in advance of a time of crisis, it's really hard to build it at that time*".[86]

---

[83] Written evidence – GCHQ, 2 November 2021; Oral evidence – GCHQ, 1 July 2021.
[84] Oral evidence – DI, 10 June 2021.
[85] Oral evidence – SIS, 27 May 2021.
[86] Oral evidence – DI, 10 June 2021.

96. Director General MI5 also told the Committee that the Intelligence Community's willingness to "*roll our sleeves up and muck in*" when it comes to joint initiatives and co-operation gains respect and recognition from allied countries' intelligence services.[87]

M. The Committee fully supports the positive approach the Intelligence Community take towards intelligence partnerships, seeking actively to develop them beyond the merely transactional. Making full use of the UK's relative strength in intelligence terms to build effective partnerships is an effective use of resources that can help keep the UK safe in times of crisis. Ministers and senior officials should resist the temptation to take a less proactive approach in this area in the interest of economy; where the Intelligence Community can work with partner nations they should – subject to the necessary legal, ethical and security considerations.

[87] Oral evidence – MI5, 17 June 2021.

LAW AND VALUES

97. The UK Intelligence Community – and SIS in particular – often have to work with countries, and foreign liaison partners, that do not share the UK's values or commitment to human rights and the rule of law. This can be the case with the UK's closest allies – including the United States (US). In the early 2000s, for example, the UK–US relationship was strained by US actions involving cruel, inhuman and degrading treatment (CIDT), torture and rendition of terrorism suspects.

98. The challenge of doing business with foreign partners was summed up in 2009 by the then Foreign Secretary and Home Secretary in an article in the *Daily Telegraph*:

> *When detainees are held by our police or Armed Forces we can be sure how they are treated. By definition, we cannot have that same level of assurance when they are held by foreign Governments, whose obligations may differ from our own.*
>
> *Yet intelligence from overseas is critical to our success in stopping terrorism. All the most serious plots and attacks in the UK in this decade have had significant links abroad. Our agencies must work with their equivalents overseas. So we have to work hard to ensure that we do not collude in torture or mistreatment.*
>
> *Whether passing information which might lead to suspects being detained; passing questions to be put to detainees; or directly interviewing them, our agencies are required to seek to minimise, and where possible avoid, the risk of mistreatment. Enormous effort goes into assessing the risks in each case. Operations have been halted where the risk of mistreatment was too high. But it is not possible to eradicate all risk. Judgements need to be made.*[88]

99. While it is clearly in the UK's national interest that the Agencies and DI work with foreign partners where they can provide intelligence that protects our national security, doing so can, if not managed correctly, risk compromising the UK's legal and ethical standards and damaging the reputation of the Agencies and DI. The Committee has previously published two Reports scrutinising what happens in such circumstances when the UK's values have been compromised.[89] (These Reports covered the important issue of detainee mistreatment: although this Report touches on this topic, it is not the main focus of this Report.)

100. The Agencies and DI now have robust legal, policy and internal guidance frameworks in place to minimise the risk of any of their work with overseas partners compromising UK law and values. This section explores the different aspects of these frameworks: we have drawn largely on the SIS evidence session, as it is at the forefront of most of these issues, given the overseas focus of its operations.

---

[88] David Miliband and Alan Johnson, 'We firmly oppose torture – but it is impossible to eradicate all risk', *Daily Telegraph*, 8 August 2009.

[89] *Detainee Mistreatment and Rendition: 2001–2010*, HC 1113, June 2018; *Detainee Mistreatment and Rendition: Current Issues*, HC 1114, June 2018.

Legal framework

101. The UK's international and domestic law obligations are a critical component of the Agencies' work with international partners. The UK is bound by international law and is a State Party to the following international treaties:

- **The International Covenant on Civil and Political Rights (ICCPR)**, which states that "*no person shall be subjected to torture or to cruel, inhuman treatment or punishment*".[90] It also prohibits arbitrary detention and provides safeguards for detained persons.
- **The European Convention on Human Rights (ECHR)**, which states that "*no one shall be subjected to torture or to inhuman or degrading treatment or punishment*".[91] Like the ICCPR, the ECHR also provides safeguards for liberty and security of the person.
- **The United Nations (UN) Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment**.[92]
- **The 1949 Geneva Conventions**, which require humane treatment of detainees and specifically prohibit torture, and cruel and degrading treatment in the context of international armed conflict.[93] **Article 3 Common to the four Geneva Conventions** covers situations of non-international armed conflict such as civil wars and requires humane treatment for all persons in detention (including those held by non-state actors). 'Common Article 3' specifically prohibits torture, cruel, humiliating and degrading treatment and unfair trial. Given that most armed conflicts today are non-international, 'Common Article 3' is of the utmost importance.
- **The Statute of the International Criminal Court**, which includes as 'war crimes' torture, and inhuman and degrading treatment prohibited under the 1949 Geneva Conventions in the context of an armed conflict.[94]

102. The UK is also bound by customary international law, and, in the context of international partnerships, Article 16 of the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts is particularly relevant. The UK considers Article 16 to reflect customary international law, and responsibility is engaged where a State materially aids or assists another State in the commission of an internationally wrongful act, if it does so with intent and knowledge of the circumstances of that wrongful act and the act would be internationally wrongful if committed by that State.

---

[90] International Covenant on Civil and Political Rights (New York, 19 December 1966; Treaty Series No.6 (1977); Cmnd 6702).

[91] Convention for the Protection of Human Rights and Fundamental Freedoms (the European Convention on Human Rights) (Rome, 4 November 1950; Treaty Series No.71 (1953); Cmd 8969). The ECHR is implemented domestically by the Human Rights Act 1998.

[92] Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (United Nations Convention Against Torture) (New York, 4 February 1985; Treaty Series No.107(1991); Cm 1775.

[93] Conventions for the protection of War Victims (Geneva, 12 August 1949; Treaty Series No.39 (1958); Cmnd 550. The UK is also party to Additional Protocols I, II 1977 and III 2005.

[94] Rome Statute of the International Criminal Court (Rome, 17 July 1998; Treaty Series No.35 (2002); Cm 5590). The International Criminal Court Act 2001 gives effect to the ICC Statute in domestic law.

103. Domestically, the UK has four key pieces of legislation that govern the Agencies' work, including with international partners:

(i) **The Intelligence Services Act (ISA) 1994** placed SIS and GCHQ on a statutory footing and defines SIS and GCHQ's functions and purposes.[95] Section 7 of the ISA allows SIS and GCHQ to apply to a Secretary of State – usually the Foreign Secretary – for authorisation to undertake acts outside the British Islands in circumstances where they would otherwise be liable under UK domestic law.

The exercise of this wide-ranging power is subject to safeguards set out in the ISA. A Secretary of State can provide an authorisation under Section 7 ISA only if they are satisfied that any acts which may be done in reliance on the authorisation or, as the case may be, the operation in the course of which acts may be done, will be necessary for the proper discharge of a function of SIS or GCHQ. Further, there must be satisfactory arrangements in place to ensure that the nature and likely consequences of any acts done in reliance on the authorisation will be reasonable and that information obtained under the authorisation will be properly protected.

Section 5 of the ISA also provides a power for a Secretary of State to issue property warrants to enable SIS, GCHQ or MI5 to enter or interfere with property or wireless telegraphy, where such activity would otherwise be unlawful.

(ii) **The Security Service Act 1989** set out the functions of MI5, which are: the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means; to safeguard the economic well-being of the UK against threats posed by the actions or intentions of persons outside the British Islands; and to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime.

(iii) **The Investigatory Powers Act (IPA) 2016** brought together all of the powers available to the Agencies and DI to obtain communications and data about communications. The IPA overhauled the way these powers are authorised and overseen. In particular, the Act brought in a 'double lock', meaning that certain warrants, including interception warrants, must be authorised by the Secretary of State *and* a Judicial Commissioner (a serving or retired member of the senior judiciary).

---

[95] Section 1(2) of the Intelligence Services Act 1994 provides that SIS can act:
a) in the interests of national security, with particular reference to the defence and foreign policies of HMG in the UK; or
b) in the interests of the economic well-being of the United Kingdom; or
c) in support of the prevention or detection of organised crime.
GCHQ has a similar provision, although the economic aspect is restricted to "*the actions or intentions of persons outside the British Islands*".

The IPA also created a new Investigatory Powers Commissioner (IPC) to oversee and report on how these investigatory powers are used. Through a formal direction from the Prime Minister, the IPC also oversees and reports on the application of 'The Principles' (these are explored in detail below).

(iv) **The Regulation of Investigatory Powers Act (RIPA) 2000**, which still regulates the use of certain investigatory techniques not covered under the IPA 2016.

Requirements when sharing intelligence with foreign partners

104. As outlined in the previous chapter, one of the building blocks of the Agencies' international partnerships is the sharing of information. However, before sharing intelligence with foreign partners, the Agencies need to think about the type of information they intend to share and what action (if any) their foreign partner will take. Sometimes the Agencies and DI will simply provide intelligence to their foreign partners 'for information'. In many cases, the Agencies and DI will provide intelligence to a foreign partner with a specific request that action be taken, e.g. "*tell us everything you know about person X*" or "*please detain person Y*". There is also a risk that, even if the Agencies share intelligence for one purpose, the foreign partner will actually use that intelligence for an entirely different purpose. As such, there are different considerations in play depending on the scenario.

(i) Sharing requirements of the IPA 2016

105. When the Agencies share data with foreign partners that has been obtained under a warrant issued under the IPA 2016, they must ensure that the receiving (foreign) partner has applied 'safeguards' to such an extent the Agencies consider appropriate. These safeguards must "*correspond*" to those required by the Agencies under the IPA ('corresponding safeguards') for the retention and disclosure of such material.

106. The Agencies therefore require foreign partners to ensure that the material they receive is stored in a secure manner; they minimise the numbers of copies taken of the material and the numbers of people to whom the material is disclosed; and they ensure the destruction of the material once there are no longer relevant grounds for retaining it.

107. Foreign partners are also required to provide safeguards in relation to: (i) the examination of material such that the communications and other information of persons known to be in the British Islands are given adequate protection; and (ii) the handling of confidential material. Further, restrictions must be in force to prevent material obtained from interception from being used in legal proceedings.

108. GCHQ told the Committee that it establishes that a prospective partner will implement IPA 'corresponding safeguards' through a negotiation that concludes with the provision of an IPA 'safeguards assurance'.[96] This is formalised through an exchange of letters with the partner in question. Relevant GCHQ warranty makes clear that data collected may only be shared with foreign partners where such corresponding safeguards have been confirmed.

[96] Written evidence – GCHQ, 20 November 2020.

109. This sharing is subject to statutory oversight by the IPC, whose Office will inspect records of the Agencies' decisions to share IPA data with foreign partners. GCHQ explained that these records include: the type of data being shared; why it is deemed to be necessary and proportionate; the existence of an IPA 'corresponding safeguards' assurance; and confirmation that the warrant authorising the acquisition of the data permits international sharing.

(ii) Intelligence sharing and executive action

110. On occasion, the UK Intelligence Community will ask a foreign counterpart to take executive action on their behalf. Examples of this might include detaining a suspected terrorist, or interviewing an individual suspected of espionage. Legal, moral and ethical considerations are paramount in these circumstances.

111. In line with the relevant legal framework set out above, the Agencies must ensure that they comply with the UK's international and domestic law obligations when asking a foreign counterpart to take executive action (in other words, they cannot ask a foreign counterpart to do something that they could not legally do themselves). The action must also comply with the liaison partners' international and domestic law obligations. For example, where the Agencies solicit a detention overseas, then the Agencies must satisfy themselves that that detention is lawful under the local law of that country and international law.

Policy framework

112. Supporting the legal framework, the UK Intelligence Community have two key policy documents that govern some of the most sensitive aspects of how UK intelligence organisations engage overseas: the Overseas Security and Justice Assistance (OSJA) guidance and 'The Principles'.

Overseas Security and Justice Assistance

113. OSJA guidance, first published in 2011, sets out the conduct expected of all UK public bodies when carrying out overseas security and justice assistance work; for example, capacity building to help address terrorist threats in other countries. The guidance is principally concerned with British values including human rights and "*the enlightened national interest*".

114. The OSJA framework is a four-stage risk assessment activity to be conducted for all new proposed international assistance activities, when significantly altering assistance programmes, or if the risks of pre-existing programmes materially change. The four stages set out in the OSJA guidance are:

1) *Assessment of the internal situation in the host country, noting its stability, attitude toward human rights, and any mitigation efforts already underway.*
2) *Identification of human rights, political, or reputational risks associated with a given proposal.*
3) *Consideration of possible mitigations of identified risks including whether stopping the activity might be more appropriate and how this can be done.*

4) *Provision of an overall assessment of whether activity is likely to strengthen international compliance with human rights and international law or whether there is a serious risk that activity might directly or meaningfully contribute to a violation of said rights.*

115. As an example of how this is applied, MI5 told the Committee that:

> *OSJA requires MI5 to consult Ministers where there is a serious risk our engagement might directly or significantly contribute to a violation of human rights, or where there is a serious reputational or political risk for the Government or MI5. MI5 considers the OSJA guidance when conducting capacity building with overseas liaison partners, and considers OSJA alongside the Principles when engaging on detainees*.[97]

116. The Agencies and DI take their obligations under this guidance seriously. Nevertheless, the principal areas of difficulty, and indeed those that garner the most media attention, are those circumstances where the Agencies and DI take action with regards to the detention and interviewing of detainees, which is covered by The Principles.

The Principles

117. *The Principles relating to the detention and interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees* (hereafter referred to simply as 'The Principles') is the most recent document outlining the specific policy around UK involvement in detention and interviewing of detainees in partnership with overseas intelligence liaison partners.

118. From 2010 to 2020, these issues were governed by the *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees* (hereafter 'the Consolidated Guidance'). However, this Committee's 2018 Reports on Detainee Mistreatment and Rendition raised serious concerns as to the overall scope and efficacy of the Consolidated Guidance.[98]

119. The Committee set out a series of recommendations for changes to the Consolidated Guidance. These included providing greater clarity on ministerial discretion and an explicit prohibition on ministerial authorisation of CIDT under any circumstances (including through section 7 authorisations under the ISA), further details as to the interpretation of 'serious risk', and expansion of the guidance to cover joint units financed or tasked by the UK.

120. In response to the concerns raised by the Committee's Reports, the Prime Minister asked the then IPC, Sir Adrian Fulford, to review the Consolidated Guidance. He proposed 'The Principles', which the Government subsequently adopted in January 2020. The main substantive changes were set out in a letter to the Prime Minister and are summarised below:[99]

---

[97] Oral evidence – MI5, 17 June 2021.

[98] *Detainee Mistreatment and Rendition: 2001–2010*, HC 1113, June 2018; *Detainee Mistreatment and Rendition: Current Issues*, HC 1114, June 2018.

[99] IPCO letter to the Prime Minister, 12 June 2019.

Issue	Consolidated Guidance	The Principles
Type of harm covered	*Covers*: torture, CIDT, arbitrary arrest and detention.	*Adds*: unlawful killing, rendition and extraordinary rendition.[100]
Threshold of risk	Officials consider whether passing intelligence or seeking detention gives rise to a 'serious risk' of harms occurring.	Wording changed to 'real risk' to bring in line with international law and is more generally applied in equivalent contexts.
Non-state actors	No reference	Principles apply in this case "*insofar as possible*" (reflecting the difficulties of these to be fully applied in this case).
Joint working	No reference	Principles apply in cases of foreign bodies wholly or partly funded or trained by the UK and acting under UK direction.

The Principles incorporated all of the ISC's recommendations, apart from one advising that Ministers should be explicitly prohibited from authorising UK action where there is a real risk of unlawful killing, torture, CIDT or extraordinary rendition.

121. The Principles apply to the passing and receipt of intelligence when personnel from SIS, MI5, GCHQ, the Ministry of Defence (MoD) (and the Armed Forces), the National Crime Agency (NCA) and SO15[101] are:

(i) interviewing a person in the detention of a foreign authority, or soliciting intelligence from a detainee via a foreign authority;

(ii) passing intelligence to a foreign authority concerning an individual detained by that authority;

(iii) passing intelligence to a foreign authority when detention is sought or when personnel know or believe detention will occur as a result of intelligence being passed;

(iv) passing intelligence to a foreign authority concerning an individual when detention is sought and there is a real risk that the foreign authority will unlawfully kill the individual in an extra-judicial killing rather than the individual being taken into custody; or

[100] IPCO made clear that, despite the original drafting, whenever there was risk of these additions occurring, Intelligence Agencies applied the Consolidated Guidance fully. These additions are therefore 'for completeness'.
[101] SO15: Counter Terrorism Policing within the Metropolitan Police Service.

(v) receiving unsolicited intelligence that has been obtained from a detainee in the custody of a foreign authority.

And when either:

(i) personnel know or believe unlawful killing, torture or extraordinary rendition will result from the passing or receipt of intelligence or in interviewing detainees; or

(ii) there is a real risk of one of these things happening or that unacceptable standards of arrest and detention will result from the passing or receipt of intelligence or in interviewing detainees.

122. The key provisions of The Principles are summarised below:

- The Principles make clear that "*the UK Government does not participate in, solicit, encourage or condone unlawful killing, the use of torture or cruel, inhuman or degrading treatment (CIDT), or extraordinary rendition. In no circumstances will UK personnel ever take action amounting to torture, unlawful killing, extraordinary rendition, or CIDT.*"[102]
- Decisions are made on the following basis:

  (i) [when] *personnel know or believe unlawful killing, torture or extraordinary rendition will take place personnel must not proceed, and Ministers must be informed. Personnel should raise their concerns with the relevant foreign authority and try to prevent* [the unacceptable treatment] *from taking place, except where doing so might itself lead to unacceptable treatment of the detainee or the safety or security of the UK personnel raising the concern may be put at risk.*

  (ii) Where a 'real risk' exists of unlawful killing, torture, CIDT, extraordinary rendition or rendition or unacceptable standards of arrest and detention, personnel should not proceed unless either: (i) There has been consultation with senior personnel and legal advisers who have concluded there is no real risk or (ii) it has been possible to effectively mitigate the risk to below the threshold of real risk through reliable caveats or assurances which have been reviewed and approved by senior personnel.

  (iii) If neither (i) or (ii) are possible, Ministers must be consulted. They should be provided with full details, including the likelihood of the relevant conduct occurring, the risks of inaction and the circumstances and causality of UK involvement. Ministers will consider whether it is possible to mitigate the risk of the relevant conduct through requesting and evaluating assurances on the detainee's treatment; assessing whether the caveats placed on information/ questions would be respected by the detaining party; and whether the UK involvement in the case, in whatever form, would increase or decrease the likelihood of the relevant conduct occurring.

[102] The Principles, HMG, July 2019.

- *Consulting Ministers does not imply that action will or will not be authorised.*[103]

'Mitigation' of risk

The Principles and the Overseas Security and Justice Assistance (OSJA) guidance use the terms "*mitigation of risk*" and "*mitigate the risk*".

The Intelligence Community use 'mitigation' and 'mitigate' as terms of art, taking their standard dictionary meaning (the Oxford English Dictionary defines mitigate as "*to make something bad less severe or serious*") to describe the 'reduction' or 'reducing' of risk rather than the elimination of risk. When working with foreign liaison partners, the calculation of risk – both before and after mitigation – is a vital part of the compliance assessment and ministerial authorisation process.

The 'mitigation' of risk is used in other areas of government including in immigration proceedings, where assurances are often sought in order to 'mitigate the risk' of mistreatment of an individual on return to their country of origin or nationality. For example, in Abu Qatada's deportation proceedings from the UK, the Special Immigration Appeals Commission heard evidence in closed session about the extent to which a Memorandum of Understanding in place between the UK and Jordan "*would mitigate the risk of torture*".[104]

Recognising, however, that there may be some confusion as to the term – which might also be interpreted to mean removal – we wish to make clear that, where this Report uses the term 'mitigate' or 'mitigation', we do so solely in order to mirror the language used in The Principles and OSJA guidance, and by the Intelligence Community, and take the standard dictionary meaning of 'to make something bad less severe or serious' rather than suggesting it is removed altogether.

Assessment

123. The first step for the Agencies in understanding the risks involved when working with a particular partner is to assess the general state of human rights and compliance standards of that partner. PURPLE[105] was established in early 2018 to conduct these liaison assessments and maintains a database of HMG assessments, mistreatment reporting, assurances, submissions and 'positive evidence' of compliance behaviour; it also acts as a cross-Agency first point of contact.

124. PURPLE assessments support the Agencies in complying with UK legal and ethical requirements by acting as the single source of information for the compliance level of any given country. As of November 2020, they had produced *** assessments.[106]

125. The assessments consider both open source material and secret intelligence (often based on prior interaction with the service in question) to build a comprehensive picture of

[103] The Principles, HMG, July 2019.
[104] *Othman (Abu Qatada) v The UK 8139/09* [2012] ECHR 56 (17 January 2012).
[105] 'PURPLE' is a code word we have substituted for the actual name of this team which is ***.
[106] Written evidence – SIS, 23 November 2020.

the overall state of human rights compliance within a country or liaison partner.[107] The Committee has been provided with an example of an open source assessment and acknowledges the comprehensive assessment found here. The Committee has also been provided with templates for the secret intelligence assessment, which appears to provide a suitable opportunity to identify issues of concern for future activity – though, without having seen a completed example, it is difficult to judge the true efficacy.

126. Within SIS, as a matter of policy, such assessments are included as part of a submission to a Minister seeking authorisation for any activity.[108] However, in any submission, the relevant operational team or overseas station should also accurately record the overall risk of torture or unacceptable treatment by a foreign liaison partner. Within GCHQ and MI5, PURPLE assessments are used to support their equivalent processes.[109]

127. PURPLE also acts as the central point of contact for reports of unacceptable conduct by liaison partners. Reports are investigated by operational teams or SIS stations, who then take any necessary action and report back to PURPLE. ***.[110]

Decision making

128. SIS provided a basic process flow which their officers follow in situations where The Principles may be engaged – for example, when interviewing a person in the detention of a foreign authority, or when passing intelligence to a foreign authority when detention is sought. Officers are required to:

(i) read The Principles;

(ii) read internal guidance provided by legal and policy colleagues;

(iii) complete mandatory online training;

(iv) familiarise themselves with the latest PURPLE assessment and any relevant previous decisions taken concerning the liaison in question;

(v) familiarise themselves with any relevant submissions or authorisations that covered similar action within the mission in question; and

(vi) familiarise themselves with any other relevant information, including views and experience from Foreign, Commonwealth and Development Office (FCDO) colleagues (including FCDO's OSJA assessment) as well as any relevant engagement with the liaison from close allies (e.g. the Central Intelligence Agency).

129. In doing so, SIS officers are also required to ensure that the proposed activity is necessary, proportionate and reasonable. In addition, officers must consider the broader risks that the activity may have on the UK's ability to operate. SIS notes that these risks

[107] 'Open source' refers to material obtained from freely available sources, such as NGOs, journalists, charities, academia, etc. In this case it may include reports from the United Nations (UN), Human Rights Watch, the US State Department etc.
[108] A 'submission' is the term used for a briefing sent to a Minister that seeks a decision on a particular policy or operational issue.
[109] Written evidence – SIS, 23 November 2020.
[110] Oral evidence – SIS, 27 May 2021.

centre on: risk to political relationships and reputation; risk to physical and psychological well-being; risk to the legal and compliance framework; and risk to enabling capabilities.[111]

130. MI5 also shared with the Committee its internal 'Liaison with Overseas Security and Intelligence Agencies' (LOSIA) forms and the associated guidance. Similar to documents in SIS, they provide a written record that the appropriate considerations of necessity, proportionality and risk have been made, and are completed when MI5 shares intelligence directly with international partners on a matter related to detainees, or where there is a real risk of unacceptable conduct or reputational/political damage. They are also completed when intelligence is received from any source suggesting that unacceptable conduct has occurred.[112] The Committee was particularly impressed with this guidance.

Managing risk

131. When the Agencies ask a partner to take action on their behalf and that action would fall under The Principles, reducing the risk(s) involved is central to the process. SIS noted the options that may be considered in order to reduce the risk associated with a country or partner organisation:

- **Not proceeding** – Where The Principles are engaged and a real risk is present, not proceeding will be considered if, for example, the benefits are not certain or can be otherwise achieved.
- **Assurances** – Credibly given by a competent authority within the liaison partner that has the power to bind action taken when working with the UK on detainee issues. (PURPLE keeps a record of assurances received from liaison partners, and works with the relevant SIS station to ensure that the assurances cover all relevant facets of The Principles.)
- **Oversight** – Drawing on pre-existing HMG or third party (e.g. US, UN) oversight of the countries' activities in this regard; if it is not in place, considering whether HMG oversight could be requested.
- **Capacity building** – Training and mentoring to improve the liaison partner's capabilities and compliance with domestic and international law.
- **Caveats** – SIS sharing intelligence with provisos relating to what use the information can be put to and to whom it can be passed.[113]

Assurances

Assurances are a key tool that intelligence Agencies use to satisfy themselves that appropriate steps are being taken to maintain human rights standards when foreign partners are working with the UK, or to protect UK information.

[111] Written evidence – SIS, 23 November 2020.
[112] LOSIA forms are not required when another organisation to which The Principles apply – e.g. SIS – is liaising with a foreign partner on MI5's behalf. This is because the other organisation would be responsible for making the relevant considerations under The Principles; Written evidence – MI5, 15 January 2021.
[113] Written evidence – SIS, 23 November 2020.

Generally, these are obtained from individuals within a foreign liaison service, judged to be credible and with the authority to ensure that unacceptable behaviour is not carried out. We recognise that the assurances process is necessary but imperfect. It cannot provide a definitive guarantee that assurances will be adhered to, but rather reflects the messy reality of intelligence work.

The Committee has questioned the Agencies (and SIS in particular) as to how assurances are used and why they should be deemed a credible tool to reduce the risk of unacceptable treatment. SIS told the Committee:

> *On the assurances received, look, they have to be believable. You know, there's an obvious trap here, isn't there, that people would be prepared to offer assurances which they have no intention of living up to.*
>
> *So the officer who's ... putting this case together has to say very clearly that they regard the assurances they're getting as being believable and they also have to assess and then record the judgement that the person giving them that assurance actually has the clout to deliver on it.*[114]

It is preferable for assurances to be provided by senior figures in writing, but this is not always done (often for practical reasons), so in such situations the judgement of the officer taking and accepting the assurance is paramount. Where assurances are not provided in writing, then a comprehensive written record should be prepared of what has been agreed and by whom. The record should record why the assurances are assessed to be credible and whether they appropriately address the situation (and are capable of being fulfilled). This can be exacerbated by the difficulty in getting an assurance in the first place – often simply asking the question can be seen as demeaning to the dignity of the liaison partner. SIS has confirmed that, where this is a real issue, and assurances cannot be received, then they would not proceed.[115]

The Intelligence Community appear to recognise the risk involved in relying on what might seem to be a rather flimsy tool, but stress that the costs of breaking such assurances are significant. They note that, if a breach was discovered:

> *we would stop immediately, we would look to find out what was going on and it would impact on any assurances that had been given by that partner, they would have to be revisited and relooked at again...*
>
> *We do routinely with some of our hardest partnerships, often alongside SIS, pause intelligence sharing or collaboration whilst we thoroughly investigate and understand the circumstances of whatever is happening and that's usually about the behaviours that we're seeing* ***.[116]

[114] Oral evidence – SIS, 27 May 2021.
[115] Oral evidence – SIS, 27 May 2021.
[116] Oral evidence – GCHQ, 1 July 2021.

Ultimately, the risk is then that the UK disengages from their relationship; while this may seem a weak weapon, SIS claims that it is a more potent threat than may be initially thought. Speaking about ***, SIS said:

> *They are sophisticated enough, I think, to recognise that if they don't* [adhere to UK legal and ethical red lines]*, that that would put us in an impossible position and the relationship will be damaged.*[117]

132. In such circumstances, SIS and GCHQ submit to the Foreign Secretary for them to take a decision based on the risk factors identified and any 'mitigations' in place to reduce the risk of unacceptable treatment – the 'net risk'. These submissions will also include details of any previous activity and the relevant PURPLE assessments. The Foreign Secretary has significant autonomy in deciding whether or not to authorise the activity or warrant.

133. For cases involving The Principles, the key thresholds are 'Knowledge and Belief' and 'Real Risk', but there is no general barrier to working with services that otherwise engage in unacceptable treatment of detainees so long as the UK puts in place suitable measures to ensure that the Agencies' and DI's engagement with the liaison partner in question fully complies with The Principles.

134. If the 'net risk' for some action is judged lower than a 'real risk', then activity may take place (though the Foreign Secretary may still be consulted to clear for other risks, e.g. political risk). However, for cases where it is not clear-cut, The Principles offer significant discretion to the Foreign Secretary to decide whether to proceed. They state:

> *14. If...* [it cannot be concluded that activity falls below 'real risk', even with mitigations in place] *Ministers must be consulted. They should be provided with full details, including the likelihood of the relevant conduct occurring, the risks of inaction and the circumstances and causality of UK involvement.*
>
> *15. Ministers will consider whether it is possible to mitigate the risk of the relevant conduct through requesting and evaluating assurances of the detainee's treatment; assessing whether the caveats placed on information/questions would be respected by the detaining party; and whether the UK involvement in the case, in whatever form, would increase or decrease the likelihood of the relevant conduct occurring.*
>
> *16. Consulting Ministers does not imply that action will or will not be authorised. Instead, it enables Ministers to look at the full complexities of the case and its legality, taking account of the longstanding stance of the UK* [to oppose unlawful killing, the use of torture, CIDT, extraordinary rendition, unacceptable standards of arrest and detention, and any placing of a detained person outside the protection of the law].[118]

135. Because of this, the Foreign Secretary plays a very significant role in shaping the UK's risk appetite and approach to dealing with risks of torture or mistreatment abroad. FCDO informed the Committee that, between April 2020 and March 2021, there were fewer than

[117] Oral evidence – SIS, 27 May 2021.
[118] The Principles, HMG, July 2019.

100 submissions to the Foreign Secretary that engaged The Principles. Typically, fewer than 5% of submissions are rejected.[119]

136. The then Foreign Secretary told the Committee the process he personally went through when making decisions on the submissions he received:

> *I'm thinking are we spending resources in the right place. So the first thing is "is this really necessary? Why are we doing it?".*
>
> *Secondly what I'd look at is what's the value added.*
>
> *Thirdly, what's the risk?*
>
> *... If there's anything that could involve risk of torture or cruel or inhumane degrading treatment, that gets looked at disproportionately carefully ...*
>
> *... I think the other issue is when you're dealing with proximity to, I don't know, a terrorist group or a hostile state, quite what level of collaboration you would engage in in order to elicit information without somehow then being complicit in what those organisations are doing, you can imagine that balance is very important.*[120]

137. The Foreign Secretary can apply conditions or caveats when approving requests for permission – this offers an alternative to rejecting a request out of hand and may explain the relatively low rejection rate. The then Foreign Secretary told the Committee:

> *what will happen is I'll say can you look at it a different way, can we do three quarters of what you want to do, can you go and seek assurances and the conversation will be like that.*[121]

Some authorisations will be subject to renewal, perhaps every six months, which provides an opportunity for the Foreign Secretary to review the situation and consider whether or not the authorisation is still appropriate.

138. The Committee asked the then Foreign Secretary about his risk appetite in relation to approving submissions involving a risk of torture or CIDT:

> *On the sort of curry menu, I'm a spicy madras. So I want to be really careful, I want them to do their job, I want to be forward leaning, I want to be really gripping the opportunities, but I don't want to take them into vindaloo or even phaal territory which means that I risk repercussions the day after ... unless we're doing things on a sustainable basis, we trip up.*[122]

He was then asked specifically whether he had authorised conduct which had a 'real risk' of torture or CIDT ('real risk' being the threshold used in The Principles):

---

[119] Written evidence – FCDO, 11 October 2021.
[120] Oral evidence – Foreign Secretary, 1 July 2021.
[121] Oral evidence – Foreign Secretary, 1 July 2021.
[122] Oral evidence – Foreign Secretary, 1 July 2021.

DAME DIANA JOHNSON: *... have you authorised action where there is a real risk of torture or* [CIDT]*?*

FOREIGN SECRETARY: *No,* [I] *don't do it.*

DAME DIANA JOHNSON: *You've never done it in two years?*

FOREIGN SECRETARY: *Not without assurances that take the risk down ... I think there are some moral red lines. I don't trust torture from an efficacy point of view as well as finding it abhorrent from a moral point of view. I also worry about the reputational integrity of our Agencies.*[123]

139. From this exchange, the Committee understood that the then Foreign Secretary had never authorised conduct that had a real risk of torture or CIDT without assurances having been received which would "*take down the risk*" – i.e. reduce it to below the threshold of 'real risk'. However, when the Committee subsequently asked for further written evidence, it transpired that this was not the case.

140. Following the session, the Committee asked FCDO for further details on those submissions that the then Foreign Secretary had considered, that engaged The Principles. This information, which was only received after the Committee had drafted this Report, revealed that the then Foreign Secretary had in fact authorised action on one occasion that carried a real risk of torture – even though assurances were sought, they did not reduce the risk down to less than a real risk of torture.[124]

141. He had also authorised action that carried a real risk of CIDT (on three occasions within a 12-month period) and had authorised action that carried a real risk of other unacceptable treatment (for example, unacceptable standards of arrest and detention) on 22 occasions within that same 12-month period.[125]

142. This is a matter of very serious concern. While the then Foreign Secretary was entitled to authorise the activity in question, and we have no reason to believe that he sought actively to mislead the Committee, FCDO and SIS officials – who accompanied him at the evidence session – did not clarify his evidence when given an opportunity to review the transcript

[123] Oral evidence – Foreign Secretary, 1 July 2021.

[124] This case – which involved the passing of threat-to-life intelligence – carried a 'real risk' of torture that could not be reduced to 'less than real'.

[125] The Principles cover the risk of a detainee being subject to: unlawful killing; torture; CIDT; extraordinary rendition or rendition; and unacceptable standards of arrest and detention. In response to the further questions from the Committee, FCDO revealed that, over a 12-month period from April 2020 to March 2021, the then Foreign Secretary considered *** submissions from SIS that engaged The Principles. Of these, *** identified a 'real risk' that, through assurances or mitigations, had been reduced to 'less than real'. *** submissions had identified a 'real risk' that remained a 'real risk', "*even when assurances and other mitigations had been applied or where it was not possible to apply mitigations because the risks were systemic*". Of these *** contained a real risk of CIDT and the remaining *** contained a real risk of other unacceptable treatment. This means that, over a 12-month period, around half of the small number of submissions approved by the then Foreign Secretary in relation to The Principles involved a real risk of a detainee being subjected to some form of treatment that the UK holds to be unacceptable, and that risk could not be reduced to below real risk, but the action was nevertheless authorised.

following the evidence session.[126] The authorising of action that carried a real risk of torture is surely so exceptional that it cannot have been merely overlooked or forgotten – yet the full picture was provided only after the Committee pressed for further information. Even at that stage, FCDO sought to argue that there was no inconsistency in the evidence provided, when this is clearly not the case.[127]

143. Furthermore, the new evidence provided is directly at odds with evidence given in 2016 – and assurances previously given to the Committee. During the course of our predecessor Committee's Inquiry into Detainee Mistreatment and Rendition, the ISC was assured, in categorical terms, that SIS would never ask for authorisation in cases where there was a serious risk of torture ('serious risk' being the threshold under the Consolidated Guidance – since replaced by The Principles).

144. The Committee was also told in 2016 (in the course of its Detainee Inquiry) by the Rt Hon. Boris Johnson MP – who at that point was Foreign Secretary – that he considered that there was an absolute prohibition on Ministers authorising action where there was a risk of torture in the handling of detainees, and that there could be "*no quibbling*" over the matter. (The Cabinet Office subsequently clarified that Boris Johnson's was "*an ethical position, it is permissible for him to be more restrictive than the Consolidated Guidance*",[128] and indeed his predecessor, the Rt Hon. Philip Hammond MP, and the Rt Hon. Theresa May MP and the Rt Hon. Amber Rudd MP, as Home Secretaries, gave different interpretations to the Committee.) This led to the Committee's conclusion that the then Guidance was insufficiently clear.[129]

145. The new evidence now supplied by FCDO clearly demonstrates the fact that there is no prohibition on Ministers authorising action that poses a real risk of torture, as Ministers have indeed authorised such activity (consistent with The Principles). We note that, had that been the case at the time of the 2016 Report, our predecessor Committee may well have reached different conclusions.

146. In order for the Committee to carry out its statutory oversight function, it is vital that the Intelligence Community, and the Government more widely, are transparent in their

[126] As a matter of course, the Committee provides a copy of the evidence transcript to witnesses following an evidence session so that any errors or discrepancies in the evidence can be identified. Should any such errors be identified, the witness – or officials working on their behalf – can submit a request for a correction to be made to the transcript (with the full original evidence transcript also being retained). This process is intended to ensure that inadvertent factual errors in oral evidence are rectified, and that the Committee does not then base its conclusions on incorrect information.

[127] FCDO held that the evidence was accurate because assurances had been sought – it was just that the risk had not been reduced sufficiently as a result.

[128] The Cabinet Office said: "*It's an ethical position, it is permissible for him* [the Rt Hon. Boris Johnson MP] *to be more restrictive than the Consolidated Guidance, and he did, I think, specifically say that that position was based on his own principles. So I think you cannot remove an element of personal judgement from Ministers' eventual decision in these cases, and it's not unreasonable for different Ministers to take a different position.*"

[129] As a result of the Committee's concerns, the Prime Minister asked the then IPC, Sir Adrian Fulford, to review the Consolidated Guidance. The IPC proposed 'The Principles' as a replacement to the Consolidated Guidance, and the Government subsequently adopted these in January 2020 (this change is explained in more detail in paragraphs 117–120 of this Report).

provision of evidence to the Committee. We expect steps to be taken to prevent any such inaccuracies in evidence to the Committee – inadvertent or otherwise – in future.

147. Returning to the question of what Ministers can and cannot authorise, when SIS was asked about the possibility of Ministers using their very wide discretion inappropriately, it told the Committee:

> *the Ministerial Code and the Civil Service Code is very clear: Ministers must comply with the law and we as SIS officers and civil servants must comply with the law. So I can't envisage a scenario where that happens and in fact, particularly working with our Foreign Secretary currently, I've never experienced a scenario where that has happened.*[130]

On the specific issue of inappropriate orders, SIS was quite clear:

> *if the hypothetical question is if the minister directed us to do something illegal, would we do it? No.*[131]

148. MI5 also explained its decision-making process and thresholds for the consideration of risk in relation to The Principles:

> *So by volume, in the overwhelming majority of cases, the decision is taken within MI5 or very often within SIS ... But when a proposal emerges to do something or make a request, in the first instance it falls to us as the operational agency to reach a professional judgement about whether the proposed course of action might contain real risk of unacceptable conduct taking place, say, and, if our judgement is that that risk is not real or that we can ourselves take steps which will mitigate that risk, then, yes, the decision rests with us. But in the rare case, but it does happen, where we think there is real risk in play, when we cannot ourselves mitigate it, then the system ... requires us to then submit to ministers who rightly and properly are the people to make the difficult decisions in those rare cases.*[132]

149. MI5 also clarified that the test within The Principles is not about 'balance' of risk – the line is clear that even in the most extreme of circumstances Agencies will neither commit CIDT, nor influence a foreign liaison partner to commit it on their behalf:

> *One specific bit of this that is quite important is ... the test here is not balance. The test is do we think there is real risk that unacceptable conduct will take place or is taking place and so, even if you had a sort of fantasy scenario with a ticking fuse on a nuclear device, you wouldn't torture or you wouldn't put up with someone else torturing, so it's not, as it were, a balance test. There are absolute lines, are they being crossed.*[133]

[130] Oral evidence – SIS, 27 May 2021.
[131] Oral evidence – SIS, 27 May 2021.
[132] Oral evidence – MI5, 17 June 2021.
[133] Oral evidence – MI5, 17 June 2021.

Accountability

150. In practice, across many of their most crucial missions, the Agencies will routinely work 'at three' – that is, SIS, MI5 and GCHQ working together to pursue a particular objective, with operational teams either collocated or simply in regular contact. On occasion, this arrangement has led to difficulties, as Director General MI5 explained to the Committee:

> *What was happening in practice was that* [MI5] *officers and SIS officers were both fairly sort of accountable for the same risks in the same way and obviously there's a narrow reason why that is bad – which is an efficiency, duplication, taxpayer reason – but the deeper reason why that is bad is that, if everyone feels a bit accountable, nobody feels fully accountable and I felt we would reach better decisions and have less friction between teams if it was clear that on any particular piece of transaction the person doing the "last pair of hands" owned the accountability.*[134]

151. The 'last pair of hands' principle is designed to ensure that there is a clear risk owner for all stages when progressing complex investigations across three Agencies. Supporting this is a network of senior governance structures, involving directors across all three Agencies, which sets overall risks, taking into account varying ministerial risk appetites, so that officers in the field who are currently 'hands on' have clear guidance for what is and is not acceptable.

152. Even within the cleanest governance structures, there is still clearly room for disagreement. Director General MI5 was realistic about this and the need to ensure the right settlement is reached:

> *But I would say… because of the system, the disagreements, as it were, between MI5 and SIS are no more or less common than disagreements within MI5, say. An investigator might want something to be pursued and an agent runner might not because of the risks to the agent. So you'll have a perfectly valid professional difference of view.*
>
> *…the reasons for the disagreements are not … institutional jockeying really, it's that these things are hard and we are making judgments of ethical and legal significance and we all want to get them right.*[135]

153. A particular risk for the UK is where UK information could form the basis for military strikes against targets that Ministers have not explicitly authorised. The legal and policy position is that the UK will make a material contribution to the use of force by a foreign partner only where: i) it is satisfied that there is a legal basis for the use of force under international law, all other relevant legal risks have been considered and the force will be used in accordance with international law; and ii) following ministerial authorisation.

154. In cases where no current ministerial authorisation is in place, GCHQ, for example, manages the risk of their information supporting such activities through a process to ensure that customers seek their authorisation to undertake executive action based upon the

[134] Oral evidence – MI5, 17 June 2021.
[135] Oral evidence – MI5, 17 June 2021.

information, and that any use made of GCHQ reporting complies with UK policy and law.[136] Responding to Committee questioning about this process, GCHQ clarified:

> *So* [whether GCHQ had made a material contribution is] *a judgement call based on our understanding of the operating environment, the impact of the intelligence and the behaviour of our customers and we have a lot of input into that. It works up through the management chain inside GCHQ, it has very strong input from policy and legal colleagues and then of course it's overseen after the fact by commissioners.*[137] *So there's a lot of governance and oversight around those judgments and to my knowledge those judgments haven't been found wanting.*
>
> *… we also have a process *** when…we know that there is potential risk of certain individuals being targeted with lethal force. So we have in that degree a proactive process to determine which individuals or entities we believe are at risk in this way and then, as we are then being asked for* [explicit permission to take action] *et cetera, that triggers a process internally and management action is then taken, so we aren't, if you like, caught out by could you provide* [a]*…response within ten minutes and us not knowing about whether there's a risk here or not.*[138]

155. ***.[139]

Ethics

156. These situations raise ethical concerns, quite apart from the legal and policy framework and processes. The Committee questioned how the Agencies seek to ensure that their ethics and values are not compromised by their work. The Chief of SIS was aware of the difficulties, saying: "*I have people working with me who think deeply about the challenges of working with some of these more difficult partners … and they often want to think that through, talk that through. It's important that their leaders help them to do that.*"[140] He described how they ensured that such concerns were aired:

> *We have a wonderful ethics counsellor in the service who is a very distinguished … former officer and also played a role in the outside world and the third sector, who makes himself available for these types of discussions. So it's kind of … wired into our DNA and we have a set of processes to make sure that we go through and we take all of these things into account.*[141]

[136] Written evidence – GCHQ, 20 November 2020; since giving evidence, GCHQ has advised that, even before this process, GCHQ considers proactively sharing intelligence on these individuals on a case-by-case basis further to ensure that they remain within legal and policy parameters.
[137] Subsequently, GCHQ corrected its evidence to make clear that retrospective oversight by IPCO occurs through the existence of legal authorisations; whilst ministerial authorisations are sought for all cases where the Agencies support the use of force by a foreign partner, it is not always the case that a legal authorisation will have been sought or is needed (this depends on the degree and nature of the legal risk arising).
[138] Oral evidence – GCHQ, 1 July 2021.
[139] Oral evidence – GCHQ, 1 July 2021.
[140] Oral evidence – SIS, 27 May 2021.
[141] Oral evidence – SIS, 27 May 2021.

On occasion, specific events and circumstances demand a more organisational approach, led from the top of the office. He told the Committee:

> *alongside my counterparts in GCHQ and MI5, I hosted a dial in session where we discussed the ethics of working with *** to recognise and answer the concerns of staff … in the light of ***, what that meant for our relationship and we had a very open discussion where we invited challenge and invited people to express sincerely their concerns about what we were doing and explained how it is that we managed those relationships.*[142]

When things go wrong

157. The legal and policy framework is clear, as are the processes to be followed by Agency staff, and we expect Ministers to understand the issues that they are required to take into account when making the ultimate decision. Nevertheless, converting policy and process into practice is not always straightforward – particularly where partners are concerned. As SIS noted:

> *This is not an exact science. You know, we're out there in a very messy world dealing with partners who sometimes, as I said right at the outset, don't share our values. So it's a question of trying to navigate that to the best possible degree we can and we have to do it in a way that is consistent with UK law and with UK obligations in international law and we have to do it in a way that is compliant with our oversight.*[143]

158. The Committee recognises that no procedures are infallible, and compliance difficulties or errors can and will occur when working with international partners. The Intelligence Community have a duty to ensure that they take steps to minimise the risk of this happening, that they report any compliance issues to the relevant authorities – namely Ministers and the IPC – and, crucially, that they learn lessons to prevent these issues reoccurring. SIS recognised the Committee's concerns in this respect:

> *But can you guarantee any more than I can guarantee that my officers won't occasionally make mistakes in compliance, can we guarantee the behaviours of our international partners? Of course not. But if we discover them doing things which have changed the basis on which we entered that relationship, then we will withdraw. In fact we will withdraw immediately … we'll suspend co-operation whilst we review an alleged compliance breach and then we'll move forward.*[144]

159. Compliance issues can be broadly brigaded into three categories:

(i) partners with different standards – some of the Agencies' most important partners have different legal and ethical standards, making it difficult to work together across the board; bespoke compliance pathways are needed when Agencies work with such partners to ensure compliant operations;

[142] Oral evidence – SIS, 27 May 2021.
[143] Oral evidence – SIS, 27 May 2021.
[144] Oral evidence – SIS, 27 May 2021.

(ii) broken assurances – when a foreign partner breaks agreed Agencies' assurances, for example on the standard of treatment of a detainee, or takes unauthorised action contrary to agreed assurances; and

(iii) human error – when Agency staff fail to follow the correct compliance procedures; for example, they fail to seek assurances or fail to follow-up on allegations of broken assurances or mistreatment.

Partners with different standards

160. Very often the areas of the world in which it is most important for the Intelligence Community to work are those in which the prevailing legal and ethical standards are not the same as those in the UK. As has been described above, the Agencies must ensure that any activity is conducted in compliance with UK legal requirements. The Chief of SIS told the Committee:

> [we are] *highly conscious that when we're operating in the overseas space, you know, we are an arm of this government operating overseas and so we are at the leading edge of not only UK adherence to the international rules based order but also promoting it to our international partners overseas and that's a key part of what we do.*
>
> *So that means whenever we're acting, we're driven, whatever the threat, to do it in compliance with our values and respecting the rule of law.*[145]

161. During its evidence session with SIS, the Committee discussed the case of *** – an example of a regime that works to very different compliance standards – where it has been necessary for SIS to establish a compliance pathway. It is also an example of needing to continue working with a partner, from which the UK extracts significant intelligence benefits, in the face of a changing compliance picture ***. This partnership is covered as a case study later in this Report.

162. It is important to note that compliance concerns are not confined to intelligence partnerships with countries that have what we might consider to be less robust legal frameworks or lower levels of democratic accountability than the UK. The previous Committee's reports on Detainee Mistreatment and Rendition, which examined the actions of the UK Intelligence Community in relation to the handling of detainees and rendition by the US authorities, demonstrated the reputational risk attached even to working with our closest ally.[146]

163. There is little question that the US treatment of detainees in the early 2000s was a particular low point; since then, however, with the introduction of the Consolidated Guidance, recently replaced by The Principles (a consequence of this Committee's scrutiny and recommendations), assurance has been substantially improved.

164. Nevertheless, the two countries continue to have different legal thresholds and interpretations, and the continued operation of Guantánamo Bay, and the US's ongoing

[145] Oral evidence – SIS, 27 May 2021.
[146] *Detainee Mistreatment and Rendition: 2001–2010*, HC 1113, June 2018; *Detainee Mistreatment and Rendition: Current Issues*, HC 1114, June 2018.

campaign against Al-Qaeda mean that the UK Intelligence Community must be careful with any detainee work with the US. Furthermore, there remains a risk that US policy could quickly shift to a more permissive stance towards activities that would be contrary to the UK's legal and policy framework. For example, in January 2018, then President Trump issued an Executive Order reversing the policy of the Obama Administration to close Guantánamo Bay prison. Trump's Executive Order provided that detention operations at Guantánamo Bay were "*legal, safe, humane, and conducted consistent with United States and International law*". It also provided that "*the United States may transport additional detainees to U.S. Naval Station Guantánamo Bay when lawful and necessary to protect the nation*".[147]

165. In evidence to this Inquiry, the Chief of SIS reiterated how it handled the US change of policy on Guantánamo:

> *Now, what we did when some of those comments were made around Guantánamo was to make clear on all channels ... the Government's position of opposition to Guantánamo and its use and we ***, made sure they understood just the sort of difficulties they would pose for our partnership if they went down this route again.*[148]

166. While that is reassuring when it comes to public announcements such as that in 2018, we note that there is always the danger that – as happened in 2001 – the UK may not be aware of the change in position until it is too late.

167. At the other end of the spectrum are cases where the compliance concerns are so severe that they cannot be reduced sufficiently and the Agencies are unable to undertake any activity with that particular foreign partner. For example, SIS has reported to the Committee that in ***. Asked during this Inquiry whether it still engaged, or whether its approach had changed in light of ***, SIS told the Committee:

> *any thoughts that we might once have had that we might have a carefully circumscribed, compliant discussion with *** has long evaporated, I'm afraid, so there is absolutely no current conversation with them on that subject.*[149]

Broken assurances

168. Given the importance of assurances regarding behaviour in enabling the Agencies to move forward, it is essential that the Agencies keep such assurances – and associated behaviours – under review. Where a breach is discovered, the Agencies must take immediate action. There is also then a need for the Agencies – together with Ministers – to consider whether, in the light of the broken assurances, a foreign partner can be trusted again, and if further measures must be put in place to prevent reoccurrence.

169. SIS provided the Committee with a specific example of how it has dealt with, and responded to, broken assurances from foreign partners in the context of capacity building:

[147] Executive Order 13823: Protecting America Through Lawful Detention of Terrorists, 30 January 2018.
[148] Oral evidence – SIS, 27 May 2021.
[149] Oral evidence – SIS, 27 May 2021.

- SIS had a longstanding programme of capacity building with a unit within DAHLIA, ***.[150] The use of this capability was governed by a Memorandum of Understanding (MoU), which allowed it to be used for joint and unilateral priorities relating to international terrorism, hostile state actors, counter-intelligence and serious and organised crime such as kidnapping.
- On 22 January 2021, SIS identified DAHLIA ***.
- SIS notified the then Foreign Secretary on 27 January 2021. In response to the breach, SIS and *** on overt and covert channels. As recommended by the then Foreign Secretary, SIS signalled the risk of withdrawal of support/capability if the issue recurred.
- On 30 January 2021, SIS identified ***. SIS told the Committee that ***.
- SIS sought ministerial approval to continue to rely on the extant section 7 ISA authorisation for the continued capacity-building programme with DAHLIA. The submission provided the then Foreign Secretary with a full update on the risks and 'mitigations'. Continued engagement was approved by the Foreign Secretary on 2 February 2021.[151]

170. As can be seen, it is critical for the Agencies to be not only alert to the possibility of breaches, but also to ***. SIS assured the Committee that it keeps assurances under review:

> ***[152]

171. Nevertheless, there will be circumstances where the Intelligence Community will receive intelligence without knowing its provenance, leaving open the possibility that information received from liaison partners may have been obtained through torture or other unacceptable treatment. MI5 noted this difficulty in its evidence to the Committee:

> *we have a legal and an ethical responsibility to have our eyes wide open and to try to understand where did this information come from … does this potentially valuable lead have some ghastly sort of ethical provenance on which we are unsighted …*
>
> *We might get cases where someone has been detained and we've asked questions about the circumstances of their detention and been given no response and we might then receive some information. So it's always a more inferential and difficult and sometimes grey set of judgments.*[153]

N. The evidence we have received reassures us that, wherever possible, appropriate due diligence is carried out to ensure that information is not obtained via prohibited methods. However, we note that that cannot be guaranteed.

[150] For the purposes of this Report, the code word 'DAHLIA' has been adopted for references to ***.
[151] Written evidence – SIS, 2 July 2021.
[152] Oral evidence – SIS, 27 May 2021.
[153] Oral evidence – MI5, 17 June 2021.

Human error

172. In organisations dealing with complex situations involving legal and policy risk, and ethical challenges, it is inevitable that mistakes are sometimes made. What is critical is that any such mistakes are identified and action taken. The Chief of SIS was frank in evidence to the Committee about the continuing difficulty SIS faces with respect to this:

> *So of course mistakes happen, you know, we're human, and the people working in the organisation are human, so they do happen from time to time.*
>
> *Usually they are kind of procedural, you know, nothing has happened, but procedurally we haven't gone through the various hoops we should have done. Sometimes it's a bit more serious than that and we have a breach of compliance.*
>
> *I'm really focused on encouraging a culture within the organisation of prompt candour. You know, if things go wrong, you fess up and you fess up fast and I think we have that culture and clearly if people have made a mistake, then, depending on the seriousness of it, there has to be consequences and there has to be accountability for it.*[154]

173. In terms of the action taken, the Chief of SIS told the Committee: "*if things go wrong, then ... we alert the Commissioners immediately ... and I get a letter fired off to the Foreign Secretary pretty damn quick on it as well*".[155]

174. The Agencies and DI are under a duty to report any errors relating to IPA, RIPA or The Principles to the IPC, who will review the cases and report on them in his annual report. The operational substance of the Agencies' work is contained in a Confidential Annex to that report. This Committee asked the IPC for sight of the Confidential Annex (the Committee having received the Confidential Annexes produced by the IPC's predecessor organisations); however, he indicated that, while he had no objection to the Committee having sight of it, his report is made to the Prime Minister and it is therefore for the Prime Minister to provide it to the Committee.

175. After a very lengthy delay, the Cabinet Office provided a copy of the Confidential Annex to the 2019 IPC Annual Report. However, the Annex has been – unexpectedly – heavily redacted. The then Deputy National Security Adviser (DNSA) attempted to justify the extensive redactions on the grounds that "[the Confidential Annexes] *contain information relating to current (rather than past) operations and operational matters not of significant national interest"*. However, her letter states that the redactions are "*based on* [the] *Agencies' understanding of what aspects were 'current' operations at the time of issue*". In other words, if an operation was current in 2019, then it has been redacted now, even if it is not 'current' in 2021.

176. This is completely contrary to the letter and spirit of the MoU between the Committee and the Prime Minister, which is clear that 'an ongoing operation' refers to something ongoing now, in the present. Whether an operation was ongoing previously – in this case at the time of publication of the Report – is not a relevant consideration. In addition, the MoU states that enduring "*long-running operations may be considered within the ISC's remit*" –

[154] Oral evidence – SIS, 27 May 2021.
[155] Oral evidence – SIS, 27 May 2021.

so, to the extent that such operations are considered 'current' on this basis, then they fall within the Committee's remit and should be provided. Further, the MoU states: "*Deciding whether a matter is or is not a part of 'any ongoing intelligence and security operation' will be a matter of judgement for the Prime Minister and the ISC*" – these are not therefore decisions for the DNSA to take. As the MoU makes clear, "[the] *final decision will rest with the Prime Minister, in conjunction with the ISC*".

177. There were no grounds for this unacceptable approach, and the Committee has written in the strongest terms to the National Security Adviser. We trust that he will consider – and advise the Prime Minister – that it is a matter of some importance that this Committee, on behalf of Parliament, is provided with a full copy of the Annual Report, including the Confidential Annex.

Joint units

178. As discussed in the chapter above on How partnerships work, the Agencies – primarily SIS – engage in 'joint units' with the intelligence services of certain international partners. Such units provide many operational benefits to SIS, *** and enabling SIS to generate a *** trusted and capable partnership which, over time, is likely to pay operational dividends. However, given that many of these units are not under the exclusive operational control of SIS – most will also be working to requirements set by their own government – ***.[156] Joint units mentored and provided with funding and capabilities by SIS therefore pose particular compliance challenges since SIS will be held legally and morally responsible for their actions.

179. The Committee's 2014 *Report on the intelligence relating to the murder of Fusilier Lee Rigby* and 2018 *Detainee Mistreatment and Rendition: Current Issues* detailed how such units can pose a very serious risk to the Agencies, both in terms of their compliance with the law and the potential damage to their reputation.[157]

***Kenyan joint unit – ARCTIC*[158]**

In 2013, as part of its Inquiry into the murder of Fusilier Lee Rigby, the Committee considered SIS's work with a joint unit, 'ARCTIC'. ARCTIC was created in 2003 when SIS recognised the need for *** to improve its counter-terrorism capability.

ARCTIC comprised *** who were attached to the unit for up to two years, who were trained, mentored and tasked by SIS. SIS's work on counter-terrorism *** was, at that time, handled primarily through ARCTIC. ARCTIC could be tasked by both SIS and ***, but not by the *** or any other organisation. In 2013, during its oral evidence to the Committee, SIS said that it provided "*about* ***" to fund ARCTIC's operations.[159]

[156] Oral evidence – SIS, 27 May 2021.
[157] *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, HC 795, November 2014; *Detainee Mistreatment and Rendition: 2001–2010*, HC 1113, June 2018.
[158] 'ARCTIC' is a code word we have substituted for the actual name of this unit, which is ***.
[159] Oral evidence – SIS, 24 October 2021.

During its 2013 Inquiry, the Committee learned that Michael Adebolajo – who was subsequently convicted of the murder of Fusilier Lee Rigby – had been arrested in Kenya in November 2010, as he was suspected to be travelling to Somalia to join the terrorist group al-Shabaab. Kenyan Police informed a locally deployed Metropolitan Police Service officer, who subsequently informed SIS officers in Kenya at the time. Adebolajo later made two separate allegations of mistreatment during his detention in Kenya to British officials, including a claim that "*he was beaten, and threatened with electrocution and rape on more than one occasion during his detention*".[160]

It transpired that Adebolajo was interviewed twice whilst in detention in Kenya: first by the Kenyan police and then by ARCTIC. When Adebolajo reported his mistreatment to UK officials, it was not clear whether he was referring to his treatment by the Kenyan Police, by ARCTIC, or by both. At the time of its Inquiry, the Committee noted that SIS did not try to establish which unit Adebolajo's allegations of mistreatment referred to, despite the fact that one of the two organisations was a unit which was part-funded and part-tasked by SIS. This was surprising to the Committee: if Adebolajo's allegations of mistreatment did refer to his interview by ARCTIC, then HMG could be said to have had some involvement, whether or not UK personnel were present in the room.

At the time, the Agencies told the Committee that there was no reference within the Consolidated Guidance to the "*particular scenario*" of Adebolajo's arrest and detention.[161] SIS repeatedly stated:

> *there is no doubt in our mind that the Consolidated Guidance was not engaged in this case ... SIS had no prior knowledge of plans to detain Adebolajo, or that the detention was about to take place, nor had SIS ever previously discussed this individual with the Kenyans ... once SIS learned of his arrest and the immediate plans to deport him, SIS did not seek to interview Adebolajo, feed in questions or seek intelligence information. They only engaged to check the progress of his deportation to the UK.*[162]

SIS went on to say:

> [the Consolidated Guidance] *cannot apply because we did not know – the consolidated guidance applies when we make something happen. By definition, we did not know it was going on. We could not have made it happen.*[163]

Followed through to its logical conclusion, this would have meant that SIS could provide funding and tasking to a unit with a foreign partner – in this case ARCTIC – and yet bear no responsibility for its actions (up to and including potential cases of torture). The Committee did not accept this position.

[160] Written evidence – Metropolitan Police Service, 25 November 2010.
[161] Written evidence – MI5, GCHQ and SIS, 30 August 2013.
[162] Written evidence – SIS, 23 April 2014.
[163] Oral evidence – SIS, 5 December 2013.

In previous high-profile cases of allegations of mistreatment, SIS in particular has been accused of 'complicity' in mistreatment, even where there was no direct involvement. 'Complicity' has been taken to mean knowledge, awareness, a reasonable expectation of awareness, etc. Given that SIS had a close relationship with ARCTIC, and was jointly responsible for both tasking and funding ARCTIC, the Committee considered that this certainly could be enough to raise questions of complicity, and the impression that a UK intelligence service was 'outsourcing' torture.

The Committee therefore concluded that, where HMG funds, trains and tasks a unit, it must share responsibility for those units' actions. The Committee recommended that HMG must seek to ensure that the same legal and moral obligations to which HMG adheres, and guidance which it follows, also apply to such units. It therefore follows that, where there is a possibility that an allegation of mistreatment might refer to a unit where HMG has such responsibility, then HMG must investigate as a matter of priority to establish whether the unit is involved.

In practice this recommendation meant that the Consolidated Guidance should be amended to make specific reference to the particular scenario of working with joint units. However, a 'light touch' review of the Consolidated Guidance by the Cabinet Office in 2016 failed to act on this recommendation. In August 2017, the Committee was provided with a copy of the draft revised Consolidated Guidance, and was notified that "*the Prime Minister would like to seek the views of the new Committee on it, once appointed*". The Committee published its response to that review as part of its 2018 Report *Detainee Mistreatment and Rendition: Current Issues*.[164]

The Committee concluded that HMG's revised draft did not go far enough and was insufficient. The Committee once again reiterated the importance of specifically addressing the question of joint units within the Consolidated Guidance and making clear that the Guidance applies to such units. Where HMG trains, funds and/or tasks a unit overseas, it must carry some responsibility for the actions of that unit. If it does not, it leaves itself open to accusations that it is outsourcing action it cannot take itself.

The Committee's recommendations and conclusions on joint units were finally taken on board in July 2019, when HMG published revised Guidance known as The Principles. The Principles, which came into force in 2020, replaced the Consolidated Guidance and – some seven years after the Committee raised the issue – finally addressed the issue of joint units.

180. Paragraph 9 of The Principles now makes clear that:

> *These Principles cover the activities of a unit of a foreign authority (which may be wholly or partly funded or trained by the UK) which engages in overseas operations directly with and in support of the work of UK personnel* [from the Agencies, the UK's Armed Forces/MoD, SO15 and NCA] *and is, for the purpose of the unit undertaking the activity described* [in The Principles]*, acting under UK direction*.

[164] *Detainee Mistreatment and Rendition: Current Issues*, HC 1114, June 2018.

181. Joint units therefore explicitly fall within the remit of The Principles so long as the joint unit is acting under UK tasking. The Committee recognises that this is often a fine distinction; however, it is vital that rigorous consideration is given to what types of capabilities are given to joint units, given the risk that these capabilities could be misused when not being tasked by the UK. The Committee was told in evidence:

> *the joint units ***. So by definition they're usually tasked by us, but not always exclusively and it's important to be clear for example on the Fulford Principles that they only come into operation when those joint units are working to our tasking on issues which are to do with detainee-type* [or] *law enforcement-type activity.*
>
> *So these joint units might well do other stuff separately, which cycles back to the point I made about us needing to be very careful ***.*[165]

O. Most countries – even our closest allies – will operate under different legal and ethical constraints to the UK. However, to protect the UK we have no choice but to work with other countries. The framework under which our Agencies engage is therefore of the utmost importance.

P. The UK's legal and compliance framework governing engagement in international partnerships is comprehensive. The importance of adhering to legal obligations seems to be clearly understood and to have been embedded into the operational culture and decision making of the Agencies. The Committee is pleased to see this cultural change.

Q. There must be no complacency. The history of the Agencies' work with partners on detainee issues has been problematic – at best. It is clear that lessons have been learnt, but it is vital that the Agencies continue to adhere to, and build upon, robust oversight arrangements when working with foreign partners on detainee matters.

R. Law and compliance should be an inherent part of operational teams, not just part of the operational process. The Agencies should consider having embedded legal and compliance teams within operational missions, and particularly in overseas hubs where detainee work with partners is central. This would help to strengthen the compliance framework and provide on-hand expertise when needed.

S. Agency policy underpinning The Principles and the Overseas Security and Justice Assistance guidance appears to be respecting both the letter and spirit of the framework – as was clear both from the evidence taken as part of this Inquiry and when considering the most recently published report from the Investigatory Powers Commissioner's Office, who oversees much of the day-to-day activity of the Agencies.

T. The Principles appear to be working well, and are well integrated into Agency processes. While the Committee is still concerned that the Foreign Secretary is given significant discretion to authorise activity that may carry a real risk, we are broadly satisfied that, with the additional oversight of the Investigatory Powers Commissioner's Office, there are sufficient checks and balances in the system.

---

165 ***

U. The Committee recognises that assurances are a necessary and important part of dealings with partners who do not necessarily share all of our values or legal frameworks. These appear to be sought and agreed effectively. We would encourage the Agencies to assign more effort where possible to the continued assessment of assurances, given that they are fundamental to the Agencies' ability to operate in certain areas.

V. The Agencies and Ministry of Defence must maintain a comprehensive written record of assurances sought and received. The Committee was impressed by MI5's Liaison with Overseas Security and Intelligence Agencies (LOSIA) form, which considers comprehensively the different elements of working with partners on detainee issues. We recommend that the Agencies introduce a single streamlined document based on LOSIA, so that recording of activity and assurances is done in a consistent way.

W. Given the need to work with some partners who engage in unacceptable treatment of detainees, the Committee is supportive of the Agencies' ability to carve out compliant pathways to enable them to work with states on a bespoke basis. This does not excuse or imply approval of unacceptable behaviour more generally, and the Agencies must do everything possible to manage and reduce risk when working in this area.

X. We welcome the introduction of the 'last pair of hands' principle, which ensures that there is a clear risk owner for all operational stages when working with a foreign liaison partner.

Y. The creation of PURPLE is a positive development for the UK Intelligence Community as a whole, and the Committee welcomes the work it has done. The tri-Agency nature of the team ensures consistency of approach across all three Agencies.

Z. The Prime Minister should provide this Committee with a full copy of the Confidential Annex to the Annual Report of the Investigatory Powers Commissioner 2019. The approach being taken by the Deputy National Security Adviser to redact operations that were 'current' in 2019 as if they were current today was severely misguided at best. When the Prime Minister determines the final outcome – in conjunction with the ISC, as set out in the Memorandum of Understanding – we trust that he will follow the spirit of the Justice and Security Act 2013 and the commitments given to Parliament during the passage of that legislation.

AA. The Committee is satisfied that, on balance, the serious risks of engaging with authoritarian and oppressive regimes are well understood by UK intelligence Agencies.

BB. The Agencies appear to take seriously the ethical dimension of their work. The Committee is pleased to learn of the staff counsellor to support officers, as well as several examples of how the organisations as a whole discuss and reflect on their more difficult partnerships. The Committee is satisfied that there is a genuine recognition of the broader impact of these relationships and the need for continued monitoring of their appropriateness.

CC. The Committee is pleased to see that its recommendation relating to joint units has finally been taken on board and that engagement with such units is now explicitly covered by The Principles. However, it is disappointing that HMG took nearly seven years to amend its policy. This is an unacceptable delay given the gravity of the compliance risks and volume of joint work undertaken by SIS.

THE FIVE EYES

182. The Five Eyes alliance is the UK Intelligence Community's most important partnership. Consisting of Australia, Canada, New Zealand, the UK and the United States (US) – countries with a shared language and history, and with common values and similar legal systems – it is of a "*fundamentally different nature*" to the other relationships maintained by the Intelligence Community.[166] It is, in the words of a previous Foreign Secretary, "*critically important*" to the UK.[167]

183. The alliance emerged during the Second World War, during which international intelligence co-operation between the UK and US advanced significantly, particularly in relation to signals intelligence (SIGINT). The 1946 British–US Communication Intelligence Agreement – subsequently known as the UKUSA Agreement – formalised the SIGINT partnership and committed the UK and US to an unprecedented level of peacetime co-operation. The UKUSA Agreement was subsequently extended to include Canada (in 1948) and Australia and New Zealand (in 1956), thereby creating the 'Five Eyes' intelligence-sharing alliance. While the partnership was initially focused on SIGINT, it has since expanded to include all forms of intelligence collection and assessment.

184. Engagement with Five Eyes partners includes formal intelligence sharing, joint operational working and joint capability development. The alliance has several key characteristics, including:

- significant levels of trust between each partner, developed over decades of collaboration;
- a presumption towards sharing all SIGINT material with the other Five Eyes partners, such that withholding information would in many instances be seen as the exception;
- unparalleled levels of integration, with many shared capabilities and operations, common objectives, ***; and
- global intelligence coverage, the result of ***, and operational capabilities of five advanced intelligence communities, each of which bring their own particular geographic, technical and thematic expertise.[168]

185. The Agencies and DI each stressed the importance of the Five Eyes:

- MI5 told the Committee that "*our Five Eyes partnerships are immensely important to MI5's mission to protect UK national security … The trust that we have is unparalleled, and we draw strength from working together against a range of security threats spanning all of MI5's mission areas.*"[169]

[166] Written evidence – SIS, 2 November 2020.
[167] Oral evidence – Foreign Secretary, 22 July 2021.
[168] Written evidence – GCHQ, 2 November 2020; Written evidence – SIS, 2 July 2021.
[169] Written evidence – MI5, 3 June 2021.

- SIS categorises the Five Eyes partnership as being of "*critical*" priority, with the alliance "*based on a high level of trust in each other, our tradecraft and our operational decision making*" and with shared "*intelligence, capabilities and technology developments*".[170]
- In evidence to the Inquiry, GCHQ said: "*The Five Eyes continue to be GCHQ's closest and ... most productive foreign partnerships. Our strategic direction and requirements remain broadly aligned ... and so we continue to derive very significant benefits from the scale of the intelligence sharing.*"[171]
- DI told the Committee: "*The Five Eyes relationship ... underpins nearly all of the work of Defence Intelligence in some shape or form, providing access to capabilities* *** ... [it is] *fundamental to delivery across DI's outputs.*"[172]

186. The Five Eyes is a flexible construct, capable of operating in different combinations of its five members, instead of always operating as a collective. Furthermore, it is important to note that the Five Eyes alliance does not inhibit the UK Intelligence Community's ability to act unilaterally or to choose not to share information when required; rather, the Five Eyes supplements and greatly enhances the UK's sovereign intelligence collection and assessment capabilities.

Engagement

187. Co-operation and collaboration with Five Eyes partners extends to every level of the Intelligence Community, from the Heads of the Agencies to desk officers and analysts working on specific issues. The Five Eyes hold regular meetings and working groups, at a variety of levels, to discuss and agree strategies, co-ordinate operations, and set future priorities for investment and intelligence collection.

188. There is an annual conference which *** attend to discuss matters of strategic importance; ***.[173] There are also a number of strategic defence-specific Five Eyes intelligence fora which are attended by the Chief of Defence Intelligence (CDI). The CDI highlighted the benefits of such meetings:

> *I would say* [the] *purpose is to reduce the friction to enable the* [working-level] *analysts to talk to each other, whether that be physically, remotely; to be able to collaborate effectively; to disseminate their product; to be able to share accesses, and the whole process of* [senior-level meetings] *is about minimising that friction and enabling people to work effectively.*[174]

189. Senior engagement does not take place within the Five Eyes only as a collective: the Heads of the Agencies and DI also hold regular bilateral meetings with their respective Five Eyes counterparts, as well as with different combinations of Five Eyes partners as required. Below the most senior groups is a series of deputies and working groups which work to specific objectives on investigations, technological development, or policy initiatives.

[170] Written evidence – SIS, 2 November 2021.
[171] Written evidence – GCHQ, 20 November 2020.
[172] Written evidence – DI, 3 November 2020.
[173] Written evidence – MI5, 23 November 2020.
[174] Oral evidence – DI, 10 June 2021.

190. Five Eyes partners also ***. This facilitates a greatly enhanced mutual understanding of Five Eyes partners' organisational processes and capabilities, thereby strengthening the alliance further.

191. DI has taken significant steps to integrate Five Eyes partners into its work through the development of its 'Pathfinder' facility at RAF Wyton. This was described to the Committee as "*a unique experiment within the Five Eyes community ... designed from the outset to accommodate Five Eyes working, both in terms of having Five Eyes personnel on the floorplate ****".[175]

Ways of working

Intelligence exchange

192. At its most basic level, the Five Eyes alliance is a vehicle to allow for the sharing of intelligence between trusted partners. This allows each partner to harness the unique capabilities, resources and expertise of the others for the purpose of protecting their own national security.

193. The default position within the alliance is to share intelligence and capabilities with the other Five Eyes partners, unless – for reasons of security or due to specific national sensitivities – it would not be appropriate to share outside the government in question. Director GCHQ described this presumption towards sharing information as "*the principle that underpins all of the Five Eyes intelligence sharing*".[176] In a similar vein, the Chief of SIS – the Agency which has traditionally been most reticent about sharing its intelligence with other countries – assured the Committee that "*the default is to share as much as we can with Five Eyes partners*".[177]

194. This willingness to share the majority of the intelligence collected by five sophisticated intelligence communities – including the US, with its unparalleled resources and capabilities – means that the flows of information between the Five Eyes partners are significant. To give two examples: over a typical month, GCHQ reissues approximately *** Five Eyes SIGINT reports to UK customers (representing around *** of the total SIGINT reporting which GCHQ issues); and in the year to November 2020, MI5 received over *** formal intelligence reports from Five Eyes partners.[178] DI benefits on a similar scale.

Challenge

195. The free exchange of information allows for a co-ordinated Five Eyes approach to particular themes or operational needs. MI5 cited the value of pooling the Five Eyes' collective understanding of a particular topic – China, for instance – to share the burden of developing expertise; in this respect, "*the totality of the Five Eyes is ... powerful*".[179] However, shared information and shared objectives do not mean that the Five Eyes always

[175] Written evidence – DI, 14 May 2021.
[176] Oral evidence – GCHQ, 1 July 2021.
[177] Oral evidence – SIS, 27 May 2021.
[178] Written evidence – GCHQ, 20 November 2020; Written evidence – MI5, 23 November 2020.
[179] Oral evidence – MI5, 17 June 2021.

agree with each other in their assessments or understanding of a problem. As the CDI told the Committee:

> *we might get access to the same material but we think about it differently … we've got that divergence of thought which is incredibly valuable, and we avoid groupthink and it means … we have a really robust conversation about our conclusions and that's … an incredible part of the experience.*[180]

196. This diversity of perspective is a great strength of the partnership, with each Five Eyes intelligence community benefiting from the wisdom and expertise of their counterparts across the alliance.

***

Burden-sharing

197. While the exchange of information and views, and ***, is of great benefit, of equal if not greater importance is the 'burden-sharing' arrangement between the partners – that is, in certain cases, the Five Eyes partners will explicitly split some intelligence work and assessment between them to avoid unnecessary duplication of effort. This allows each partner to focus on developing expertise in certain subjects (often defined by respective capabilities and national interests), and lessens the risk of spreading finite resources too thinly. Extensive burden-sharing of this sort – based on deep trust in the other members' capabilities and analysis – is a unique aspect of the Five Eyes alliance, and one from which the UK derives huge advantage.

198. The divisions of labour are generally based on relative proximity and traditional expertise. For instance, when it comes to DI's geospatial intelligence (GEOINT) analysis, the UK covers much of the analysis of ***.

199. The CDI explained how burden-sharing enables DI to access intelligence and expertise on subjects for which it does not have a regular intelligence requirement, without having to make a disproportionate investment of resources in order to do so:

> *why would I bother applying a vast amount of effort into* [for example] *** *when we've got *** expertise both on the ground as well as in their analytical teams at home and that's part of the strength of the partnerships. So … if I need something on *** … I need to be able to phone my opposite number and say I need this and I need it tomorrow … and that's part of the benefit of the relationships.*[181]

200. The Chief of SIS made a similar point, citing *** as an example of a country on which SIS had limited coverage, but for which it could rely on Five Eyes partners for intelligence: "*when I find myself with no independent reporting on ***, both our American and Australian friends have been very responsive on coming back to us on it*".[182]

[180] Oral evidence – DI, 10 June 2021.
[181] Oral evidence – DI, 10 June 2021.
[182] Oral evidence – SIS, 27 May 2021.

201. The CDI also explained to the Committee that geography enables the Five Eyes to achieve more complete and consistent intelligence coverage. This is done through so-called 'follow the sun' working, whereby high priority tasks can be 'passed' around the Five Eyes community to allow 24-hour working:

> *imagery analysts that are at* [RAF] *Wyton … hand the mission on to analysts that are in Washington D.C. or St Louis and to our Canadian partners who will then hand on to Australian and New Zealand partners who then hand back to us*[183]

202. The benefits of burden-sharing were brought to the fore during the Covid-19 pandemic, with DI reporting: "*The Five Eyes burden-sharing arrangements, particularly on GEOINT, have been especially helpful in mitigating risks amongst the partners.*"[184]

Capability development and operation

203. In addition to sharing intelligence and mounting joint operations, Five Eyes' burden-sharing extends to decisions around investments in new capabilities. For example, the CDI explained to the Committee:

> *we're looking hard, at the moment, as a consequence of the Integrated Review … about UK space assets and what ISR* [intelligence, surveillance and reconnaissance] *assets we may put into space and I think there are two benefits that accrue. One is it gives us greater sovereign capacity and … it also enables me to pay more into the Five Eyes pot. So, whatever satellite capacity we may develop in future, I'm very keen to make sure that … as a group of Five Eyes nations, we get more collectively* [rather than duplicating US capability].[185]

204. Even more significantly, this co-operation also extends to the development and operation of some *** capabilities. By its nature, such co-operation requires significant trust as it involves sharing openly with partners the extent of the UK's existing intelligence capabilities. For this reason, the Intelligence Community limit their co-operation capability development largely to Five Eyes partners.

205. Joint capability development with the Five Eyes occurs across the spectrum of the Intelligence Community's activities. They might look to develop ***.[186]

206. Much of the Intelligence Community's capability development work with Five Eyes partners is led by the Agencies' jointly run teams from MI5 and SIS (***). Five Eyes partners ***.[187]

207. Collaboration of this nature is mutually beneficial and allows Five Eyes partners to make contributions proportionate to their own requirements (for example, ***).[188] SIS told the Committee: "*In addition to burden-sharing ***, Five Eyes partners bring additional*

[183] Oral evidence – DI, 10 June 2021.
[184] Written evidence – DI, *Covid-19: Impact on DI Business (Annex to CDI letter)*, 3 November 2020.
[185] Oral evidence – DI, 10 June 2021.
[186] Written evidence – SIS, 2 July 2021.
[187] ***
[188] ***; Written evidence – SIS, 2 July 2021.

capabilities, skills and resources that are either unique or would have been costlier for [the Agencies] *to develop … or acquire from the market.*"[189]

208. *** is another particularly productive avenue for joint capability development. GCHQ stressed the importance of this during evidence, noting that ***.[190]

209. However, joint capability development, though beneficial, is not without risk. It relies on all the intelligence partners being able to protect the integrity of the capability or capabilities in question – with potentially very serious consequences should this not happen. The leak in 2013 of huge volumes of National Security Agency (NSA) and (allegedly) GCHQ information by former US intelligence contractor Edward Snowden is a case in point. As GCHQ explained to the Committee, ***[191]

210. The Committee was told that the Snowden leaks "*led to a severe dip in intelligence output, and* ***".[192] ***.

211. In response to the Snowden leaks and the resulting severe damage ***.[193]

Medical intelligence at DI

***.

DI maintains the UK's only permanent medical intelligence (MEDINT) capability.[194] This unique capability, which continues to mature, *** DI told the Committee that "*pre-existing MEDINT relationships *** were instrumental in enabling us to build our capabilities and understanding* [of the Covid-19 pandemic] *quickly*".[195]

***.[196]

The Chief of Defence Intelligence explained to the Committee how, during the Covid-19 pandemic, DI worked with *** to develop a range of MEDINT which was used to inform policy-makers in the UK and overseas:

> ***.[197]

[189] Written evidence – SIS, 2 July 2021.
[190] Oral evidence – GCHQ, 1 July 2021.
[191] Oral evidence – GCHQ, 1 July 2021.
[192] Written evidence – GCHQ, SIS and MI5, 18 October 2021.
[193] Oral evidence – GCHQ, 1 July 2021.
[194] DI defines MEDINT as "*the expert fusion, analysis and assessment of medical, bio-scientific, epidemiological, environmental and other information related to human or animal health from classified, open and technical sources*"; Written evidence – DI, 17 September 2020.
[195] Written evidence – DI, 9 September 2020.
[196] Written evidence – DI, 14 May 2021.
[197] Oral evidence – DI, 10 June 2021.

Prohibition on espionage

212. One of the features of the Five Eyes alliance is that ***. This is a reflection of the deep and enduring levels of trust between the partners, and their collective approach to common threats. The Chief of SIS was explicit about this, saying: "*As is fully on record, we do not spy on Five Eyes countries.*"[198]

213. ***.[199]

214. We also note that long-standing agreements between the Five Eyes countries mean they cannot ask each other to target each other's citizens or individuals that they cannot themselves target, or in any other way seek to circumvent their own or each other's legal and policy obligations.[200]

DD. The Five Eyes alliance is a remarkable testament to the power of international partnerships to increase the reach, influence and capability of the parties concerned such that the whole amounts to more than the sum of its parts.

EE. Providing access to intelligence and capabilities far beyond that which the UK Intelligence Community alone can obtain, and facilitating burden-sharing for intelligence collection and analysis in a way that allows the respective members to develop greater expertise and coverage, the Five Eyes alliance is a truly exceptional arrangement that is wholly in the UK's interest. Maintaining and reinforcing the Five Eyes alliance, and the UK's place within it, should be the Intelligence Community's highest priority in relation to international partnerships.

The United States

The US Intelligence Community (USIC) consists of a total of 18 organisations. However, the UK Intelligence Community work primarily with six of these:

- The Federal Bureau of Investigation (FBI) – the domestic security and intelligence service of the US, with which MI5 has a strong relationship.
- The Central Intelligence Agency (CIA) – the US government's all-source foreign intelligence and assessment service. Given its foreign intelligence remit, SIS is the main interlocutor for the CIA within the UK system, and MI5 also has a strong relationship with the CIA.
- The National Security Agency (NSA) – GCHQ's counterpart SIGINT agency and a part of the Department of Defense (DoD).
- The Defense Intelligence Agency (DIA) – a part of the DoD and DI's direct counterpart.

[198] Oral evidence – SIS, 27 May 2021.
[199] ***
[200] The Committee noted the existence of such agreements in a public statement on 17 March 2017, following allegations that the former President of the United States, Barack Obama, had tasked GCHQ to 'wire tap' the then President of the United States, Donald Trump, during the 2016 US Presidential election.

- The National Geospatial-Intelligence Agency (NGA) – also part of the DoD, the US lead agency for GEOINT and another direct counterpart of DI.
- The National Reconnaissance Office – an agency of the DoD with responsibility for designing, building and maintaining US intelligence satellites, and with which GCHQ and DI also partner.

215. The Intelligence Community's partnership with the US is the most important that they maintain. The product of decades of collaboration and trust, it is the backbone of the Five Eyes alliance and, arguably, of the broader relationship between the UK and US. It is also a partnership from which the UK benefits hugely – and to which the UK contributes significantly, not least by sharing some of its finest minds and best-kept secrets.

216. The Agencies and DI each maintain their own relationships with counterparts in the US system, supported by engagement at the highest levels of government.

MI5

217. MI5 describes the US agencies as "*our closest partners with huge reach and unrivalled intelligence capabilities*".[201] MI5 works with all three main agencies in the USIC: the CIA, the FBI and the NSA. The FBI, with its domestic security remit, would appear to be the natural counterpart for MI5. *** MI5 shares *** information with the CIA ***.[202] ***.[203]

218. MI5's intelligence sharing with the US is *** extensive – for example, between November 2019 and November 2020, MI5 received *** formal intelligence reports from the USIC (***).[204] Following a scaling-up in co-operation, MI5 now also ***.[205] MI5's written evidence explained the operational benefits of its *** arrangements with US counterparts:

> ***.[206]

***.[207]

SIS

219. SIS's direct US counterpart is the CIA. SIS considers this partnership its "*most important liaison intelligence relationship*", and has told the Committee that "*the UK is markedly safer because of this collaboration*".[208] ***.[209]

---

[201] Written evidence – MI5, 23 November 2020.
[202] Written evidence – MI5, 23 November 2020.
[203] ***
[204] Written evidence – MI5, 23 November 2020.
[205] Written evidence – MI5, 23 November 2020.
[206] Written evidence – MI5, 23 November 2020.
[207] Written evidence – MI5, 23 November 2020; Written evidence – MI5, 26 November 2021.
[208] Written evidence – SIS, 20 January 2020; Written evidence – SIS, 24 August 2018.
[209] Written evidence – 20 January 2020.

220. SIS has previously reported to the Committee that the CIA acknowledges SIS "*as being staffed with world-class agent-runners and recruiters*", and that it is "*seen as bringing quality rather than quantity*" to the partnership.[210] SIS intelligence reports have a high impact in Washington D.C.: SIS has been told by US counterparts that those preparing the President's daily intelligence brief "*cite UK intelligence *** regularly ****".[211]

221. The Chief of SIS was keen to emphasise the value the CIA gains from the partnership:

> *Despite* [the US's] *size, despite their ability to span the globe as they do, we can still do things, it seems, that they sometimes find difficult to do and we can still recruit agents that provide intelligence which they deeply value …*
>
> *So I think they see us … as a force-multiplier and an enabler for them … it's a great partnership; I'm not pretending it is an equal partnership, but they get a lot of value out of it.*[212]

222. In return, SIS benefits from receiving large quantities of intelligence from the CIA. The Chief of SIS told the Committee:

> *it goes up and down, but routinely something between *** per cent of our published intelligence comes from the Americans. That's a huge contribution to our intelligence output.*[213]

US intelligence is particularly important for SIS in relation to the most acute state threats to the UK – for instance, around *** of SIS reporting on *** is derived from CIA intelligence.[214]

223. SIS and the CIA also collaborate on the development of new capabilities ***. One example of joint SIS–CIA capability development was the *** programme, ***.

224. The *** programme was conceived as a response to ***. SIS told the Committee that the project had "*** *and it established a platform for further bilateral co-operation*".[215]

225. Such collaboration is founded on deep mutual trust. SIS noted candidly ***:

> *There is a *** initiative where we can sit down and be pretty frank with one another about our methods and put that on the table. It really is a *** our most up-to-date methodology.*[216]

[210] Written evidence – SIS, 24 August 2018.
[211] Written evidence – SIS, 24 August 2018.
[212] Oral evidence – SIS, 27 May 2021.
[213] Oral evidence – SIS, 27 May 2021.
[214] Written evidence – SIS, 16 November 2020.
[215] Written evidence – SIS, 2 July 2021.
[216] Oral evidence – SIS, 27 May 2021.

226. SIS's willingness to share its methods with the CIA is indicative of its approach towards the CIA more broadly. The Chief of SIS explained to the Committee:

> *we share some of our most sensitive secrets* [with the CIA] *and they share some of their most sensitive secrets with us, because there is an intimacy and trust built up over many, many decades.*[217]

GCHQ

227. GCHQ's main US counterpart is the NSA, which performs similar (though not identical) functions.[218] GCHQ considers the NSA to be its single most important partner, making "*a critical contribution to almost all of GCHQ's intelligence capabilities and missions*".[219] Of the Intelligence Community's partnerships with the US, GCHQ's partnership with the NSA is the most extensive and trusting.

228. In March 2021, Director GCHQ and the Director of the NSA celebrated the 75th anniversary of the UKUSA Agreement with a joint public statement. After noting the history, and evolution, of the partnership between the two organisations, and its expansion to form the Five Eyes alliance, the Directors said:

> *For 75 years, this extraordinary partnership has enabled us to evolve and learn from each other. It helps us equip our leaders with the information they need. And it ultimately makes the UK and US safer. We celebrate those 75 years and we look forward to the future together.*[220]

229. In evidence to the Committee, Director GCHQ expanded on the importance of the NSA partnership:

> [The formal GCHQ-NSA relationship, based on the UKUSA Agreement] *is still without doubt our most important intelligence relationship. It forms the basis for what became the Five Eyes, which was a SIGINT construct at the beginning, and has expanded out into the broader Five Eyes intelligence, security and defence relationship ever since. So it's absolutely the heart of our … relationship with the US.*[221]

230. The importance of the UKUSA Agreement lies in the mutual presumption towards unrestricted sharing of SIGINT with the other party, keeping exceptions to an absolute minimum. GCHQ has told the Committee that this aspect of the partnership "*makes it quite different in character*" to other partnerships which – while exceptionally close – do not have that same level of presumption towards information sharing.[222] The practical consequence can be seen in GCHQ's output: a significant proportion (approximately ***) of GCHQ's

[217] Oral evidence – SIS, 27 May 2021.
[218] GCHQ also has a partnership with US Cyber Command, which has responsibility for offensive cyber operations (in the UK sense). Although the NSA and Cyber Command are different organisations, they are headed by the same four-star US military officer to ensure coherence between their activities.
[219] Written evidence – GCHQ, 2 November 2020.
[220] Joint public statement by Director GCHQ and the Director of the NSA, 5 March 2021.
[221] Oral evidence – GCHQ, 1 July 2021.
[222] Written evidence – GCHQ, 20 December 2019.

total SIGINT reporting comes from Five Eyes partners – and the majority of this is from the NSA.[223]

231. However, the partnership goes far beyond simply sharing intelligence. Director GCHQ told the Committee:

> *This isn't a transactional, "you give us this bit of intelligence and we'll give you this back"* [type of partnership].
>
> *... when we sit down and, for example, talk about ***,* [we] *decide between us *** ... in all of those areas we divvy it up.*[224]

232. This level of sharing, and the closeness of their operational work, means that clear legal frameworks, and shared legal interpretations, are necessary. GCHQ told the Committee how this works in practice:

> *Five Eyes partners respect each other's laws and policies: no partner may ask another to do something that they themselves cannot lawfully do or that it would be unlawful for the other partner to do. For example, GCHQ may not ***.*[225] *Should a case arise in which a Five Eyes partner believed another partner had not adhered to this principle, this would be directly challenged with the partner.*[226]

233. In addition to operational collaboration, the GCHQ–NSA partnership – which brings together some of the finest mathematicians and technologists in the world – has been particularly fruitful for both parties in terms of developing new technologies and capabilities for ***. Cryptology is just one example:

> *Over the history of the UKUSA partnership, there has been particularly valuable analytic co-operation in the field of* [cryptology]*, with many major breakthroughs against target cipher systems being the result of joint work between GCHQ, NSA and other partners.*[227]

234. ***.[228]

235. The extensive co-operation between GCHQ and the NSA requires close co-ordination at all levels. At a senior level, Director GCHQ and the Director of the NSA speak regularly, and also hold more formal reviews at which progress on a broad range of strategic issues – for instance, intelligence priorities, policy developments, and capability programmes and projects – are assessed.[229] This sets the tone for collaboration elsewhere:

> [senior GCHQ staff] *in all the mission areas will ... be in regular co-operation with their opposite numbers in the NSA ... pretty much every week or so.*

---

[223] Written evidence – GCHQ, 20 November 2020.
[224] Oral evidence – GCHQ, 1 July 2021.
[225] GCHQ subsequently corrected this to add that it may not ***; Written evidence – GCHQ, 9 February 2022.
[226] Written evidence – GCHQ, 2 November 2020.
[227] Written evidence – GCHQ, 20 November 2020.
[228] ***
[229] Oral evidence – GCHQ, 1 July 2021.

> *... Then at the team level you will have individuals who are leading different operations, again closely in contact with their opposite numbers, and then that goes right down to the level of our 24/7 operations, where our Event Management Centre pretty much will be in daily contact with ... the NSA's* ***.[230]

***.[231]

236. As well as close working ***, NSA and GCHQ officers work side by side at a number of sites ***.

Case study: *

237. ***.[232] The weight of advantage in the partnership with the NSA is overwhelmingly in GCHQ's favour, and GCHQ was frank about the need for the UK to continue to invest in the partnership in order to maintain access: "*... in order to keep gaining the benefits of partnership we need to be seen to pull our weight*".[233] However, GCHQ has previously told the Committee that the NSA values its contribution. In 2016, then Director GCHQ told the Committee:

> *I think if you asked … the senior people* [in NSA]*, they would say the core of the relationship is still maths and crypt. That's the kind of Crown Jewels. But in just about every area of their business and ours, we have some contribution to make.*
>
> *The other big one of course is *** ... it gives a fantastic advantage to have this ***.*
>
> *So, access is very important to them. ***, and we are not pointlessly competing.*[234]

238. More recently, GCHQ has also told the Committee that US interlocutors "*place a high value*" on, in particular:

1) *the expertise of GCHQ's mathematicians and cryptanalysts;*
2) *GCHQ's internet access;*
3) ****;*
4) *the contribution we make on Cyber, and the prospect of structured co-operation on ***; and*
5) *our analytical and technical expertise.*[235]

[230] Oral evidence – GCHQ, 1 July 2021.
[231] ***
[232] ***
[233] Written evidence – GCHQ, 20 December 2019.
[234] Oral evidence – GCHQ, 8 December 2016.
[235] In this context, 'internet access' refers to GCHQ's ability to intercept lawfully internet traffic running over fibre optic cables or via satellites and other more traditional forms of communication; Written evidence – GCHQ, 20 December 2019.

Defense Intelligence

239. The US is by some distance the most important international partner for DI. It is the only partner with which DI co-operates across all intelligence disciplines, and DI receives a disproportionate return on its 'investment' in this partnership. Overall, DI estimates that around half of its intelligence source material comes from the US.[236] DI's position as a key defence intelligence partner for the US greatly extends its ability to deliver intelligence support to military operations and the wider UK Intelligence Community.

240. DI's main US counterparts are the DIA and the NGA. The latter ***.

241. The British Defence Intelligence Liaison Staff, based in Washington D.C., is responsible for managing the day-to-day relationship between DI and the DIA and NGA, as well as with the DoD more broadly.[237] DI has around *** members of staff posted on liaison and exchange roles in the US – significantly more than it has based in other locations.[238] In return, the US has *** liaison and exchange officers based in the UK.[239]

242. By way of an example, an important aspect of the US partnership for DI is the exchange of GEOINT – in terms of *** – for which DI provides the only capability within the Intelligence Community. ***.[240]

243. Furthermore, DI is not simply a recipient of imagery ***.[241] As the CDI put it to the Committee: "*instead of it being seen … as a sort of 'gifting' of imagery to the UK, actually this is a collaborative mission*".[242]

244. ***.[243]

245. The CDI also stressed that, while DI's ability to match US investments in new capabilities was limited, the UK contributed by using those US capabilities to solve problems and develop intelligence to mutual benefit:

> *we are the beneficiaries of enormous US investment* [in capabilities] *but we bring ingenuity, expertise, innovation and imagination to that enterprise, which adds real value to what they do.*[244]

FF. The UK's intelligence partnership with the US is of a breadth and depth without parallel anywhere else in the world. It is the envy of our allies and adversaries alike. In particular, the partnership between GCHQ and the National Security Agency represents, perhaps, the pinnacle of intelligence co-operation; it is a testament to the ambition and commitment of generations of intelligence personnel on both sides of the Atlantic. Long may it continue.

---

[236] Oral evidence – DI, 31 January 2019.
[237] Written evidence – DI, 14 May 2021.
[238] Written evidence – DI, 3 November 2020.
[239] Written evidence – DI, 14 May 2021.
[240] Oral evidence – DI, 10 June 2021; Written evidence – DI, 3 November 2020.
[241] ***
[242] Oral evidence – DI, 10 June 2021.
[243] ***
[244] Oral evidence – DI, 10 June 2021.

Reliance on the US

246. The importance to the UK of the US intelligence partnership is such that there are few aspects of the Intelligence Community's work that do not to some extent rely on US input – whether that be in the form of intelligence reporting, collection capabilities and technologies, analytical capacity ***. It is a hugely valuable partnership from which the UK is, without question, the net beneficiary.

247. This is extremely positive, and is to be welcomed. However, it does beg the question of whether the UK Intelligence Community are too reliant on their US counterparts. While GCHQ's evidence stated that "*the strength and value of the partnership is such that it tends to be immune to wider governmental or political tensions*", it is not inconceivable that political matters could, in the future, have a material impact on the intelligence partnership.

248. The Committee asked the Heads of the Agencies and DI whether they considered the Intelligence Community to be over-reliant on the US, and what the effects might be of a serious breakdown in the US intelligence relationship:

- The Chief of SIS told us:

  > *Would it be a mortal blow? Well, I hope not. We lived in a world before UKUSA as a service for the first 40 years of our being…*
  >
  > *But would it be a very, very serious blow? Of course. They are incredibly important partners and the UKUSA arrangements – the relationship between GCHQ and NSA, and ourselves and the CIA – are the Crown Jewels of the special relationship. It is absolutely critical.*[245]

- Director GCHQ was clear about the vital importance of the US partnership:

  > *if the Americans walked away, then we would be affected in every area of our intelligence mission … It would be a material impact to us and in some areas it would mean that we couldn't operate …*

  However, he also emphasised the mutual benefit – or dependence – of the arrangement:

  > [but] *I think the same is true for America. So barely a day goes past where there isn't some GCHQ-derived SIGINT in the presidential brief, and we know that they are as dependent on us in areas of capability – *** – as we are on them. So we are the junior partner,* [but] *it's not a* [partnership] *that either of us can cut off easily.*[246]

- MI5 similarly emphasised the closely integrated nature of the partnership:

  > *I don't think we are over-reliant, because we have really strong insights ourselves* [to offer]*, particularly about the threats that we care about. We have*

[245] Oral evidence – SIS, 27 May 2021.
[246] Oral evidence – GCHQ, 1 July 2021.

> *a really deep dependency, though, on a much bigger US machine than the UK – much more resource, much greater reach – and, when we look at the* [terrorism] *threat, for example, a lot of our capacity is based on a US footprint that we partner with.*
>
> *So I don't think it's an over-reliance, but I think it's very woven through in terms of shared capabilities – not just in the Intelligence Community but through diplomatic and defence infrastructure that we can sit on and use.*[247]

- The CDI acknowledged the risk of over-reliance:

> *I think there's always a risk that you get used to something and that, as an intelligence professional, you get used to the access to information,* [and] *it becomes a … routine thing that you can rely upon.*[248]

However, he also suggested that the changing nature of intelligence work would lead to a relative reduction on reliance on partners, including the US:

> *I think there's a fundamental shift ongoing around how we do intelligence work … Increasingly we'll be providing information in … the form of data, to go into decision systems* [for example, on a ship or a fast jet]. *… That's us providing intelligence but it's not traditional intelligence in the sense of providing insight and information.*
>
> *... I think alongside that we're going to see far greater exploitation of publicly available information, and that opens up a wealth of opportunity … we will construct the broad situational understanding and context through open source, over which we will drape our* [secret intelligence] *… it doesn't change our reliance on partners for that secret insight, but it is going to mean that there's a much broader context of what we do.*[249]

GG. The Intelligence Community are right to recognise the difference in size and resources between the UK and US agencies, and to target their investments accordingly so as to ensure that the UK remains an essential partner for the US.

HH. Nevertheless, Ministers and the Intelligence Community must ensure that the UK retains sovereign intelligence capabilities to enable it to stand on its own two feet in intelligence terms, in the highly unlikely and undesirable event that there is a breakdown in the US partnership.

Challenges in the partnership

249. Despite the positive relationship between the UK and US intelligence communities, there can be differences in the legal and policy frameworks under which they operate, and how those are interpreted, as well as differences in the policies, law and values of their respective governments. As noted earlier in this Report, US policy on the treatment of

[247] Oral evidence – MI5, 17 June 2021.
[248] Oral evidence – DI, 10 June 2021.
[249] Oral evidence – DI, 10 June 2021.

detainees following the invasions of Afghanistan and Iraq caused serious difficulties in the partnership.

250. However, two other incidents have also risked strain in the relationship over the past decade.

Case study: Binyam Mohamed

Binyam Mohamed is an Ethiopian national and UK resident who was arrested in Pakistan in April 2002, having fled Afghanistan where he had been fighting with the Taliban. He was subsequently transferred to Guantánamo Bay by the US in September 2004. He alleged that he had been mistreated, including being tortured, and that UK intelligence officers had been complicit in this mistreatment. The Committee, in its 2007 report on *Rendition*, could confirm only part of this story, namely that he had been ultimately transferred to Guantánamo Bay, but at that time was unable to investigate allegations about mistreatment or further rendition as SIS did not provide the Committee with full evidence.[250]

In 2008, Mr Mohamed's lawyers made an application in the UK for disclosure under *Norwich Pharmacal* principles to compel the then Foreign Secretary to provide Mr Mohamed's lawyers with information and documents to support his account of what happened to him.[251] The Divisional Court ruled that the Foreign Secretary should disclose this material. The Foreign Secretary appealed and tried to prevent disclosure of this material on public interest grounds, stating that such publication would lead to a real risk of serious harm to the national security of the UK. The Court of Appeal rejected the Foreign Secretary's appeal and decided to include within its open judgment seven short sub-paragraphs relating to Mr Mohamed's treatment in detention.

However, the publication in the UK of US intelligence material – even at the direction of a court – was a clear breach of the 'control principle': put simply, the information was not the UK's to publish. ***.[252] ***.[253]

[250] *Rendition*, Cm 7171, July 2007.
[251] A *Norwich Pharmacal* Order (NPO) is a disclosure order which allows information to be obtained from third parties who have become 'mixed-up' in wrongdoing, helping victims to investigate and pursue those ultimately responsible. NPOs are often used where a victim of wrongdoing does not know the identity of the wrongdoer but can point to a third party who has this information.
[252] Written evidence – 10 July 2012.
[253] Written evidence – 10 July 2012.

The situation was rectified only by the Government undertaking to legislate to prevent a similar situation occurring again. This led to provisions in the Justice and Security Act 2013 prohibiting the Court from making a *Norwich Pharmacal* disclosure order where the information is 'sensitive information' which includes information held by an intelligence service, or obtained, or derived in whole or part, from an intelligence service. The Justice and Security Act 2013 also brought in provisions allowing HMG to apply for a 'closed material procedure' in civil cases enabling claims involving national security issues to be heard in closed sessions.

Case study: Edward Snowden

In June 2013, Edward Snowden, a National Security Agency (NSA) contractor, leaked tens of thousands of NSA and (allegedly) Five Eyes information to the UK and US media who alleged – incorrectly – that the NSA and GCHQ were illegally gathering bulk intelligence on US and UK respective citizens. One of the allegations centred on agreements the NSA held with US Communications Service Providers to receive bulk telephony Communications Data (including the dates of calls, their lengths, and the numbers involved), and a particular NSA programme – PRISM – which was an interception regime targeting foreign nationals and was authorised under the US Foreign Intelligence Surveillance Act.

***. In addition, there were allegations that GCHQ was receiving intelligence from the US on UK citizens without a warrant – thus circumventing the legal process. The Committee investigated the allegations but concluded that there was no evidence GCHQ had acted unlawfully (a proper warrant was in place in each case where GCHQ sought information from the US).

Despite the findings of the Committee, there was a significant media backlash over the activities of both the NSA and GCHQ. In addition, the disclosures had "*a significant impact on ... operations and capabilities*" and "*led to a severe dip in intelligence output*".[254] Nevertheless, the Committee was told that, while some working practices were changed, there is no record of any significant breakdown in trust between GCHQ and NSA over this issue.

251. The comparison of the Edward Snowden disclosures with the Binyam Mohamed case is striking – when the UK broke the norms of intelligence sharing, the relationship took a heavy blow; where the US was the source of a major, highly damaging leak of capabilities, the UK – rightly, in the Committee's view – did not break ranks with the US.

252. The Committee questioned the then Foreign Secretary about this difference in approach. The then Foreign Secretary told us:

[254] Written evidence – 18 October 2021.

> *in terms of what action we took* [after the Binyam Mohamed court disclosures]*, we looked at our own domestic safeguards, as well as looking as to what would go into the public domain … we did both of those things to protect the integrity of our operations as a domestic matter, in tune with our laws and our norms, and our moral judgments; but we also made sure that we preserved the integrity of the relationship with the US.*
>
> *I think Binyam Mohamed was a key moment, but we always have these issues … there will be shades of grey between* [UK and US] *opinions on this. The truth is* [that] *that pales into insignificance compared to the value of the overlap of interests and values that we have.*[255]

253. More reassuringly, GCHQ told the Committee that the recent differences in policy positions between the UK and US governments regarding the use of Huawei equipment in telecommunications infrastructure "*have had no impact on the scale and quality of intelligence co-operation with NSA*".[256] The Committee was told by GCHQ that "*whilst the policy differences raised some diplomatic challenges for the NCSC* [National Cyber Security Centre] *with their US counterparts*, *they did not cause any obstacles to our continuing close partnership*".[257]

II. As with any strong partnership, occasional – even serious – differences in policy are unavoidable. What matters is the response to such disagreements. In the Committee's view, the UK acting in solidarity with the US following the Snowden disclosures was – despite the damage caused to UK intelligence capabilities – the right approach. Strong partners stand together. In contrast, the US response to the Binyam Mohamed court disclosures was unfortunate. In a partnership such as that between the UK and US, both partners should be held to the same high standards and levels of mutual respect.

JJ. The Committee was, therefore, reassured to learn that recent policy differences over Huawei did not affect the intelligence relationship with the US. This is indicative of the maturity and seriousness with which both countries approach the partnership.

Broader issues – 'Big Tech', end-to-end encryption and data-sharing

254. A significant challenge facing the Intelligence Community and law enforcement organisations is the adoption of 'end-to-end' encryption by instant messaging and Communications Service Providers (CSPs) – and particularly by the so-called 'Big Tech' US companies such as Facebook, whose dominant market position makes them extremely influential.

255. Messages sent via an end-to-end encrypted service are viewable only by the sender and recipient; the company providing the service cannot view the content. While this has benefits from a privacy perspective, it also poses a significant national security risk: although some end-to-end encrypted systems could allow for exceptional access by the authorities –

[255] Oral evidence – Foreign Secretary, 22 July 2021.
[256] Written evidence – GCHQ, 20 November 2020.
[257] Written evidence – GCHQ, 20 November 2020.

subject to the granting of a legal warrant for the interception of the communication – many implementations of end-to-end encryption do not allow for this.

256. The UK Government's position is that "*it is technically possible for tech companies to implement an 'end-to-end' encrypted service whilst retaining the capability to provide data exceptionally in response to lawful warrants*";[258] however, the Committee has previously reported that technology companies have been unwilling to build such capabilities into their platforms. Debates over this issue have therefore become a feature of the UK diplomatic and security partnership with the US. Despite broad agreement at the political level – including, most recently, a joint commitment from President Biden and the Prime Minister in June 2021 to "*work together to maintain tightly-controlled lawful access to communications content that is vital to the investigation and prosecution of serious crimes including terrorism*" – at the time of taking evidence for this Report, it appeared that little tangible progress had been made.[259]

257. The Agencies are increasingly willing to speak out on the issue. In a public speech in 2021, Director General MI5 was unambiguous about the threat posed by technology companies' adoption of end-to-end encryption to MI5's ability to keep the public safe:

> *End-to-end encryption, done in the way Facebook is currently proposing, will hand a gift to the terrorists MI5 has to find and tackle – and a gift to the child abusers our colleagues in the National Crime Agency have to find and tackle. The CEO of WhatsApp … recently branded government objections to end-to-end encryption as "Orwellian", akin to demands that video cameras be placed in every living room … But that's not what we're asking for …*
>
> *I want to make a public plea to tech companies to engage seriously with governments … Encryption should not be falsely presented as* [a] *binary privacy or safety* [matter]*: the public needs the tech companies to find solutions which both maintain users' privacy and support everyone's safety*.[260]

258. Furthermore, the Committee was told that "*the irresponsible implementation of 'end-to-end' encryption *** will have a disastrous impact on public safety*".[261] In particular, in relation to counter-terrorism alone:

> [end-to-end encryption] *impacts on almost all of the 800 live Counter-Terrorism Policing investigations in the UK. Evidential thresholds mean that law enforcement can rarely arrest and prosecute someone, or safeguard a victim, without the evidence provided from messaging content; this content is being lost as a consequence of "end-to-end" encryption*.[262]

---

[258] Written evidence – Cabinet Office, 1 November 2021.
[259] 'Joint Statement on the Visit to the United Kingdom of the Honorable Joseph R. Biden, Jr., President of the United States of America at the invitation of the Rt Hon. Boris Johnson MP, the Prime Minister of the United Kingdom of Great Britain and Northern Ireland', GOV.UK, 10 June 2021.
[260] Annual Threat Update – Director General MI5, 14 July 2021.
[261] Written evidence – Cabinet Office, 1 November 2021.
[262] Written evidence – Cabinet Office, 1 November 2021.

259. The Home Office leads on engagement with technology companies on encryption. However, the Agencies *** have played an important supporting role, ***. The Committee was told that, "*on occasion,* [the Agencies'] *partnerships have ... been critical to securing the support of friendly governments towards HMG's wider efforts* [on encryption and other technology issues]".[263] The NCSC has also engaged directly with technology companies ***.[264]

260. Whilst the problem of end-to-end encryption is of overriding concern, it is essential that there are no legal obstacles to US technology companies sharing the information lawfully required by UK law enforcement. The ISC, in its 2014 *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, highlighted the fact that US CSPs could not be compelled to share information with UK authorities, and recommended that an agreed procedure for data sharing be established as a matter of priority. Therefore, the Committee welcomed the UK–US Data Access Agreement which was signed in October 2019.[265] The Committee was told that the Agreement "*will play a significant role in removing obstacles to accessing data from US tech companies for the purpose of preventing, detecting, investigating and prosecuting serious crime*".[266] It does so by providing US technology companies with the legal basis on which they can share data with UK authorities, and in doing so "*will result in data being returned for use in serious crime investigations far more quickly than is currently the case, reducing the time in many cases from years to days*".[267]

261. However, the Agreement has not, at the time of writing, entered into force.[268] This is a matter of some concern. The Committee asked the Home Office about prospects for the entry into force of the Agreement. We were told that the delays were ***, and were assured that "*both governments remain absolutely committed to realising the benefits of the Agreement*" and that "*significant effort is being invested to conclude* [negotiations] *as soon as possible*".[269] This includes direct engagement with senior US officials by a range of UK agencies, in support of Home Office efforts to persuade the US administration to enter the Agreement into force as soon as possible.[270]

262. The Committee was told that ***, and systems and processes have been updated in preparation for the Agreement entering into force.[271]

---

[263] Written evidence – Cabinet Office, 1 November 2021.

[264] Written evidence – Cabinet Office, 1 November 2021.

[265] The UK–US Data Access Agreement is the first agreement signed following the passing into law in 2018 of the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act). The CLOUD Act provides for the streamlining of information-sharing between US Communications Service Providers (CSPs) and foreign law enforcement agencies, subject to the conclusion of an appropriate agreement (such as the UK–US Data Access Agreement) governing this process.

[266] Written evidence – Cabinet Office, 1 November 2021.

[267] Written evidence – Home Office, 12 July 2021.

[268] The Agreement came into force on 3 October 2022, after we had completed our Report, but while we were still awaiting confirmation from the Prime Minister that it could be published.

[269] Written evidence – Home Office, 12 July 2021.

[270] ***

[271] Written evidence – Cabinet Office, 1 November 2021; ***

KK. The dominance of the US 'Big Tech' companies means that their actions are an increasingly important aspect of the partnership between the UK and the US. Both governments need to work together to engage with the companies to ensure a constructive dialogue.

LL. The UK–US Data Access Agreement is a positive development, and demonstrates what can be achieved when the UK and US governments work together to facilitate the work of law enforcement. While it is a matter of some concern that its implementation has been delayed, the Committee is reassured that a range of UK agencies – alongside other parts of the Government – have engaged with the issue at the highest levels within the US government.

MM. The current debate concerns end-to-end encryption, which is frequently presented as a matter of privacy versus security. This is a false dichotomy; it is not an either/or choice. It is technically possible for technology companies to implement end-to-end encryption in a responsible way which maintains privacy while still allowing lawful access to encrypted communications – and which, therefore, does not hand a gift to terrorists.

NN. It is unacceptable that technology companies have appeared to, hitherto, refuse to facilitate lawful access to encrypted communications; their irresponsible actions cannot continue to put lives at risk. If they will not address this issue proactively, the Government should explore international action with the US and others in order to compel them.

Australia, Canada and New Zealand

263. While the US is by some distance the most influential partner in the Five Eyes, due to its unparalleled capabilities and scale, the other three Five Eyes partners – Australia, Canada and New Zealand – are also exceptionally important intelligence partners for the UK in their own right.

Australia

Australia's principal intelligence agencies are the Australian Security Intelligence Organisation (ASIO), counterpart to MI5; the Australian Secret Intelligence Service (ASIS), equivalent to SIS; and the Australian Signals Directorate (ASD), with which GCHQ works.

DI's main counterparts are the Defence Intelligence Organisation and the Australian Geospatial-Intelligence Organisation (which now forms part of the Australian Defence Intelligence Group).

The Australian Office of National Intelligence performs an intelligence assessment function similar to the JIO, but also has a broader co-ordinating remit for the intelligence community.

264. ***. ***. MI5 has a "*** *thematic* *** *relationship*" with ASIO, "*based on common threats and modus operandi*".[272] In evidence to the Committee, MI5 explained that its co-operation with ASIO spans a wide range of subject matters:

> *I think at the moment … we have, as MI5, *** operational co-operation with Australia *** and* [where] *we can learn from the Australian experience; and some very specific *** where we've had real success working together and that has strengthened ***.*[273]

265. SIS considers ASIS to be "*one of the few allied services that are global and capable*".[274] The two agencies have a long shared history – *** – and this adds to the strength of the partnership.[275]

266. Australia is a particularly important partner with regard to SIS's work ***. Around *** of SIS's reporting *** is derived from Australian intelligence.[276] SIS has also reported to the Committee that Australia ***.[277] This is a measure of the deep trust that has been developed between SIS and its ASIS counterparts. More broadly, Australia performs an important burden-sharing role for SIS in ***.[278]

267. GCHQ has "*a long-standing and mature relationship*" with the ASD and shares "*common priorities*" – ***. It reported that co-operation on operations is "*longstanding and advanced*": Director GCHQ emphasised the "*very strong cultural and ethical and legal ties*" between GCHQ and the ASD, and noted that collaboration *** continues to deepen.[279] As with MI5 and SIS, GCHQ views the priority for the future of the partnership as being "*about joint work we can do ****".[280]

268. The CDI explained that recent changes to the structure of the Australian defence intelligence enterprise have laid the groundwork for increased collaboration:

> *the Australian change, over the last couple of years, of creating their Defence Intelligence Group, creating a three-star CDI* [Chief of Defence Intelligence]*, bringing the geospatial organisation together with their Defence Intelligence Organisation – a similar thing to DI although not the same scale or with the same breadth – has made them an easier partner to us to work with and has given them … increased focus.*[281]

269. DI considers Australia to be a highly capable partner, and also values highly Australia's ***. The CDI noted that "*** *being the … *** focus for them in their region means they have not just capacity, but they also have a range of insights which are perhaps different to those which we might deduce*".[282] Combined with the UK's own assessments and insight regarding ***, this leads to a richer mutual understanding of the situation.

---

[272] Written evidence – SIS, 7 May 2021.
[273] Oral evidence – MI5, 17 June 2021.
[274] Written evidence – SIS, 7 May 2021.
[275] Written evidence – SIS, 7 May 2021.
[276] Written evidence – SIS, 16 November 2021.
[277] Oral evidence – SIS, 15 October 2021.
[278] Written evidence – SIS, 7 May 2021.
[279] Written evidence – SIS, 7 May 2021; Oral evidence – GCHQ, 1 July 2021.
[280] Oral evidence – GCHQ, 1 July 2021.
[281] Oral evidence – DI, 10 June 2021.
[282] Oral evidence – DI, 10 June 2021.

270. The CDI also stressed the broader burden-sharing value of the Australian partnership, telling the Committee that DI can rely on the Australians to provide intelligence and expertise on a range of ***, thereby alleviating the need for DI to commit significant resources.[283] This works both ways: by way of example, the CDI explained that, when Australia was considering ***, DI "*prepared a bespoke set of intelligence products for the Australians to use in their briefings to their ministers*".[284]

Canada

Canada has two main intelligence services: the Canadian Security Intelligence Service (CSIS), which has a largely domestically focused national security remit – akin to MI5 – but which also has a limited international liaison function with stations overseas; and the Communications Security Establishment (CSE), the SIGINT agency and counterpart to GCHQ.

The Royal Canadian Mounted Police, Canada's federal police force, works alongside CSIS to investigate national security threats such as terrorism and espionage.

DI works with the Canadian Forces Intelligence Command (CFIC), which broadly mirrors the same activities as DI.

The Canadian Privy Council Office conducts intelligence assessments, but also has a broader co-ordination role which goes beyond the UK JIO's remit.

271. Canada was the third country to join the UKUSA intelligence-sharing Agreement (in 1948), and as such is one of the UK's oldest intelligence partners. The Committee was told that these links remain "*strong and trusting*".[285]

272. CSIS has a primarily domestic remit, and therefore works *** with MI5; and, while it does have a foreign liaison function which is in some respects similar to SIS's, its legal authorities place certain limits on its ability to gather intelligence overseas. Nonetheless, both MI5 and SIS have strong working relationships with CSIS – ***.[286]

273. The UK–Canadian intelligence partnership is mutually beneficial.[287] Some of Canada's capabilities – for instance, *** – are "*more advanced*" than the UK Intelligence Community's, and CSIS and CSE provide valuable reporting on a range of intelligence topics.[288]

274. From the evidence received during this Inquiry, it is apparent that GCHQ's partnership with its CSE counterparts – described as "*flourishing*" to the Committee – is particularly strong.[289] GCHQ noted in particular Canada's mature and leading role on cyber security within the Five Eyes:

[283] Oral evidence – DI, 10 June 2021.
[284] Oral evidence – DI, 10 June 2021.
[285] Written evidence – SIS, 7 July 2021.
[286] Written evidence – SIS, 7 July 2021.
[287] ***
[288] Written evidence – SIS, 7 July 2021.
[289] Written evidence – SIS, 7 July 2021.

> *Canada has been with us at the head of the pack on cyber security and our relationship on cyber security is extremely strong and deep. It's the deepest of the Five Eyes actually and they have pioneered some things that we are using, including how you monitor for threats across government, and similarly we've shared capability in the other direction. So I think Canada is really nimble and they're very focused on cyber security.*[290]

275. GCHQ also highlighted Canada's "*very good analytical understanding* ***" and the fact that, ***, Canada has become a "*world leader in* ***".[291]

276. DI reported that it finds the CFIC to be an effective interlocutor which is focused on adding value to the Five Eyes alliance rather than duplicating capabilities and analyses carried out by others.[292] The CDI explained that, ***: "*** *we gain enormous benefit as a consequence of that*".[293]

277. ***.[294]

New Zealand

The New Zealand Intelligence Community consists of the New Zealand Security Intelligence Service, which performs similar functions to both MI5 and SIS; the Government Communications Security Bureau, the New Zealand SIGINT agency with which GCHQ partners; and the National Assessments Bureau, which is similar to the JIO.

New Zealand Defence Intelligence, part of the New Zealand Defence Force, is DI's counterpart organisation.

278. In evidence to the Inquiry, ***; the Chief of SIS told the Committee that New Zealand is "*a deeply valued player and they make a very significant contribution*".[295]

279. GCHQ told the Committee that, while New Zealand are "*not large contributors to the SIGINT pool of data on which we all operate*", its unique capabilities provide benefit to the Five Eyes ***.[296]

280. MI5 also recognises New Zealand as a valuable partner and noted to the Committee that, following the 2019 Christchurch terrorist attack (the impact of which was amplified using the internet), "*New Zealand* [now] *punches way above its weight on preventing terrorist use of the internet*".[297]

---

[290] Oral evidence – GCHQ, 1 July 2021.
[291] Oral evidence – GCHQ, 1 July 2021.
[292] Oral evidence – DI, 31 January 2019.
[293] Oral evidence – DI, 31 January 2019; Oral evidence – DI, 10 June 2021.
[294] Written evidence – GCHQ, 3 August 2021; Written evidence – SIS, 23 November 2020; Written evidence – DI, 14 May 2021.
[295] Oral evidence – SIS, 27 May 2021.
[296] Oral evidence – GCHQ, 1 July 2021.
[297] Oral evidence – MI5, 20 May 2021.

281. ***.[298]

282. In April 2021, it was noted in press reporting that New Zealand had declined to join the other Five Eyes countries in issuing a public condemnation of the Chinese government's treatment of its Uighur minority population in Xinjiang province. Asked by the Committee whether New Zealand's commitment to the Five Eyes alliance was in question, the Chief of SIS said:

> *As an intelligence construct, Five Eyes carries on completely as it was …* ***.[299]

Director General MI5 similarly told the Committee that he did not consider the Five Eyes partnership to be at risk:

> ***.[300]

OO. While the Intelligence Community's partnerships with Australia, Canada and New Zealand are more limited in scale and ambition than those with the US, they are highly valuable, both individually and as a collective. Each offers unique capabilities and regional expertise which are of great benefit to the UK.

PP. The Intelligence Community should consider investing further in order to deepen these relationships *.**

Potential for expansion

283. While the membership of the Five Eyes alliance has not changed since 1956, there is nothing, in principle, to prevent another country being invited to join, with the agreement of the five current members. There is occasional press speculation to this effect, with Japan often considered the most likely candidate for joining the alliance.

284. However, the evidence taken by the Committee in this and previous Inquiries suggests that there is little prospect of expansion, at least in the medium term. The levels of mutual trust required by each partner to share its most sensitive and closely guarded secrets are such that the threshold for entry, which must inevitably be very high, may never be met by another country. This is a point that GCHQ acknowledged explicitly in evidence to the Inquiry: "*The barriers to another country joining the SIGINT element of the Five Eyes … remain formidable.*"[301]

285. The CDI also *** about the prospect of expanding the alliance:

> *the complexity of adding new members to what is a club which, as I said earlier, has got opportunities* [and] *obligations,* ***.[302]

[298] Written evidence – DI, 14 May 2021.
[299] Oral evidence – SIS, 27 May 2021.
[300] Oral evidence – MI5, 29 April 2021.
[301] Written evidence – GCHQ, 20 November 2021.
[302] Oral evidence – DI, 10 June 2021.

286. Commenting on the suggestion often made in the media that Japan might join the alliance, ***.[303]

287. The then Foreign Secretary explained to the Committee that increased UK security and defence engagement with *** should not be interpreted as a strategic shift away from the Five Eyes: "*what we do with ***, what we do with ***, what we do with* *** [is] *crucially important, but I don't think that will supplant Five Eyes or somehow displace the centrality of the Five Eyes partnership*".[304]

288. While a formal expansion of the alliance may be unlikely, in certain fields it engages with close allies ***.[305]

QQ. The Committee acknowledges that the level of trust necessary between members of the Five Eyes alliance creates a very high barrier to entry, and as a result the Intelligence Community are reticent about the prospect of expansion. It appears to the Committee that, at present, the risks of allowing another country to join the alliance far outweigh the benefits *.**

RR. The Intelligence Community should instead play a leading role in encouraging Five Eyes partners to engage collectively with other close allies in the 'Five Eyes-plus' concept, when this would provide operational benefits.

[303] ***

[304] Oral evidence – Foreign Secretary, 22 July 2021.

[305] Oral evidence – DI, 10 June 2021.

289. In 2014, Sir Iain Lobban, then Director GCHQ, spoke about the vital contribution made by French and Polish cryptographers, in the run-up to the Second World War, to British efforts to break the German Enigma code. In Sir Iain's view, the value of the partnership to the UK was hard to overstate:

> *the UK's SIGINT Agency was able to meet the challenge posed by German cryptography in WWII simply because France and Poland were prepared to share what they knew about Enigma*.[306]

290. The same could be said of the Intelligence Community's ability to meet many of their most pressing challenges today, and shared threats continue to underpin extensive European co-operation. In 2016, then Director General MI5 told the Committee: "*half of Europe is scared of terrorism and the other half is scared of Russia, and both halves want us to help them*".[307]

291. The European angle is particularly important to MI5, as almost every aspect of its domestic national security remit has a cross-border dimension, and events in one country can trigger attacks in neighbouring countries (for example, the UK National Terrorist Threat Level was raised in November 2020 from 'Substantial' to 'Severe' due to the potential for the attacks in France and Austria to have a galvanising effect on UK-based terrorists).[308] MI5's bilateral and multilateral European partnerships have grown in breadth and depth over the past five to ten years, and there is every indication that this trend will continue. The same is, to varying degrees, true of SIS, GCHQ and DI as well: European partnerships will remain central to their ability to carry out their respective functions. They each prioritise different partnerships and often take differing approaches towards co-operation (with, for instance, SIS having a clear preference for working bilaterally).

Avowed bilateral partnerships

292. The Intelligence Community do not unilaterally 'avow' their partnerships with foreign counterparts; to do so would be to breach the trust on which such relationships rely. However, in recent years, a small number of bilateral European partnerships have been jointly avowed.

293. In February 2018, the then Chief of SIS made a joint public statement with his French and German counterparts, emphasising the need for continued intelligence co-operation following the UK's departure from the EU.[309] Later that year, then Director General MI5 gave a public speech at the headquarters of MI5's German counterparts, which he described as "*a vital partner for MI5*".[310] MI5's website also declares its partnership with the Irish police service on national security issues.

---

[306] Speech given by Sir Iain Lobban KCMG CB, then Director GCHQ, in Warsaw on 3 July 2014.
[307] Oral evidence – MI5, 1 December 2016.
[308] Security Minister statement to the House of Commons on the UK Terrorism Threat Level, 5 November 2020; the Threat Level was reduced again to 'Substantial' on 4 February 2021.
[309] 'European spy chiefs in joint plea for post-Brexit co-operation', BBC News,16 February 2018.
[310] Speech given by Andrew Parker (now Lord Parker of Minsmere) to the *Bundesamt für Verfassungsschutz* Symposium in Berlin, 14 May 2018.

France

France has three main intelligence agencies: the *Direction Générale de la Sécurité Intérieure*, the domestic security service; the *Direction Générale de la Sécurité Extérieure*, which has a remit similar to SIS and GCHQ combined; and the *Direction du Renseignement Militaire*, the French military intelligence service.[311]

294. ***.[312]

Germany

Germany has two main Federal-level intelligence services with which the UK Intelligence Community work: the *Bundesamt für Verfassungsschutz* (Federal Office for the Protection of the Constitution), which is largely analogous to MI5; the *Bundesnachrichtendienst* (Federal Intelligence Service), which has a very broad remit and fulfils similar functions to SIS, GCHQ, DI and the JIO combined.

295. ***.[313]

The Republic of Ireland

MI5 works with the Irish police service, *An Garda Síochána* (often known as the 'Garda'), on national security matters. This partnership is conducted in close conjunction with the Police Service of Northern Ireland.

296. ***.[314]

Other bilateral partnerships

297. Clearly, the relationships with these three countries do not, by any means, represent the totality of the Intelligence Community's European partnerships. The Committee has taken evidence on the full range of European bilateral and multilateral partnerships during this Inquiry (and indeed previously – for example, in relation to its Russia and China Inquiries, given how closely the Intelligence Community must work with others to tackle state threats).

***.[315]

---

[311] The Committee noted the conclusion of the trilateral Australia–UK–US (AUKUS) security pact, and the subsequent press reporting regarding potential damage to the UK–France diplomatic relationship as a consequence of the cancelling of Australia's submarine deal with France. It has not been possible formally to consider this matter as part of this Inquiry; however, the Committee has not seen any evidence suggesting that AUKUS has had a negative impact on the UK–France intelligence partnership.

[312] ***

[313] ***; Speech given by Andrew Parker (now Lord Parker of Minsmere) to the *Bundesamt für Verfassungsschutz* Symposium in Berlin, 14 May 2018.

[314] ***

[315] ***

Multilateral intelligence fora

The Counter Terrorism Group

The Counter Terrorism Group (CTG) is an avowed group of 30 European domestic security and intelligence services which work together to counter the threat to Europe from Islamist terrorism.[316]

Established in 2001 following the September 11 attacks in the US, with a view to improving European security services' co-ordination on Islamist terrorism, CTG membership has expanded considerably as the EU has grown; however, EU membership is not a prerequisite for participation and the CTG exists outside of EU structures. ***.[317]

298. MI5 represents the UK Intelligence Community on the CTG and has played a leading role in driving the agenda for the Group throughout its existence. In 2018, then Director General MI5 spoke at some length about the benefits of the CTG in a public speech:

> [The CTG] *is the largest multinational CT* [counter-terrorism] *intelligence enterprise in the world, with thousands of exchanges on advanced secure networks every week.*
>
> *This multilateral co-operation doesn't look like frosty gatherings of strangers reading out national positions at each other. It looks like intelligence officers from 30 countries permanently co-located together as a joint operational platform. It looks like real-time intelligence sharing and agreeing joint tactics to combine each country's resources to best effect.*
>
> *It looks like professionals from all across Europe who know and trust each other working together and sharing data on shared systems about terrorist fighters dispersing from Syria. It looks like developing new ways to run and de-conflict human intelligence operations together. It looks like attacks thwarted and terrorists arrested who could not otherwise have been found in time by any one nation alone.*[318]

(i) Investigative co-operation

299. The "*joint operational platform*" referred to in the speech above is ***. According to MI5, the platform enables the "*streamlined sharing of investigative and operational information and exploitation of collective capabilities*" between different European intelligence agencies.[319]

300. We asked MI5 about the practical benefits of such a joint platform. The Committee was told: "*absolutely we get benefit from it: both direct operational benefit that comes from our ability to be able to share information more quickly and also the kinds of relationships*

[316] Despite its name, the CTG works primarily on Islamist extremism; ***.
[317] Written evidence – MI5, 23 November 2020.
[318] Speech given by Sir Andrew Parker (now Lord Parker of Minsmere) to the *Bundesamt für Verfassungsschutz* Symposium in Berlin, 14 May 2018.
[319] ***; Written evidence – MI5, 2 November 2020.

that you can build up if you work in very close proximity with your partners".[320] This is consistent with the other evidence the Committee has taken in the course of this Inquiry: that, even in a world of increasing interconnectivity, the continued importance of personal relationships to international partnerships is a running theme.

301. In the year to April 2021, MI5 made *** requests for information from European partners through the platform.[321] MI5 explained that, in addition to general co-operation on ongoing investigations, the platform was particularly useful for post-incident response: if one CTG member experiences an Islamist terrorist attack, it can immediately brief other CTG members through the platform, thereby facilitating a shared picture of the situation and allowing other members quickly *** to identify any information which may assist in the investigation.[322]

(ii) Data-sharing

302. In addition to the platform, CTG data-sharing on Islamist terrorist Subjects of Interest (SOIs) is a key benefit of the forum for MI5. This intelligence sharing *** allows terrorist SOI information to be shared across CTG members on a real-time or near real-time basis.

303. MI5 is a significant contributor of SOI data ***, alongside ***.[323] MI5 describes access to this data as "*a valuable tool for identifying potential connections between different individuals and networks which we may not otherwise have been sighted on*".[324]

304. ***.[325]

***.[326]

SS. Co-operation between European domestic intelligence services is clearly to be welcomed, and it is plain to the Committee that consistent engagement with the Counter Terrorism Group * is strongly in the UK's interest. We would also support any efforts to focus European partners' minds on Hostile State Activity – particularly the growing threat from China.**

TT. The Committee supports MI5's ambition for the Counter Terrorism Group *. However, more important overall is that MI5 continues to play a leading role, shaping priorities and operational focuses in the interest of the UK's national security.**

***.[327]

[320] Oral evidence – MI5, 17 June 2021.
[321] Oral evidence – MI5, 17 June 2021.
[322] Oral evidence – MI5, 17 June 2021.
[323] Written evidence – MI5, 23 November 2020.
[324] Written evidence – MI5, 23 November 2020.
[325] ***
[326] ***
[327] ***

NATO

The North Atlantic Treaty Organisation (NATO) remains a cornerstone of UK defence, security and foreign policy, and the 2021 Integrated Review of Security, Defence, Development and Foreign Policy reaffirmed the UK's commitment to the alliance. NATO has a dedicated intelligence function, and both NATO and the UK view intelligence as a key enabler in its security and deterrence objectives; the Integrated Review notes: "*Through NATO, we will ensure a united Western response* [to Russian aggression]*, combining our military, diplomatic and intelligence assets in support of collective security.*"[328]

305. DI plays the leading role within the UK Intelligence Community in terms of engagement with NATO on intelligence matters. The Chief of Defence Intelligence (CDI) attends the NATO Military Intelligence Committee (the NATO defence intelligence heads' forum for policy development and intelligence co-operation) and DI considers itself a "*net contributor*" to the alliance's intelligence efforts, "*both in terms of product but particularly in terms of thought leadership*".[329]

306. NATO has limited intelligence-collection capabilities of its own. It relies on member states to provide it with intelligence and assessments, which it then 'fuses' to produce NATO intelligence products. DI provides NATO with a range of all-source assessments (releasable to all NATO members), mostly as a by-product of material produced for UK customers. For example, in 2020, DI provided NATO policy-makers with an assessment of Russia's strategic nuclear strike capability – and NATO's ability to deter this – to help inform NATO policy.[330]

307. In addition to assessments, the UK sometimes collects intelligence on NATO's behalf; for example, UK Armed Forces collection platforms undertake periodic NATO intelligence-collection tasks against possible threats to NATO. Processed intelligence from this activity is then provided to NATO intelligence organisations.[331]

308. However, DI's relationship with NATO is not merely a passive one. DI told the Committee that it uses intelligence to help shape NATO policies towards, and understanding of, key strategic issues (as well as those of its members). ***.[332]

309. DI's co-operation with NATO takes place at a number of levels. At a strategic level, much of the co-operation is conducted through representatives at the UK Delegation to NATO (in Brussels) or through the UK's National Military Representative at Supreme Headquarters Allied Powers Europe (usually known as 'SHAPE', and located in Mons,

[328] *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*, HMG, March 2021; although NATO is not restricted in membership or remit to European defence and security, it is included in this section due to the significant overlap between its membership and that of the EU.
[329] Written evidence – DI, 14 May 2021; Oral evidence – DI, 10 June 2021.
[330] Written evidence – DI Quarterly Report, 1 July 2020 to 30 September 2020.
[331] Written evidence – DI, 3 November 2020.
[332] Oral evidence – DI, 13 December 2020; ***.

Belgium).[333] DI and other MoD personnel integrated throughout the NATO command structure and within NATO intelligence structures also provide access and co-operation.[334]

310. The Intelligence Community's engagement with NATO is not confined to DI: SIS contributes to the intelligence effort both in support of military operations and political decision making and to improve the effectiveness of the NATO Intelligence Enterprise; and GCHQ, in particular, has been increasingly active in its engagement with NATO on *** in recent years. GCHQ explained:

> *for the last four or five years, GCHQ has devoted a lot of effort to help NATO understand its vulnerabilities but also to focus more broadly on the resilience it needs on the platforms it's deploying … I think it's really important for the UK that we're projecting a leadership role around all of this*.[335]

311. This area of work is likely to increase in importance for the UK, and by extension GCHQ: NATO members have agreed that a cyber attack could trigger Article 5 of the NATO Treaty, and have designated cyberspace as a military domain (a development strongly advocated by the UK and supported by GCHQ).[336]

312. In terms of ***, GCHQ told the Committee ***, GCHQ's ambition is to help "*improve the overall levels of resilience and make sure that there are some* [***] *tools available for NATO to call upon*".[337]

UU. The Committee was greatly impressed with the breadth of DI's contribution and commitment to NATO. We also recognise GCHQ's increasingly important role in relation to NATO, given the ambition for the UK to be the leading cyber power in the alliance.

VV. The rest of the Intelligence Community should ensure they capitalise on the UK's influential position within NATO to share intelligence and assessments where appropriate, and to build consensus on key security issues.

Joint Expeditionary Force

The Joint Expeditionary Force (JEF) is a UK-led multinational high-readiness military task group of more than 10,000 personnel. Launched initially in 2014, the JEF consists of the UK (the 'framework nation') plus Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, the Netherlands, Norway and Sweden.[338] The JEF's primary objective is to contribute to Euro-Atlantic security, with a particular focus on the High North, North Atlantic and Baltic regions. It sits outside NATO structures, but is intended to complement NATO's deterrence efforts in northern Europe.

[333] Written evidence – DI, 3 November 2020.
[334] Written evidence – DI, 3 November 2020.
[335] Oral evidence – GCHQ, 1 July 2021.
[336] Written evidence – GCHQ, 20 November 2020.
[337] Oral evidence – GCHQ, 1 July 2021.
[338] Iceland joined the JEF in April 2021.

313. DI leads the JEF Intelligence Group, which is chaired by the Deputy Chief of Defence Intelligence.[339] DI told the Committee that this activity:

> *focuses mostly on collective capacity-building with the participating nations' defence intelligence organisations and sharing analyses on the threats the Force is most likely to encounter, particularly the Russian threat*.[340]

314. As well as being an important DI contribution to a broader MoD initiative with a practical military focus, the JEF partnerships (both bilateral and multilateral) also enable DI to obtain strategic intelligence to which it might not otherwise have access. ***.[341]

WW. Although it is a less mature partnership and more modest in scope and ambition than the NATO intelligence partnership, DI's position as the framework nation for the Joint Expeditionary Force (JEF) Intelligence Group – and the consequent access this provides to new streams of intelligence – shows the value of seeking a leadership role in multilateral intelligence organisations. DI should continue to look for further opportunities to capitalise on the JEF construct to build stronger bilateral partnerships with its individual members.

Multilateral intelligence fora: the balance of opportunity and risk

315. All international partnerships – diplomatic, military and economic – present both opportunities and risk. Intelligence partnerships involve the same dynamic, although the risks are arguably more acute as the stakes are higher. The UK Intelligence Community have to balance the benefits of sharing intelligence with the risk that intelligence will fall into the wrong hands, potentially putting lives or valuable capabilities at risk. This risk is perhaps accentuated in the case of large multilateral organisations such as NATO. For example, although many NATO countries individually have highly sophisticated intelligence services and armed forces which are capable of protecting information, the challenge of sharing intelligence through NATO structures (as opposed to bilaterally) is that there only needs to be one 'weak link' in the 30 NATO members for that information to be compromised. In the case of NATO, it is also a significant espionage target in its own right; the Committee has been told that NATO, together with the US, would be Russia's highest intelligence priorities.[342]

316. Asked about how DI approaches this issue, the CDI acknowledged that the size of NATO sometimes posed challenges to security when sharing intelligence:

> **** you need to be cognisant over what you give and where that information might go, either by accident or by design*.[343]

317. As a result, the information shared by DI through NATO structures is generally of a lower sensitivity ***. It is mostly composed of intelligence assessments based on a variety

[339] Oral evidence – DI, 31 January 2018.
[340] Written evidence – DI 3 November 2020.
[341] Oral evidence – DI, 31 January 2018; Oral evidence – DI, 10 June 2021.
[342] *Russia*, HC 632, 21 July 2020.
[343] Oral evidence – DI, 10 June 2021.

of sources, rather than single-source intelligence which – if compromised – might put sources or collection methods at risk. Intelligence assessments can be 'sanitised' to disguise the source of the information, thereby allowing them to be shared at a lower classification with allies ***. DI emphasised that, while this process could be time-consuming, "*it's really important that we get it right in order to make the most of our international partnerships and* [to share] *as much as we can whilst managing the risk*".[344]

318. This challenge extends to the other key multilateral European groupings in which the Intelligence Community participate. For instance, ***.[345]

319. MI5 explained to the Committee why it puts security of information at the heart of its interactions with allies:

> *there is not in my experience a willingness to … turn a blind eye to some* [partner intelligence] *service being insecure … we owe to our staff and to our agents, and ultimately to the public, the secrecy of what we do and we take a very dim view of any sort of frailties*.[346]

Brexit and the European Union

Implications for intelligence sharing

320. As with many other areas of co-operation with European partners, the UK's departure from the European Union (EU) has also provided the political context for intelligence partnerships over the past five years. The sharing of secret intelligence – as opposed to policing and other law enforcement data – is not an EU competence and, as such, has always been conducted largely outside of EU structures. Instead, intelligence sharing and co-operation have been carried out bilaterally, or through non-EU European fora such as the CTG ***.

321. The direct impact on intelligence sharing of the UK leaving the EU was, therefore, always likely to be very limited: the (mostly) bilateral mechanisms by which intelligence is shared were unaffected by Brexit. None of the witnesses to this Inquiry felt that the UK's departure was likely to have any material bearing on their ability to share secret intelligence with EU partners:

- Director General MI5 stressed this point to the Committee: "*national security was always a member-state competence, and so the effect of EU exit has not been directly profound in MI5's operating domain*".[347]
- The Chief of SIS also emphasised his Agency's preference for sharing intelligence on a bilateral basis: "*we're a very sovereign asset and most of what we do is bilateral. I mean, with CT* [counter-terrorism] *work, we might go trilateral or sometimes quadrilateral, but we're creaking when we do. Bilateral is the way we do business.*"[348]

[344] Oral evidence – DI, 10 June 2021.
[345] ***
[346] Oral evidence – MI5, 17 June 2021.
[347] Oral evidence – MI5, 29 April 2021.
[348] Oral evidence – SIS, 27 May 2021.

- GCHQ evidence stated that: "*The UK's withdrawal from the EU does not directly affect the nature of* [GCHQ's bilateral and multilateral European] *relationships, which have developed over decades. We have made significant efforts to ensure that those relationships remain strong.*"[349]
- DI evidence likewise stated that: "*The UK's departure from the EU does not raise significant issues for DI. Most of DI's European intelligence co-operation is conducted either through the vehicle of NATO or bilaterally with key European partners. This will not change as a result of Brexit. DI is not dependent on the EU as a provider of intelligence.*"[350]

322. Nevertheless, the Intelligence Community do still share intelligence directly with EU institutions. Prior to Brexit, the Intelligence Community maintained close working relationships with the main EU intelligence structures ***. While the Intelligence Community no longer *** they continue to provide assessed intelligence directly to the EU. The CDI explained:

> *the information we share with the EU is usually and almost exclusively the same information that we would share with NATO … there are EU members that are not part of NATO, and this is another way of getting information into the hands of those non-NATO nations*.[351]

323. This is viewed as an essentially cost-free way of maintaining links and influence with *** close military allies (***): "*I think actually it's an easy win for me in terms of maintaining some of those broader *** relationships.*"[352]

Co-operation with European partners

324. As noted above, intelligence sharing is not an EU competence and it has always taken place outside EU structures. However, while the mechanisms for sharing intelligence are unaffected, there was – and remains – a risk that the cooling of the diplomatic relationship between the UK and the EU could have an effect on day-to-day co-operation between the Intelligence Community and their partners. MI5 told the Committee:

> *I would say we are *** same level of trust and standing* [with European partners], *** *the wider context has shifted a bit, ****.[353]

325. MI5's evidence to the Inquiry suggested *** co-operation has continued to be good *** post-Brexit: "*** *European partners have been very keen to continue working with MI5, recognising our expertise and contribution to European security*".[354] The Committee was told that: ***.[355] Overall, Director General MI5 remains confident of good co-operation with EU partners:

---

[349] Written evidence – GCHQ, 20 November 2020.
[350] Written evidence – DI, 2 November 2020.
[351] Oral evidence – DI, 10 June 2021.
[352] Oral evidence – DI, 10 June 2021.
[353] Oral evidence – MI5, 17 June 2021.
[354] Written evidence – MI5 Quarterly Report, 1 October 2020 to 31 December 2020.
[355] Written evidence – MI5 Quarterly Report, 1 October 2020 to 31 December 2020.

> *I don't think* [Brexit] *has led to a material diminution in the UK's standing* [in terms of intelligence co-operation] *and *** the position remains very strong*.

326. Giving evidence to this Inquiry, the Heads of the other Agencies were also keen to stress to the Committee that Brexit had not had an effect on intelligence co-operation with EU member states:

- The Chief of SIS told the Committee: "*I can honestly put my hand on my heart and say it hasn't made any difference to us post-Brexit … heads of EU* [intelligence] *services have made a point of lining up and saying to me that they are determined to maintain the relationship*."[356]
- Director GCHQ explained: "*We're doing more with European countries now than we were at the point of referendum.*"[357]

327. This lack of impact is largely down both to the fact that their activities and co-operation with European counterparts has always taken place outside EU structures, and that, at the non-political level, national security has tended to transcend and be unaffected by disagreements on other matters.

XX. Overall, the Committee is reassured that Brexit has not had a negative impact on intelligence co-operation between the UK and EU member states. The Agencies must invest time to reassure their counterparts of the UK's continuing commitment to European security, and update us on any impact this has on resources.

Access to European Union data

328. Although the mechanisms for exchanging secret intelligence with EU partners were unaffected by Brexit, concerns were raised before and after the EU referendum about the implications of a potential reduction in co-operation with EU member states on law-enforcement investigations, including those relating to national security. For example, speaking in March 2020 as Brexit negotiations were ongoing (and with specific reference to the UK's departure from Europol), former Director General MI5, Lord Evans of Weardale, stated that "*it is unlikely we will be in as advantageous a position in terms of law enforcement co-operation as when we were* [EU] *members. The net effect will be a less effective response.*"[358]

329. One particularly important aspect of modern *** investigations is the free flow of law-enforcement-related information with foreign partners; for example, a swift notification that a potential terrorist has crossed a border, or is on a particular flight, can make a difference when seeking to thwart an attack. This means that access to partners' data is particularly important for *** close partnerships with police and other law-enforcement agencies, both in the UK and overseas.

---

[356] Oral evidence – SIS, 27 May 2021.
[357] Oral evidence – GCHQ, 1 July 2021.
[358] Combating Terrorism Center at West Point, 'A View from the CT Foxhole: Jonathan Evans, Former Director General, MI5', *CTC Sentinel*, Volume 13, Issue 3 (March 2020).

330. The UK's post-Brexit relationship with the EU on law-enforcement matters – including mutual access to law-enforcement data – is set out in the UK–EU Trade and Cooperation Agreement. The Agreement, concluded on 24 December 2020 and implemented on 31 December 2020, covers a wide range of matters (most notably, in the public and political discourse, trade), with one part dealing with law enforcement and criminal justice co-operation. ***.

331. The Agencies appear, broadly speaking, to be satisfied with the outcome of the negotiations. Director General MI5 told us: "*The Trade and Co-operation Agreement secured really important continuation of tools and measures* ***."[359] However, that is not to say that leaving the EU has had no impact ***. The Director General told the Committee, with reference to UK *** access to EU data and systems, "*there have been some shifts* [in UK access following the negotiations]*, for most of which we have adequate mitigations* ***".[360]

332. We questioned MI5 on the nature of these changes and how they were responding to them. One significant consequence of the Trade and Cooperation Agreement is that the UK is no longer a party to the Schengen Information System (known as 'SIS II'), a real-time EU travel alert system to which the UK had access for policing and law-enforcement purposes from April 2015. In written evidence to the Committee, provided in November 2020 prior to the conclusion of the negotiations, ***.

333. ***.[361]

334. A potential loss of access to EU Passenger Names Record (PNR) data was also flagged to the Committee in November 2020 as a risk ***.[362] PNR provides flight manifest and booking data for individuals travelling in and out of the UK, and as such is an important tool in *** police investigations.

335. The arrangements that have subsequently been agreed with the EU have given the UK similar access to this data as it had as a member state. ***.[363]

336. The Committee also questioned MI5 about the implications of a potential negative outcome in the then-ongoing negotiations regarding 'data adequacy' – a status granted by the European Commission to third countries outside the European Economic Area (EEA) which provide a level of personal data protection comparable to that provided for in European law.[364]

337. In written evidence to the Committee, provided before the conclusion of the negotiations, MI5 stated that "*achieving adequacy is important but not essential to UK national security*". MI5 was confident that it had sufficient measures *** to "*reduce the*

[359] Oral evidence – MI5, 17 June 2021.
[360] Oral evidence – MI5, 29 April 2021.
[361] ***
[362] ***
[363] ***
[364] The practical effect of a data adequacy agreement is that personal data can flow from the EEA to the third country without further safeguards being necessary.

impact of a 'no adequacy' scenario to a satisfactory level".[365] Nonetheless, the Director General told the Committee that "*the successful conclusion of the data adequacy negotiation clearly matters* ***".[366] ***.[367]

338. On 28 June 2021, the EU formally adopted adequacy decisions recognising the UK's post-EU data protection standards. This formal recognition of the UK's data protection standards effectively preserved the status quo regarding this element of UK–EU relations (the UK Government having already made the equivalent decision with regard to EU data). The 'no adequacy' scenario has not therefore come to pass for the time being. The arrangement is, however, subject to a four-year 'sunset clause', and the EU may choose not to renew the deal at that stage.

***.

Implications of Brexit for Northern Ireland-related terrorism

339. In October 2019, MI5 judged that: "*Whatever form EU Exit takes,* ***."[368] While this assessment may yet prove correct, *** in the overall threat from Northern Ireland-related terrorism (NIRT) ***: MI5 told the Committee in June 2021 that "*it is factually the case that* *** *as a consequence of EU Exit*".[369]

340. Nevertheless, there *** that the manner in which Brexit is implemented could have a material impact on the security situation in Northern Ireland. *** MI5 considers its operations and capabilities to have been broadly unaffected by Brexit; Director General MI5 told the Committee that ***.[370]

341. In June 2019, the Committee had questioned MI5 in detail on the potential impact of Brexit on NIRT. At that time, the focus was on the potential for new infrastructure at the border between north and south to increase the security risk. MI5 stated: ***.[371] Although we now know that new infrastructure at the north–south border has not been necessary, in November 2020 MI5 still judged that ***.[372]

342. Since the conclusion of the transition period, it has been the implementation of the Northern Ireland Protocol, rather than border infrastructure, that has been the focus of attention with regard to the security situation in Northern Ireland.[373] When there was a

[365] Written evidence – MI5, 23 November 2020.
[366] Oral evidence – MI5, 29 April 2021.
[367] ***
[368] Written evidence – MI5 Quarterly Report, 1 July 2019 to 30 September 2019.
[369] Oral evidence – MI5, 17 June 2021.
[370] Oral evidence – MI5, 29 April 2021.
[371] Oral evidence – MI5, 6 June 2019.
[372] Written evidence – MI5, 23 November 2020.
[373] The Withdrawal Agreement, a treaty between the UK and EU which set out the terms under which the UK left the EU, provided for a transition period from the UK's formal departure on 31 January 2020 until 31 December 2020, during which time the UK remained in the EU Single Market. After this point, the Northern Ireland Protocol – agreed as part of the Withdrawal Agreement – came into force. Its primary purpose was to avoid the need for customs and other checks on the land border between the UK and the Republic of Ireland. Under the current terms of the Protocol, this is achieved by Northern Ireland continuing to follow EU customs and certain other rules, with checks on goods instead conducted on the sea border between Northern Ireland and Great Britain.

significant increase in unrest in Loyalist communities in March and April 2021, leading to violent disorder and clashes with the police and (to a much more limited extent) with Republican communities, much of the public commentary focused on whether this was related to the ongoing challenges of implementing the Protocol, and therefore a consequence of Brexit. We asked Director General MI5 for his assessment. He told the Committee:

> ***.[374]

343. Changes to the political status quo in Northern Ireland have previously been identified by MI5 as a potential risk from a national security perspective. Speaking to the Committee in 2019, Director General MI5 said that if the:

> *arrangements between Northern Ireland and the UK mainland were to change in any way, shape or form* ***.[375]

344. ***, as at June 2021, MI5 *** that recent tensions in Loyalist communities ***.[376]

YY. It appears that Brexit has not led to a noticeable increase in terrorist attacks, and this is greatly to be welcomed. However, there is no room for complacency, and it is incumbent on political leaders on all sides of the debate in Belfast, Westminster, Dublin and Brussels to take full account of the unique security conditions in Northern Ireland and ensure that the inevitable practical consequences of Brexit for Northern Ireland – in particular the implementation of the Northern Ireland Protocol – are managed in such a way that they do not have a negative impact on the security situation.

[374] Oral evidence – MI5, 17 June 2021.
[375] Oral evidence – MI5, 6 June 2019.
[376] Written evidence – MI5, 2 June 2021.

ANNEX A: FULL LIST OF CONCLUSIONS AND RECOMMENDATIONS

A. Even within a well-integrated intelligence community such as that in the UK, varying operational imperatives mean it is inevitable that there will be differences of strategy between organisations when it comes to their international partnerships. This should not be problematic provided there is effective co-ordination between the different organisations engaging with foreign partners.

B. In the Committee's view, MI5, GCHQ and DI each have overarching strategies appropriate to their distinct functions and operational priorities. While we recognise that SIS's tasking via the Intelligence Outcomes Prioritisation helps give focus and direction to its many important international partnerships, we were surprised that SIS does not have a single overarching strategy for managing these, even at a high level. The Committee recommends that SIS follow the lead of GCHQ – which receives its tasking via the same process – and develop a standalone international partnerships strategy.

C. It is important that co-ordination between all three Agencies and DI remains strong. In particular, care should be taken that MI5 and DI, which are not tasked through the Intelligence Outcomes Prioritisation process, are nonetheless aligned with SIS and GCHQ where this is appropriate, and that the Agencies take care to read across to DI's strategy, which is derived from the Ministry of Defence's broader strategies and plans.

D. The introduction of the Fusion Doctrine in 2018 saw policy departments across the Government brought into national security work. There is therefore also a need for the three Agencies and DI now to co-ordinate their engagement with foreign partners with policy departments' own international strategies.

E. The Committee is satisfied that arrangements for ministerial engagement with the Intelligence Community's international partnerships are mature and proportionate.

F. While most interaction with foreign liaison partners is best carried out between intelligence professionals, the Intelligence Community should continue to be alive to opportunities for Ministers to engage with foreign counterparts on intelligence matters where this is appropriate. In addition, it may be beneficial for the Home Secretary to receive submissions on MI5 and SIS/GCHQ joint activity with foreign partners in parallel with the Foreign Secretary rather than simply receiving a copy for information afterwards.

G. The Committee was satisfied that instant messaging applications are not used for the exchange of classified information with foreign counterparts. Nonetheless, it is essential that audit trails are maintained of diplomatic exchanges that are made using these means – not least so that retrospective oversight can be applied by Parliament should this be required.

H. The SIS global network of stations overseas is a vital enabler for the work of the Intelligence Community, including the maintenance of international partnerships. While the Committee recognises that financial pressures will always require decisions to be made on the value for money provided by each station, SIS should maintain a general ambition to grow, rather than consolidate, its global footprint.

I. The Committee is supportive of the Intelligence Community's capacity-building efforts. However, working with some partners carries inherent risk, and the Agencies must continue to take great care about what capabilities they choose to share with which countries and to ensure robust safeguards are put in place (including the ability to withdraw if this becomes necessary).

J. Intelligence diplomacy is an important aspect of modern international intelligence partnerships. * partnerships can be utilised in the national interest when co-ordinated with the Government's other levers of international influence. Ministers and policy departments should continue to be alive to the Intelligence Community's ability to have a tangible influence on broader diplomatic objectives.**

K. The UK's overseas collection facilities are indispensable in terms of the contribution they make to the UK's national security, and the Intelligence Community should continue to exploit them for intelligence gain. Ministers should also ensure that broader government policy – * – fully takes into account such intelligence considerations.**

L. It is clear to the Committee that the UK's relative strength across a broad range of intelligence disciplines and subject matters makes it a partner of choice for many countries. The Intelligence Community should continue to foster this reputation – which, like all reputations, is hard won and easily lost.

M. The Committee fully supports the positive approach the Intelligence Community take towards intelligence partnerships, seeking actively to develop them beyond the merely transactional. Making full use of the UK's relative strength in intelligence terms to build effective partnerships is an effective use of resources that can help keep the UK safe in times of crisis. Ministers and senior officials should resist the temptation to take a less proactive approach in this area in the interest of economy; where the Intelligence Community can work with partner nations they should – subject to the necessary legal, ethical and security considerations.

N. The evidence we have received reassures us that, wherever possible, appropriate due diligence is carried out to ensure that information is not obtained via prohibited methods. However, we note that that cannot be guaranteed.

O. Most countries – even our closest allies – will operate under different legal and ethical constraints to the UK. However, to protect the UK we have no choice but to work with other countries. The framework under which our Agencies engage is therefore of the utmost importance.

P. The UK's legal and compliance framework governing engagement in international partnerships is comprehensive. The importance of adhering to legal obligations seems to be clearly understood and to have been embedded into the operational culture and decision making of the Agencies. The Committee is pleased to see this cultural change.

Q. There must be no complacency. The history of the Agencies' work with partners on detainee issues has been problematic – at best. It is clear that lessons have been learnt, but it is vital that the Agencies continue to adhere to, and build upon, robust oversight arrangements when working with foreign partners on detainee matters.

R. Law and compliance should be an inherent part of operational teams, not just part of the operational process. The Agencies should consider having embedded legal and compliance teams within operational missions, and particularly in overseas hubs where detainee work with partners is central. This would help to strengthen the compliance framework and provide on-hand expertise when needed.

S. Agency policy underpinning The Principles and the Overseas Security and Justice Assistance guidance appears to be respecting both the letter and spirit of the framework – as was clear both from the evidence taken as part of this Inquiry and when considering the most recently published report from the Investigatory Powers Commissioner's Office, who oversees much of the day-to-day activity of the Agencies.

T. The Principles appear to be working well, and are well integrated into Agency processes. While the Committee is still concerned that the Foreign Secretary is given significant discretion to authorise activity that may carry a real risk, we are broadly satisfied that, with the additional oversight of the Investigatory Powers Commissioner's Office, there are sufficient checks and balances in the system.

U. The Committee recognises that assurances are a necessary and important part of dealings with partners who do not necessarily share all of our values or legal frameworks. These appear to be sought and agreed effectively. We would encourage the Agencies to assign more effort where possible to the continued assessment of assurances, given that they are fundamental to the Agencies' ability to operate in certain areas.

V. The Agencies and Ministry of Defence must maintain a comprehensive written record of assurances sought and received. The Committee was impressed by MI5's Liaison with Overseas Security and Intelligence Agencies (LOSIA) form, which considers comprehensively the different elements of working with partners on detainee issues. We recommend that the Agencies introduce a single streamlined document based on LOSIA, so that recording of activity and assurances is done in a consistent way.

W. Given the need to work with some partners who engage in unacceptable treatment of detainees, the Committee is supportive of the Agencies' ability to carve out compliant pathways to enable them to work with states on a bespoke basis. This does not excuse or imply approval of unacceptable behaviour more generally, and the Agencies must do everything possible to manage and reduce risk when working in this area.

X. We welcome the introduction of the 'last pair of hands' principle, which ensures that there is a clear risk owner for all operational stages when working with a foreign liaison partner.

Y. The creation of PURPLE is a positive development for the UK Intelligence Community as a whole, and the Committee welcomes the work it has done. The tri-Agency nature of the team ensures consistency of approach across all three Agencies.

Z. The Prime Minister should provide this Committee with a full copy of the Confidential Annex to the Annual Report of the Investigatory Powers Commissioner 2019. The approach being taken by the Deputy National Security Adviser to redact operations that were 'current' in 2019 as if they were current today was severely misguided at best. When the Prime Minister determines the final outcome – in conjunction with the ISC, as set out in the Memorandum of Understanding – we trust that he will follow the spirit of the Justice and Security Act 2013 and the commitments given to Parliament during the passage of that legislation.

AA. The Committee is satisfied that, on balance, the serious risks of engaging with authoritarian and oppressive regimes are well understood by UK intelligence Agencies.

BB. The Agencies appear to take seriously the ethical dimension of their work. The Committee is pleased to learn of the staff counsellor to support officers, as well as several examples of how the organisations as a whole discuss and reflect on their more difficult partnerships. The Committee is satisfied that there is a genuine recognition of the broader impact of these relationships and the need for continued monitoring of their appropriateness.

CC. The Committee is pleased to see that its recommendation relating to joint units has finally been taken on board and that engagement with such units is now explicitly covered by The Principles. However, it is disappointing that HMG took nearly seven years to amend its policy. This is an unacceptable delay given the gravity of the compliance risks and volume of joint work undertaken by SIS.

DD. The Five Eyes alliance is a remarkable testament to the power of international partnerships to increase the reach, influence and capability of the parties concerned such that the whole amounts to more than the sum of its parts.

EE. Providing access to intelligence and capabilities far beyond that which the UK Intelligence Community alone can obtain, and facilitating burden-sharing for intelligence collection and analysis in a way that allows the respective members to develop greater expertise and coverage, the Five Eyes alliance is a truly exceptional arrangement that is wholly in the UK's interest. Maintaining and reinforcing the Five Eyes alliance, and the UK's place within it, should be the Intelligence Community's highest priority in relation to international partnerships.

FF. The UK's intelligence partnership with the US is of a breadth and depth without parallel anywhere else in the world. It is the envy of our allies and adversaries alike. In particular, the partnership between GCHQ and the National Security Agency represents, perhaps, the pinnacle of intelligence co-operation; it is a testament to the ambition and commitment of generations of intelligence personnel on both sides of the Atlantic. Long may it continue.

GG. The Intelligence Community are right to recognise the difference in size and resources between the UK and US agencies, and to target their investments accordingly so as to ensure that the UK remains an essential partner for the US.

HH. Nevertheless, Ministers and the Intelligence Community must ensure that the UK retains sovereign intelligence capabilities to enable it to stand on its own two feet in intelligence terms, in the highly unlikely and undesirable event that there is a breakdown in the US partnership.

II. As with any strong partnership, occasional – even serious – differences in policy are unavoidable. What matters is the response to such disagreements. In the Committee's view, the UK acting in solidarity with the US following the Snowden disclosures was – despite the damage caused to UK intelligence capabilities – the right approach. Strong partners stand together. In contrast, the US response to the Binyam Mohamed court disclosures was unfortunate. In a partnership such as that between the UK and US, both partners should be held to the same high standards and levels of mutual respect.

JJ. The Committee was, therefore, reassured to learn that recent policy differences over Huawei did not affect the intelligence relationship with the US. This is indicative of the maturity and seriousness with which both countries approach the partnership.

KK. The dominance of the US 'Big Tech' companies means that their actions are an increasingly important aspect of the partnership between the UK and the US. Both governments need to work together to engage with the companies to ensure a constructive dialogue.

LL. The UK–US Data Access Agreement is a positive development, and demonstrates what can be achieved when the UK and US governments work together to facilitate the work of law enforcement. While it is a matter of some concern that its implementation has been delayed, the Committee is reassured that a range of UK agencies – alongside other parts of the Government – have engaged with the issue at the highest levels within the US government.

MM. The current debate concerns end-to-end encryption, which is frequently presented as a matter of privacy versus security. This is a false dichotomy; it is not an either/or choice. It is technically possible for technology companies to implement end-to-end encryption in a responsible way which maintains privacy while still allowing lawful access to encrypted communications – and which, therefore, does not hand a gift to terrorists.

NN. It is unacceptable that technology companies have appeared to, hitherto, refuse to facilitate lawful access to encrypted communications; their irresponsible actions cannot continue to put lives at risk. If they will not address this issue proactively, the Government should explore international action with the US and others in order to compel them.

OO. While the Intelligence Community's partnerships with Australia, Canada and New Zealand are more limited in scale and ambition than those with the US, they are highly valuable, both individually and as a collective. Each offers unique capabilities and regional expertise which are of great benefit to the UK.

PP. The Intelligence Community should consider investing further in order to deepen these relationships *.**

QQ. The Committee acknowledges that the level of trust necessary between members of the Five Eyes alliance creates a very high barrier to entry, and as a result the Intelligence Community are reticent about the prospect of expansion. It appears to the Committee that, at present, the risks of allowing another country to join the alliance far outweigh the benefits *.**

RR. The Intelligence Community should instead play a leading role in encouraging Five Eyes partners to engage collectively with other close allies in the 'Five Eyes-plus' concept, when this would provide operational benefits.

SS. Co-operation between European domestic intelligence services is clearly to be welcomed, and it is plain to the Committee that consistent engagement with the Counter Terrorism Group * is strongly in the UK's interest. We would also support any efforts to focus European partners' minds on Hostile State Activity – particularly the growing threat from China.**

TT. The Committee supports MI5's ambition for the Counter Terrorism Group *. However, more important overall is that MI5 continues to play a leading role, shaping priorities and operational focuses in the interest of the UK's national security.**

UU. The Committee was greatly impressed with the breadth of DI's contribution and commitment to NATO. We also recognise GCHQ's increasingly important role in relation to NATO, given the ambition for the UK to be the leading cyber power in the alliance.

VV. The rest of the Intelligence Community should ensure they capitalise on the UK's influential position within NATO to share intelligence and assessments where appropriate, and to build consensus on key security issues.

WW. Although it is a less mature partnership and more modest in scope and ambition than the NATO intelligence partnership, DI's position as the framework nation for the Joint Expeditionary Force (JEF) Intelligence Group – and the consequent access this provides to new streams of intelligence – shows the value of seeking a leadership role in multilateral intelligence organisations. DI should continue to look for further opportunities to capitalise on the JEF construct to build stronger bilateral partnerships with its individual members.

XX. Overall, the Committee is reassured that Brexit has not had a negative impact on intelligence co-operation between the UK and EU member states. The Agencies must invest time to reassure their counterparts of the UK's continuing commitment to European security, and update us on any impact this has on resources.

YY. It appears that Brexit has not led to a noticeable increase in terrorist attacks, and this is greatly to be welcomed. However, there is no room for complacency, and it is incumbent on political leaders on all sides of the debate in Belfast, Westminster, Dublin and Brussels to take full account of the unique security conditions in Northern Ireland and ensure that the inevitable practical consequences of Brexit for Northern Ireland – in particular the implementation of the Northern Ireland Protocol – are managed in such a way that they do not have a negative impact on the security situation.

ANNEX B: LIST OF WITNESSES

Ministers

The Rt Hon. Dominic Raab MP – then Foreign Secretary

Officials

SECURITY SERVICE (MI5)

Mr Ken McCallum – Director General, MI5

Other officials

SECRET INTELLIGENCE SERVICE (MI6)

Sir Richard Moore KCMG – Chief, SIS

Other officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS (GCHQ)

Sir Jeremy Fleming KCMG CB – then Director, GCHQ

Other officials

DEFENCE INTELLIGENCE (DI)

General Sir James Hockenhull KBE ADC Gen – then Chief of Defence Intelligence

Other officials

ANNEX C: FOREIGN LIAISON PARTNER PROFILE AND CASE STUDY

***[377]

[377] ***

ISBN 978-1-5286-4400-6
E02961539