Intelligence and Security Committee of Parliament

Russia

HC 632

Intelligence and Security Committee of Parliament

Russia

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

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

HC 632

© Intelligence and Security Committee of Parliament copyright 2020

The material must be acknowledged as Intelligence and Security Committee of Parliament copyright and the document title specified. Where third party material has been identified, permission from the respective copyright holder must be sought.

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

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 978-1-5286-1686-7

CCS1019402408 07/20

Printed on paper containing 75% recycled fibre content minimum

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

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

The Rt Hon. Dr Julian Lewis MP (Chair)

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

This Report is the result of an Inquiry conducted by the previous Committee, which sat from November 2017 to November 2019:

The Rt Hon. Dominic Grieve QC MP (Chair)

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

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

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

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

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

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

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

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

CONTENTS

INTRODUCTION

1. The dissolution of the USSR was a time of hope in the West. In the 1990s and early 2000s, Western thinking was, if not to integrate Russia fully, at least to ensure that it became a partner. By the mid-2000s, it was clear that this had not been successful. The murder of Alexander Litvinenko in 2006 demonstrated that Russia under President Putin had moved from potential partner to established threat. Since then, there have been a number of attempts to repair relations between Western countries and Russia (for example, the US 'Russian reset' in 2009, and the Prime Minister's visit to Moscow in 2011 in which he expressed a desire to rebuild the relationship), but the events of recent years show that none has had any impact on Russian intent, and therefore on the security threat that Russia poses.

2. Russia is simultaneously both very strong and very weak. The strengths which Russia retains are largely its inheritances from the USSR and its status as a victor of the Second World War: nuclear weapons, a space presence and a permanent seat on the UN Security Council. By contrast, it has a small population compared with the West; a lack of both reliable partners and cultural influence outside the countries of the former USSR; a lack of strong public and democratic institutions, including the rule of law; and, of course, a weak economy.

3. Despite its economic weakness, it nonetheless heavily resources its intelligence services and armed forces, which are disproportionately large and powerful. Moreover, Russia is adept at using its apparent weaknesses to its advantage: for example, its poor national brand and lack of long-term global friends appear to feed its enormous risk appetite – perhaps on the basis that it thinks it has nothing to lose; its lack of democracy and rule of law allows its intelligence agencies to act quickly, without constraint or consideration; and its lack of strong independent public bodies and the fusion of government and business allow it to leverage all its intelligence, military and economic power at the same time to pose an all-encompassing security threat.

What does Russia want?

4. The security threat posed by Russia is difficult for the West to manage as, in our view and that of many others, it appears fundamentally nihilistic. Russia seems to see foreign policy as a zero-sum game: any actions it can take which damage the West are fundamentally good for Russia. It is also seemingly fed by paranoia, believing that Western institutions such as NATO and the EU have a far more aggressive posture towards it than they do in reality. There is also a sense that Russia believes that an undemocratic 'might is right' world order plays to its strengths, which leads it to seek to undermine the Rules Based International Order – whilst nonetheless benefitting from its membership of international political and economic institutions.

5. Russia's substantive aims, however, are relatively limited: it wishes to be seen as a resurgent 'great power' – in particular, dominating the countries of the former USSR – and to ensure that the privileged position of its leadership clique is not damaged.

Why the UK?

6. It appears that Russia considers the UK one of its top Western intelligence targets: while we may not experience the level and type of threat that countries on Russia's borders suffer, witnesses have suggested that we would sit just behind the US and NATO in any priority list. This is likely to be related to the UK's close relationship with the US, and the fact that the UK is seen as central to the Western anti-Russian lobby.[1]

7. This perception will have been reinforced by the UK's firm stance recently in response to Russian aggression: following the UK-led international response to the Salisbury attack – which saw an unprecedented 153 Russian intelligence officers and diplomats expelled from 29 countries and NATO – it appears to the Committee that Putin considers the UK to be a key diplomatic adversary. The threat to the UK – and any changes to this following the actions taken in response to the Salisbury attack – is described in this Report, together with the action that the UK Intelligence Community is taking to counter those threats.[2]

The Report

8. This has been a major Inquiry, spanning a number of evidence sessions with a broad range of witnesses over the course of eight months, in addition to a substantial volume of written evidence. We are grateful to those outside the Intelligence Community – in particular Anne Applebaum, William Browder, Christopher Donnelly, Edward Lucas and Christopher Steele – for volunteering their very substantial expertise on Russia, which provided us with an invaluable foundation for the classified evidence sessions.

9. We also express our particular gratitude to the late Sir Charles Farr, who was Chair of the Joint Intelligence Committee for much of the duration of our Inquiry. The evidence he provided directly and his wider assistance in the progression of our Inquiry were both very helpful. We wish to take this opportunity to pay tribute more broadly to his lifetime of exceptional service to the Intelligence Community.

10. The matters covered by our Inquiry are highly sensitive. We have been told, repeatedly, that the Russian Intelligence Services will analyse whatever we put in the public domain and therefore, on this subject more than any other, the potential to damage the capabilities of the intelligence and security Agencies and Defence Intelligence was both real and significant. It was clear, therefore, that any Report would have to be subjected to extensive redaction, and risked becoming unreadable. In order to be able to publish a Report at all, we have accordingly decided to produce a shorter Report than usual, which takes the form of a summary of the most important points we have noted during the Inquiry, at a high level, without revealing underlying detail. We have supplemented this with a substantial Annex, which provides both greater detail on the points we have raised and further rationale for the judgements we have reached. This Annex is not published at this time, in view of the current Russian threat.

---

[1] There is, of course, also a long history of hostile engagement between the Russian – and previously Soviet – intelligence services and their UK counterparts.

[2] Throughout this report the term 'Intelligence Community' is used to refer to the seven organisations that the Committee oversees: the intelligence and security Agencies (MI5, SIS and GCHQ); Defence Intelligence in the Ministry of Defence; the Office for Security and Counter-Terrorism (OSCT) in the Home Office; and the National Security Secretariat (NSS) and Joint Intelligence Organisation (JIO) in the Cabinet Office.

11. The Report covers aspects of the Russian threat to the UK (Cyber; Disinformation and Influence; and Russian Expatriates) followed by an examination of how the UK Government – in particular the Agencies and Defence Intelligence – has responded (Allocation of Effort; Strategy, Co-ordination and Tasking; A Hard Target; Legislation; International Partnerships; and Engagement with Russia).

12. As a result of our scrutiny, we have reached conclusions as to what is working well, where there is a need for more, or different, effort, or where a strategy may need updating, and we have commissioned a number of actions. These are embedded throughout the Report. We note here, however, that there have been a number of cross-cutting themes which have emerged during the course of our work:

- Most surprising, perhaps, was the extent to which much of the work of the Intelligence Community is focused on ***. We had, at the outset of our Inquiry, believed they would be taking a rather broader view, given that it is clearly acknowledged that the Russians use a whole-of-state approach.

- This focus has led us to question who is responsible for broader work against the Russian threat and whether those organisations are sufficiently empowered to tackle a hostile state threat such as Russia. In some instances, we have therefore recommended a shift in responsibilities. In other cases, we have recommended a simplification: there are a number of unnecessarily complicated wiring diagrams that do not provide the clear lines of accountability that are needed.

- The clearest requirement for immediate action is for new legislation: the Intelligence Community must be given the tools it needs and be put in the best possible position if it is to tackle this very capable adversary, and this means a new statutory framework to tackle espionage, the illicit financial dealings of the Russian elite and the 'enablers' who support this activity.

- More broadly, the way forward lies with taking action with our allies; a continuing international consensus is needed against Russian aggressive action. The West is strongest when it acts collectively and that is the way in which we can best attach a cost to Putin's actions. The UK has shown it can shape the international response, as it did in response to the Salisbury attacks. It must now seek to build on this effort to ensure that momentum is not lost.

A sophisticated player

13. GCHQ assesses that Russia is a highly capable cyber actor with a proven capability to carry out operations which can deliver a range of impacts across any sector:

- Since 2014, Russia has carried out malicious cyber activity in order to assert itself aggressively in a number of spheres, including attempting to influence the democratic elections of other countries – for example, it has been widely reported that the Russians were behind the cyber-enabled 'hack and leak' operation to compromise the accounts of members of the French political party *En Marche!* in the run-up to the 2017 French elections.[3]

- Russia has also undertaken cyber pre-positioning[4] activity on other nations' Critical National Infrastructure (CNI).[5] The National Cyber Security Centre (NCSC) has advised that there is *** Russian cyber intrusion into the UK's CNI – particularly marked in the *** sectors.

- GCHQ has also advised that Russian GRU[6] actors have orchestrated phishing[7] attempts against Government departments – to take one example, there were attempts against ***,[8] the Foreign and Commonwealth Office (FCO) and the Defence Science and Technology Laboratory (DSTL) during the early stages of the investigation into the Salisbury attacks.[9]

14. Russia has sought to employ organised crime groups to supplement its cyber skills: SIS has observed that "*this comes to the very muddy nexus between business and corruption and state power in Russia*".[10] GCHQ told the Committee that there is "*a quite considerable balance of intelligence now which shows the links between serious and organised crime groups and Russian state activity*" and that "*we've seen more evidence of *** serious and organised crime *** being connected at high levels of Russian state and Russian intelligence*", in what it described as a "*symbiotic relationship*".[11]

15. Russia's cyber capability, when combined with its willingness to deploy it in a malicious capacity, is a matter of grave concern, and poses an immediate and urgent threat to our national security.

---

[3] 'Hack and leak' refers to the obtaining of private information by hacking, and making it public.
[4] Pre-positioning in the context of cyber activity is the process of exploring and securing an entry point in a network that now, or in the future, could be used to disruptive effect. It is not always immediately apparent whether the intrusion is for espionage purposes or pre-positioning.
[5] Critical National Infrastructure (CNI) comprises the facilities, systems, sites, information, people, networks and processes necessary for a country to function and upon which daily life depends. In the UK, there are 13 CNI sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water.
[6] The GRU is the Main Intelligence Directorate of the General Staff of the Russian Armed Forces.
[7] Phishing – the fraudulent practice of sending emails purporting to be from reputable organisations in order to reveal personal information, such as passwords and credit card numbers.
[8] ***
[9] GCHQ, *Quarterly Report to the ISC*, July–September 2018.
[10] Oral evidence – SIS, *** February 2019.
[11] Oral evidence – GCHQ, *** February 2019.

Leading the response

16. The NCSC – part of GCHQ – leads on protecting the UK from cyber attack and, as the authority on the UK's cyber security environment, sharing knowledge and addressing systemic vulnerabilities. It is the Government's interface with industry on cyber security and leads on incident response (for example, in the event of a cyber attack on the UK's CNI).

17. However, it is clear that cyber is a crowded domain – or a "*complex landscape*".[12] There are a number of agencies and organisations across the Intelligence Community which have a role in countering the Russian cyber threat, and it was not immediately apparent how these various agencies and organisations are co-ordinated and indeed complement each other. The next iteration of the National Cyber Security Strategy must address this need for greater cohesion.

18. Accountability is an issue in particular – whilst the Foreign Secretary has responsibility for the NCSC, which is responsible for incident response, the Home Secretary leads on the response to major cyber incidents. Indeed, there are a number of other Ministers with some form of responsibility for cyber – the Defence Secretary has overall responsibility for Offensive Cyber as a 'warfighting tool' and for the National Offensive Cyber Programme, while the Secretary of State for the Department for Digital, Culture, Media and Sport (DCMS) leads on digital matters, with the Chancellor of the Duchy of Lancaster being responsible for the National Cyber Security Strategy and the National Cyber Security Programme. It makes for an unnecessarily complicated wiring diagram of responsibilities; this should be kept under review by the National Security Council (NSC).

Attribution: a new approach

19. What is clear about the Government's response is that it has now begun to take a more assertive approach. Cyber attribution is the process of identifying and then laying blame on the perpetrator of a cyber attack. The UK has historically been reticent in attributing cyber attacks – as recently as 2010, this Committee was asked to redact mention of Russia as a perpetrator of cyber attacks, on diplomatic grounds.[13]

20. This new approach was indicated first by the response to the November 2017 WannaCry attack (with a statement by Foreign Office Minister Lord Ahmad condemning the attack) and the subsequent response to the February 2018 NotPetya attack, then more recently when the Foreign Secretary took the step, on 3 October 2018, of announcing publicly that the UK and its allies had identified a campaign by the GRU of indiscriminate and reckless cyber attacks targeting public institutions, businesses, media and sport[14] – including attribution of the attempted hacking of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Hague.[15] This must be the right approach; there has to now be a cost attached to such activity. When attacks can be traced back – and we accept that this is in itself resource-intensive – the Government must always consider 'naming and shaming'.

---

[12] Oral evidence – NSS, *** February 2019.
[13] The Committee did not accept this request, and published the information.
[14] NCSC, *Reckless campaign of cyber attacks by Russian military intelligence service exposed*, 3 October 2018, (www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed).
[15] A joint statement was made by the Prime Minister, the Rt Hon. Theresa May MP, and the Prime Minister of the Netherlands, Mr Mark Rutte, on 4 October 2018.

HMG as a player: Offensive Cyber

21. Nonetheless, this is an era of hybrid warfare and an Offensive Cyber capability is now essential. The Government announced its intention to develop an Offensive Cyber capability in September 2013, and in 2014 the National Offensive Cyber Programme (NOCP) – a partnership between the Ministry of Defence and GCHQ – was established.[16]

22. The UK continues to develop its Offensive Cyber capability. The Ministry of Defence and GCHQ have described it as a "*genuinely joint endeavour*".[17] This has led us to question whether there are clear lines of accountability. The Committee was assured by the Chief of Defence Intelligence that:

> *By executing a joint mission, we* [the Ministry of Defence and GCHQ] *can move seamlessly between one set of authorisations and another, making sure we're acting appropriately, but those that are managing the capability are able to make that switch and run those operations effectively.*[18]

We expect to be kept updated on how the dual authorisation process is working as the capability itself continues to develop.

23. GCHQ and the Ministry of Defence have in recent years adopted a more open posture on Offensive Cyber,[19] for example with public references to the successful prosecution of a major Offensive Cyber campaign against Daesh. The issue of Offensive Cyber is addressed in more detail in the classified Annex to this Report.

24. *** – GCHQ acknowledged that *** it would have to broaden its recruitment base, with a shift towards recruiting on aptitude rather than on pre-existing skills. It was also interesting to hear that Defence Intelligence is taking steps to develop and retain these skills through revision of the military resourcing model, which will mean military personnel remaining in cyber roles for longer than the current one to two years. The Committee supports the lengthening of posts as a general principle across the board, not just in Defence Intelligence and not just in cyber. Corporate knowledge and experience are continually lost across Government with such short rotations, and there is a question as to how long an individual needs in a post in order to start contributing or whether they move on just as they are up to speed. We commend Defence Intelligence for being the first to recognise this problem and take action.

International actions

25. Whilst the UK must have its own defensive and offensive capabilities, it must also be prepared to lead international action. In terms of attribution, it is apparent that not everyone is keen to adopt this new approach and to 'call out' Russia on malicious cyber activity. The Government must now leverage its diplomatic relationships to develop a common international approach when it comes to the attribution of malicious cyber activity by Russia and others.

26. There is also a need for a common international approach in relation to Offensive Cyber. It is clear there is now a pressing requirement for the introduction of a doctrine, or set of

[16] The announcement by then Defence Secretary Philip Hammond also included the launch of a Cyber Reserve Unit.
[17] Oral evidence – GCHQ, *** February 2019.
[18] Oral evidence – Defence Intelligence, *** February 2019.
[19] The Director of GCHQ referenced the cyber campaign against Daesh in a speech at CyberUK on 21 April 2018.

protocols, to ensure that there is a common approach to Offensive Cyber. While the UN has agreed that international law, and in particular the UN Charter, applies in cyberspace, there is still a need for a greater global understanding of how this should work in practice. The Committee made this recommendation over two years ago in its Annual Report 2016–2017.[20] It is imperative that there are now tangible developments in this area in light of the increasing threat from Russia (and others, including China, Iran and the Democratic People's Republic of Korea). Achieving a consensus on this common approach will be a challenging process, but as a leading proponent of the Rules Based International Order it is essential that the UK helps to promote and shape Rules of Engagement, working with our allies.[21]

[20] *Intelligence and Security Committee of Parliament Annual Report 2016–2017*, HC 655.
[21] The UK's position on applying international law to cyberspace was set out in a speech, *Cyber and International Law in the 21st century*, delivered by the Attorney General, the Rt Hon. Jeremy Wright QC MP, at Chatham House on 23 May 2018.

DISINFORMATION AND INFLUENCE

27. The spreading of disinformation (by which we mean the promotion of intentionally false, distorting or distracting narratives) and the running of 'influence campaigns' are separate but interlinked subjects. An influence campaign in relation to an election, for example, may use the spreading of disinformation, but may also encompass other tactics such as illicit funding, disruption of electoral mechanics or direct attacks on one of the campaigns (such as 'hack and leak'). Equally, the spreading of disinformation is not necessarily aimed at influencing any individual outcome; it can simply have broad objectives around creating an atmosphere of distrust or otherwise fracturing society.[22]

28. Russia's promotion of disinformation and its attempts at broader political influence overseas have been widely reported.[23] Examples include:

- use of state-owned traditional media: open source studies have shown serious distortions in the coverage provided by Russian state-owned international broadcasters such as RT and Sputnik;[24]

- 'bots' and 'trolls': open source studies have identified significant activity on social media;

- 'hack and leak': the US has publicly avowed that Russia conducted 'hack and leak' operations in relation to its presidential election in 2016, and it has been widely alleged that Russia was responsible for a similar attack on the French presidential election in 2017; and

- 'real life' political interference: it has been widely reported that Kremlin-linked entities have made 'soft loans' to the (then) *Front National* in France, seemingly at least in part as a reward for the party having supported Russia's annexation of Crimea,[25] and the GRU sponsored a failed coup in Montenegro in October 2016[26] – an astonishingly bold move in a country just a few months from its accession to NATO.

29. Russia may spread disinformation or seek to influence political events for a wide range of purposes, but all in support of its underlying foreign policy objectives:

- direct support of a pro-Russian narrative in relation to particular events (whilst some of the outright falsehoods which are put forward may not be widely believed, they may still succeed in casting doubt on the true account of events: "*When people*

[22] Promoting disinformation does not usually lead to any criminal or civil liability under UK law, but an influence campaign which interferes in a democratic process could (this is considered further in the *Legislation* section of this Report).
[23] We note that Russia's disinformation efforts against the West are dwarfed by those which the Russian state conducts against its own population.
[24] A survey of some such studies can be found in the Digital, Culture, Media and Sport Select Committee's report *Disinformation and 'Fake News'*, HC 1791, 18 February 2019. In the case of RT, Edward Lucas informed the Committee that the direct "*impact of RT ... is tiny ... Any one time ... there is an average of 1,300 people in this country watching RT ... the real point of RT is it is a way of gaining legitimacy in elite circles and not least saying to MPs and Peers 'Here is [say] £2,000 in cash if you appear on our programme*'" and Christopher Donnelly explained that "*in the UK its main impact ... is through social media output. It gets out its message on any serious activity that happens* [on social media] *within 20 minutes ...*" (oral evidence – 12 July 2018).
[25] ***
[26] Written evidence – HMG, 29 June 2018.

start to say 'You don't know what to believe' or 'They're all as bad as each other', the disinformers are winning"[27]);

- direct support of Russia's preferred outcome in relation to an overseas election or political issue; and

- general poisoning of the political narrative in the West by fomenting political extremism and 'wedge issues',[28] and by the 'astroturfing'[29] of Western public opinion; and general discrediting of the West.[30]

30. In terms of the direct threat to elections, we have been informed that the mechanics of the UK's voting system are deemed largely sound: the use of a highly dispersed paper-based voting and counting system makes any significant interference difficult, and we understand that GCHQ has undertaken a great deal of work to help ensure that the online voter registration system is safe.[31] Nonetheless, GCHQ informed us that "***",[32] and the Deputy National Security Adviser noted that "*there is a lot of work going on* [in relation to electoral mechanics] *to map the end-to-end processes … *** and to make sure where we can we are mitigating the risks there*".[33] This was reflected in the Joint Intelligence Committee (JIC) judgement in May 2017 that "*the UK paper-based voting process is protected from cyber operations but ****".[34] ***. The Committee will expect an update on this in six months.

A 'hot potato'

31. The UK is clearly a target for Russia's disinformation campaigns and political influence operations[35] and must therefore equip itself to counter such efforts. The Agencies have emphasised that they see their role in this as providing secret intelligence[36] as context for other organisations, as part of a wider HMG response:[37] they do not view themselves as holding primary responsibility for the active defence of the UK's democratic processes from hostile foreign interference, and indeed during the course of our Inquiry appeared determined to distance themselves from any suggestion that they might have a prominent role in relation to the democratic process itself, noting the caution which had to be applied in relation to intrusive powers in the context of a democratic process. They informed us that the Department for Digital, Culture, Media and Sport (DCMS) holds primary responsibility for disinformation

[27] *The Integrity Initiative Guide to Countering Russian Disinformation*, 2018 (the Integrity Initiative is a project run by the Institute for Statecraft, a UK-based think-tank and charity, aimed at countering Russian disinformation campaigns).
[28] 'Wedge issues' are highly divisive subjects which bifurcate a country's population, often (but not always) into socially liberal and socially conservative camps, and which often to at least some degree transcend traditional political party boundaries. Examples of wedge issues include abortion and gun control in the US and Brexit in the UK.
[29] 'Astroturfing' is a propaganda technique whereby a viewpoint is falsely presented as belonging to a certain group. In this instance, employees of the Russian state and Russian-controlled bots may masquerade as ordinary British citizens on social media and give the UK's politicians, journalists and other people who may have power and influence the impression – simply via the sheer quantity of posts – that the views espoused are genuinely those of a majority of their country's public.
[30] Whilst the purpose of this sort of campaign is sometimes to directly damage Western positions, some of this effort is aimed at ensuring that the nature of Russia's ruling elite is not exposed. In the words of Edward Lucas in his evidence to the Committee: "*If you believe that the West is run by hypocritical, incompetent, greedy politicians, then it becomes much harder to take any kind of moral high ground about Russia which really is run by very, very bad people.*"
[31] Oral evidence – GCHQ, *** December 2018; oral evidence – NSS, *** February 2019.
[32] Oral evidence – GCHQ, *** February 2019.
[33] Oral evidence – NSS, *** February 2019.
[34] JIC(17)053.
[35] We note that the formal HMG assessment categorises the UK as a "***" target for political influence operations.
[36] In addition to providing secret intelligence, the Agencies may ***.
[37] We note that the Centre for the Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC) also support the Government security architecture and play a role in protecting the mechanics of elections, including informing improvements to electoral management software and through protective security advice to political parties.

campaigns, and that the Electoral Commission has responsibility for the overall security of democratic processes.

32. However, DCMS told us that its function is largely confined to the broad HMG policy regarding the use of disinformation rather than an assessment of, or operations against, hostile state campaigns. It has been surprisingly difficult to establish who has responsibility for what. Overall, the issue of defending the UK's democratic processes and discourse has appeared to be something of a 'hot potato', with no one organisation recognising itself as having an overall lead.

33. Whilst we understand the nervousness around any suggestion that the intelligence and security Agencies might be involved in democratic processes – certainly a fear that is writ large in other countries – that cannot apply when it comes to the protection of those processes. And without seeking in any way to imply that DCMS is not capable, or that the Electoral Commission is not a staunch defender of democracy, it is a question of scale and access. DCMS is a small Whitehall policy department and the Electoral Commission is an arm's length body; neither is in the central position required to tackle a major hostile state threat to our democracy. Protecting our democratic discourse and processes from hostile foreign interference is a central responsibility of Government, and should be a ministerial priority.

34. In our opinion, the operational role must sit primarily with MI5, in line with its statutory responsibility for "*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 …* ".[38] The policy role should sit with the Office for Security and Counter-Terrorism (OSCT) – primarily due to its ten years of experience in countering the terrorist threat and its position working closely with MI5 within the central Government machinery. This would also have the advantage that the relationship built with social media companies to encourage them to co-operate in dealing with terrorist use of social media could be brought to bear against the hostile state threat; indeed, it is not clear to us why the Government is not already doing this.

35. With that said, we note that – as with so many other issues currently – it is the social media companies which hold the key and yet are failing to play their part; DCMS informed us that ***.[39] The Government must now seek to establish a protocol with the social media companies to ensure that they take covert hostile state use of their platforms seriously, and have clear timescales within which they commit to removing such material. Government should 'name and shame' those which fail to act. Such a protocol could, usefully, be expanded to encompass the other areas in which action is required from the social media companies, since this issue is not unique to Hostile State Activity. This matter is, in our view, urgent and we expect the Government to report on progress in this area as soon as possible.

The Defending Democracy programme

36. The problems identified above regarding roles and responsibilities may be addressed by the Government's Defending Democracy programme, which was publicly announced in

[38] Section 1(2), Security Service Act 1989; MI5 has informed us that it currently has a role to (i) "investigate leads to any of this sort of clandestine activity by foreign states"; (ii) "translate [the] intelligence picture into protective advice to defend our systems"; and (iii) "provide assessed intelligence reporting into the policy system to assist in policy formulation" (oral evidence – MI5, *** December 2018).
[39] Written evidence – DCMS, 13 February 2019.

July 2019. We have been told that this will co-ordinate the Government's work on protecting democratic discourse and processes from interference under the leadership of the Cabinet Office, with the Chancellor of the Duchy of Lancaster[40] and the Deputy National Security Adviser holding overall responsibility at ministerial and official level respectively.

37. The aim is sound, but the response proposed is still rather fragmented (with at least ten separate teams within Government involved, as well as the Electoral Commission and Information Commissioner's Office). In addition, it seems to have been afforded a rather low priority: it was signed off by the National Security Council only in February 2019, almost three years after the EU referendum campaign and the US presidential election which brought these issues to the fore. In the Committee's view, a foreign power seeking to interfere in our democratic processes – whether it is successful or not – cannot be taken lightly; our democracy is intrinsic to our country's success and well-being and any threat to it must be treated as a serious national security issue by those tasked with defending us.

Political advertising on social media

38. The regulation of political advertising falls outside this Committee's remit. We agree, however, with the DCMS Select Committee's conclusion that the regulatory framework needs urgent review if it is to be fit for purpose in the age of widespread social media. In particular, we note and affirm the Select Committee's recommendation that all online political adverts should include an imprint stating who is paying for it.[41] We would add to that a requirement for social media companies to co-operate with MI5 where it is suspected that a hostile foreign state may be covertly running a campaign.

Case study: the EU referendum

39. There have been widespread public allegations that Russia sought to influence the 2016 referendum on the UK's membership of the EU. The impact of any such attempts would be difficult – if not impossible – to assess, and we have not sought to do so. However, it is important to establish whether a hostile state took deliberate action with the aim of influencing a UK democratic process, irrespective of whether it was successful or not.

40. Open source studies have pointed to the preponderance of pro-Brexit or anti-EU stories on RT and Sputnik, and the use of 'bots' and 'trolls', as evidence of Russian attempts to influence the process.[42] We have sought to establish whether there is secret intelligence which supported or built on these studies. In response to our request for written evidence at the outset of the Inquiry, MI5 initially provided just six lines of text. It stated that ***, before referring to academic studies.[43] This was noteworthy in terms of the way it was couched (***) and the reference to open source studies ***. The brevity was also, to us, again, indicative of the extreme caution amongst the intelligence and security Agencies at the thought that they might have any role in relation to the UK's democratic processes, and particularly one as contentious as the EU referendum. We repeat that this attitude is illogical; this is about the

[40] The Chancellor of the Duchy of Lancaster delegates to the Minister for the Constitution as appropriate.
[41] DCMS Select Committee, *Disinformation and 'Fake News',* HC 1791, 18 February 2019.
[42] The DCMS Select Committee's report *Disinformation and 'Fake News'* (HC 1791, 18 February 2019) surveys and comments on some of these studies.
[43] Written evidence – HMG, 3 April 2018.

protection of the process and mechanism from hostile state interference, which should fall to our intelligence and security Agencies.

(i) Failure to prepare

41. There has been credible open source commentary suggesting that Russia undertook influence campaigns in relation to the Scottish independence referendum in 2014.[44] However, at the time ***. It appears that *** what some commentators have described as potentially the first post-Soviet Russian interference in a Western democratic process. We note that – almost five years on – ***.[45]

42. It was only when Russia completed a 'hack and leak' operation against the Democratic National Committee in the US – with the stolen emails being made public a month after the EU referendum – that it appears that the Government belatedly realised the level of threat which Russia could pose in this area, given that the risk thresholds in the Kremlin had clearly shifted, describing the US 'hack and leak' as a "*game changer*",[46] and admitting that "*prior to what we saw in the States,* [Russian interference] *wasn't generally understood as a big threat to* [electoral] *processes*".[47]

43. It appears that the Intelligence Community did learn lessons from the US experience, and HMG recognised the Russian threat to the UK's democratic processes and political discourse. In May 2017, the Joint Intelligence Committee (JIC) concluded that "***" and that "***".[48] Had the relevant parts of the Intelligence Community conducted a similar threat assessment prior to the referendum, it is inconceivable that they would not have reached the same conclusion as to Russian intent, which might then have led them to take action to protect the process.

(ii) Narrow coverage

44. The written evidence provided to us appeared to suggest that HMG had not seen or sought evidence of successful interference in UK democratic processes or any activity that has had a material impact on an election, for example influencing results.[49],[50] ***. ***.[51]

45. This focus on *** indicates that open source material (for example, the studies of attempts to influence the referendum using RT and Sputnik, or social media campaigns referred to earlier) was not fully taken into account. Given that the Committee has previously

---

[44] For example, it was widely reported shortly after the referendum that Russian election observers had suggested that there were irregularities in the conduct of the vote, and this position was widely pushed by Russian state media. We understand that HMG viewed this as being primarily aimed at discrediting the UK in the eyes of a domestic Russian audience. More recently, we note the study by Ben Nimmo – *#ElectionWatch: Scottish Vote, Pro-Kremlin Trolls*, 12 December 2017.

[45] Oral evidence – GCHQ, *** December 2018 ***.

[46] ***

[47] ***

[48] JIC Key Judgement, ***, 26 May 2017.

[49] *** (written evidence – HMG, 29 June 2018).

[50] We note that Arron Banks became the biggest donor in British political history when he gave £8m to the Leave.EU campaign. In October 2018, the Electoral Commission – which had been investigating the source of this donation – referred the case to the National Crime Agency, which investigated it ***. In September 2019, the National Crime Agency announced that it had concluded the investigation, having found no evidence that any criminal offences had been committed under the Political Parties, Elections and Referendums Act 2000 or company law by any of the individuals or organisations referred to it by the Electoral Commission.

[51] ***

been informed that open source material is now fully represented in the Government's understanding of the threat picture, it was surprising to us that in this instance it was not.

46. Whilst it may be true that some issues highlighted in open source did not require the secret investigative capabilities of the intelligence and security Agencies or were at the periphery of their remits, the Agencies nonetheless have capabilities which allow them to 'stand on the shoulders' of open source coverage: for example, GCHQ might attempt to look behind the suspicious social media accounts which open source analysis has identified to uncover their true operators (and even disrupt their use), or SIS might specifically task an agent to provide information on the extent and nature of any Russian influence campaigns.[52] However, we have found *** which suggests that ***. ***.

(iii) Lack of retrospective assessment

47. We have not been provided with any post-referendum assessment of Russian attempts at interference, ***.[53] This situation is in stark contrast to the US handling of allegations of Russian interference in the 2016 presidential election, where an intelligence community assessment[54] was produced within two months of the vote, with an unclassified summary being made public. Whilst the issues at stake in the EU referendum campaign are less clear-cut, it is nonetheless the Committee's view that the UK Intelligence Community should produce an analogous assessment of potential Russian interference in the EU referendum and that an unclassified summary of it be published.[55]

48. ***. Even if the conclusion of any such assessment were that there was minimal interference, this would nonetheless represent a helpful reassurance to the public that the UK's democratic processes had remained relatively safe.

---

[52] ***

[53] ***

[54] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections,* 6 January 2017.

[55] We note that the DCMS Select Committee has called on the Government to launch an independent investigation into foreign influence, disinformation, funding, voter manipulation and the sharing of data in relation to the Scottish independence referendum, the EU referendum and the 2017 General Election. If the Government were to take up this recommendation for a wider investigation, the assessment we recommend should take place could feed into it (DCMS Select Committee, *Disinformation and 'Fake News'*, HC 1791, 18 February 2019, recommendation 39).

Welcoming oligarchs with open arms

49. Whilst the Russian elite have developed ties with a number of countries in recent years, it would appear that the UK has been viewed as a particularly favourable destination for Russian oligarchs and their money. It is widely recognised that the key to London's appeal was the exploitation of the UK's investor visa scheme, introduced in 1994, followed by the promotion of a light and limited touch to regulation, with London's strong capital and housing markets offering sound investment opportunities. The UK's rule of law and judicial system were also seen as a draw. The UK welcomed Russian money, and few questions – if any – were asked about the provenance of this considerable wealth. It appears that the UK Government at the time held the belief (more perhaps in hope than expectation) that developing links with major Russian companies would promote good governance by encouraging ethical and transparent practices, and the adoption of a law-based commercial environment.

50. What is now clear is that it was in fact counter-productive, in that it offered ideal mechanisms by which illicit finance could be recycled through what has been referred to as the London 'laundromat'. The money was also invested in extending patronage and building influence across a wide sphere of the British establishment – PR firms, charities, political interests, academia and cultural institutions were all willing beneficiaries of Russian money, contributing to a 'reputation laundering' process. In brief, Russian influence in the UK is 'the new normal', and there are a lot of Russians with very close links to Putin who are well integrated into the UK business and social scene, and accepted because of their wealth. This level of integration – in 'Londongrad' in particular – means that any measures now being taken by the Government are not preventative but rather constitute damage limitation.

51. It is not just the oligarchs either: the arrival of Russian money resulted in a growth industry of enablers – individuals and organisations who manage and lobby for the Russian elite in the UK. Lawyers, accountants, estate agents and PR professionals have played a role, wittingly or unwittingly, in the extension of Russian influence which is often linked to promoting the nefarious interests of the Russian state. A large private security industry has developed in the UK to service the needs of the Russian elite, in which British companies protect the oligarchs and their families, seek *kompromat*[56] on competitors, and on occasion help launder money through offshore shell companies and fabricate 'due diligence' reports, while lawyers provide litigation support. William Browder told the Committee that:

> *Russian state interests, working in conjunction with and through criminal private interests, set up a 'buffer' of Westerners who become de facto Russian state agents, many unwittingly, but others with a reason to know exactly what they are doing and for whom. As a result, UK actors have to deal with Russian criminal interests masked as state interests, and Russian state interests masked by their Western agents.*[57]

[56] *Kompromat* – compromising information collected for use in blackmailing, discrediting or manipulating someone, typically for political purposes.
[57] Written evidence – William Browder, 14 September 2018.

Trying to shut the stable door

52. The links of the Russian elite to the UK – especially where this involves business and investment – provide access to UK companies and political figures, and thereby a means for broad Russian influence in the UK. To a certain extent, this cannot be untangled and the priority now must be to mitigate the risk and ensure that, where hostile activity is uncovered, the tools exist to tackle it at source.

53. The extent to which Russian expatriates are using their access to UK businesses and politicians to exert influence in the UK is ***: it is widely recognised that Russian intelligence and business are completely intertwined. The Government must ***, take the necessary measures to counter the threat and challenge the impunity of Putin-linked elites. Legislation is a key step, and is addressed later in this Report.

54. Several members of the Russian elite who are closely linked to Putin are identified as being involved with charitable and/or political organisations in the UK, having donated to political parties, with a public profile which positions them to assist Russian influence operations. It is notable that a number of Members of the House of Lords have business interests linked to Russia, or work directly for major Russian companies linked to the Russian state – these relationships should be carefully scrutinised, given the potential for the Russian state to exploit them. It is important that the Code of Conduct for Members of the House of Lords, and the Register of Lords' interests, including financial interests, provide the necessary transparency and are enforced. In this respect, we note that the Code of Conduct for Members of Parliament requires that MPs register individual payments of more than £100 which they receive for any employment outside the House – this does not apply to the House of Lords, and consideration should be given to introducing such a requirement. A 'Foreign Agents Registration Act' (an issue which is addressed in the section on Legislation) would also be helpful in this respect.

55. The Government effort on the disruption of Russian illicit financial activity in the UK is led and co-ordinated by the National Crime Agency (NCA).[58] Its work also encompasses the investigation of UK-based professional enablers in the financial and property sectors, with the aim of hardening the UK financial and property markets from the proceeds of crime, and challenging any perception that the UK is a safe haven for illicit funds. The extent to which this money has now been invested, and reinvested, calls into question the efficacy of the recently introduced Unexplained Wealth Orders when applied to the investigation of individuals with such long-established – and to all intents and purposes now apparently legitimate – financial interests in the UK. Whilst the Orders appear to provide the NCA with more clout and greater powers, the reality is that it is highly probable that the oligarchy will have the financial means to ensure their lawyers – a key group of professional enablers – find ways to circumvent this legislation (we return to this issue later in the Report). By contrast, the NCA lacks the resources required in terms of financial investigators, technical experts and legal expertise – this must be rectified.[59]

56. The inherent tension between the Government's prosperity agenda and the need to protect national security that has led to the current situation has been played out across

[58] The Committee is grateful to the NCA for providing evidence for this Inquiry. The Committee does not oversee the NCA; its work and operations usually fall outside the remit of the ISC.
[59] The Serious and Organised Crime Strategy, published on 1 November 2018, announced the establishment of a multi-agency National Assessment Centre (NAC) and the National Economic Crime Centre within the NCA.

Whitehall departments. However, the formation of the new Serious and Organised Crime (SOC) Group within the Home Office at the end of 2018 was a tangible acknowledgement of economic crime as a national security issue. The SOC Group has a wide-ranging remit – it is hoped that it will be provided with the necessary resources and will give sufficient priority to disrupting the threat posed by illicit Russian financial activity. One key measure would be an overhaul of the Tier 1 (Investor) visa programme[60] – there needs to be a more robust approach to the approval process for these visas.

Russians at risk

57. Whilst the oligarchs and their money have been the most obviously visible part of the Russian diaspora, recent events have highlighted the number of Russians in the UK who are on the opposing side. Since Putin came to power in 1999, a number of critics of Putin and the Russian government have sought sanctuary in the UK, fearing politically motivated criminal charges and harassment.[61] They are of interest to the Russian Intelligence Services (RIS), which may seek to target them in a number of ways:

- it is possible the RIS will seek to monitor some of these individuals using human sources (i.e. agents) and by technical means, for example by intercepting phone calls and hacking into their personal electronic devices;
- RIS collection of intelligence could also be used in support of 'influence operations', with the objective of degrading an individual's ability to encourage international or domestic Russian political opposition to Putin and his government; or
- the RIS may seek to identify or engineer opportunities to arrange an individual's arrest and transfer to Russia to stand trial, or indeed meet a worse fate.

58. On 15 June 2017, BuzzFeed News published the results of its investigation into 14 deaths in the UK of Russian business figures and British individuals linked to them.[62] The attempted assassination of Sergei and Yulia Skripal in March 2018 prompted calls for the Government to investigate the allegations that had been made in the BuzzFeed report and, on 6 March 2018, the Chair of the Home Affairs Select Committee wrote to the Home Secretary calling for a review of the 14 deaths, given the "*considerable concerning evidence*" from BuzzFeed which raised "*questions over the robustness of the police investigations*".[63]

59. The Committee has taken evidence on these matters. We have been told that ***. ***.[64]

60. We questioned whether the need to protect those at risk in the UK has been given sufficient priority. We were assured that all figures at risk – Russian or otherwise – receive protection according to the level of risk, through a police-led process ***.[65]

61. We welcomed this process, but questioned whether the Intelligence Community has a clear picture of how many Russians there are in the UK who are at risk – for example, would

[60] A Tier 1 (Investor) visa allows the recipient to stay in the UK for three years and four months in exchange for a £2m investment in the UK.
[61] These include such high-profile figures as ***.
[62] 'From Russia with Blood', *BuzzFeed News*, 15 June 2017.
[63] Letter from the Chair of the Home Affairs Select Committee to the Home Secretary, 6 March 2018.
[64] ***
[65] Oral evidence – *** February 2019.

MI5 or any other relevant agency ***? This would appear to be an immediate and obvious way in to the issue, and the ***, so it would appear manageable. In response we were told that ***.

62. The events of 4 March 2018 showed that it is not only individuals who are openly critical of Putin who are at risk here in the UK. The Salisbury attack has highlighted the vulnerability of former Russian intelligence officers who have settled in the UK. This issue was investigated by the Committee as part of its Inquiry, and is addressed in the classified Annex to this Report.

ALLOCATION OF EFFORT

63. It is clear that Russia currently poses a significant threat to the UK on a number of fronts – from espionage to interference in democratic processes, and to serious crime. The question is how that has happened – and what the Intelligence Community is now doing to tackle it.

Coverage

64. In its Annual Report 2001–2002, the Committee raised a concern that, as resources were being transferred to counter-terrorism, coverage of other areas had become increasingly thin:

> *These reductions are causing intelligence gaps to develop, which may mean that over time unacceptable risks will arise in terms of safeguarding national security and in the prevention and detection of serious organised crime. The Agencies must be given sufficient resources to enable them not only to fill the staff vacancies that have been created but also to expand sufficiently to ensure that they can meet the new demands now being placed on them.*[66]

The Government responded:

> *The Government recognises that the increase in demand for intelligence to support the campaign against terrorism has meant that the Agencies, amongst others, have been obliged to review their priorities within their own budgets. This process has been carried out professionally and carefully, and the Government will continue to keep the situation under review. It is inevitable that if some areas of activity become relatively more important to the national interest, others become relatively less so and may have less resources devoted to them. All decisions about matching resources to tasks involve a degree of risk. Identifying, quantifying, managing, and where possible mitigating those risks is one of the basic responsibilities of the management of the Agencies. The Government is confident that the judgements taken so far have been the right ones, and that no unacceptable risks with or to national security have been, or will be taken.*[67]

65. In its Annual Report 2002–2003, the Committee reported that it believed that the problem of intelligence collection gaps had worsened, concluding that:

> *The Committee believes that, with the focus on current crises, the Agencies' long-term capacity to provide warnings is being eroded. This situation needs to be addressed and managed by Ministers and the JIC* [Joint Intelligence Committee].[68]

---

[66] *Intelligence and Security Committee of Parliament Annual Report 2001–2002*, Cm 5542.
[67] As quoted in the *Intelligence and Security Committee of Parliament Annual Report 2002–2003*, Cm 5837.
[68] *Intelligence and Security Committee of Parliament Annual Report 2002–2003*, Cm 5837.

In 2003–2004, the Committee again expressed concern:

> *We remain concerned that, because of the necessary additional effort allocated to counter-terrorism by the Security Service, significant risks are inevitably being taken in the area of counter-espionage.*[69]

MI5

66. MI5's remit – as set out in the Security Service Act 1989 – is 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*".[70] MI5 states its objectives in this area as being to "*seek to find those trying to pass sensitive UK information and equipment to other countries and ensure they don't succeed*" and to "*investigate and disrupt the actions of foreign intelligence officers where these are damaging to our country's interests*".[71]

67. Twenty years ago, MI5 devoted around 20% of its effort to Hostile State Activity, which includes Russian activity alongside the hostile activity of other states, such as China and Iran.[72] This allocation of effort declined, as the terrorist threat grew. By 2001/02, it had reduced to 16% and by 2003/04 to 10.7%. This fall continued until, by 2008/09, only 3% of effort was allocated by MI5 to all its work against Hostile State Activity (noting that reductions in proportion of overall effort do not translate directly into changes in resource).[73] It was not until 2013/14 that effort began to increase significantly, rising to 14.5%[74] – a level that MI5 says meant that slightly more staff were working on Russia than had been during the Cold War.[75] The past two years have seen ***: currently, ***% is allocated to Hostile State Activity, approximately *** which is dedicated to countering Russian Hostile State Activity.[76]

SIS and GCHQ

68. SIS is the UK's foreign human intelligence (HUMINT) agency, with a "*global covert capability*"[77] focusing on intelligence gathering. Areas of intelligence coverage work that SIS undertakes in relation to Russia include cultivating agents who are in a position to pass on secret information, particularly in relation to the capabilities and intent of the Russian government, and its intelligence effects work includes ***. In 2001, SIS's operational effort against Russia was ***%. This declined to ***% in 2007. It only began to increase significantly in *** and currently stands at approximately ***%.[78]

---

[69] *Intelligence and Security Committee of Parliament Annual Report 2003–2004*, Cm 6240.
[70] Section 1(2) of the Security Service Act 1989.
[71] www.mi5.gov.uk/espionage
[72] Written evidence – MI5, 31 October 2018.
[73] Intelligence and Security Committee of Parliament Annual Reports: 2001–2002, Cm 5542; 2003–2004, Cm 6240; 2008–2009, Cm 7807.
[74] Written evidence – MI5, 31 October 2018.
[75] *Intelligence and Security Committee of Parliament Annual Report 2016–2017*, HC 655.
[76] Written evidence – MI5, 12 March 2019; MI5's overall resource has increased significantly over this period. *** allocation of effort on Hostile State Activity has ***, spending on Hostile State Activity has ***. This operational effort also benefits from the support of corporate and 'enabling' services across MI5 (which is not reflected in these figures).
[77] www.sis.gov.uk
[78] Written evidence – SIS, 17 December 2018.

69. GCHQ is the UK's signals intelligence (SIGINT) agency – also focusing on intelligence gathering.[79] GCHQ's intelligence effects work primarily comprises Offensive Cyber. Areas of intelligence coverage work that GCHQ undertakes include: applying selectors to emails obtained by bulk interception; targeted interception of the phone calls of people of interest; intercepting material transmitted over military communications systems; and hacking into computer systems in order to obtain the information they contain.

70. At the height of the Cold War, 70% of GCHQ's effort was focused on the Soviet bloc.[80] By 2000, this had fallen to 16% and by 2006 effort was at a low point of just 4%. In 2012, this had recovered to 10%, which stayed fairly constant until 2016 when a significant further increase began.[81] Approximately ***% of GCHQ's current operational effort is on Russia.[82]

Defence Intelligence

71. Defence Intelligence has wide-ranging responsibilities for intelligence collection and analysis, and a key role within Government in the preparation of All Source intelligence on Russia. It leads the UK's work on geospatial intelligence (GEOINT) and measurement and signature intelligence (MASINT).[83] It also holds a SIGINT role ***, and has a HUMINT unit which is primarily used to support military operations. Alongside GCHQ, it also has a major role in the UK's Offensive Cyber capability. Defence Intelligence effort on Russia also underwent significant reduction in the early 2000s. Although Defence Intelligence has been unable to provide figures for its allocation of effort over the past 20 years, we have been told that in 2013 there were relatively few All Source analysts in the Russia/Eurasia team (in addition to Russia-focused analysts in other teams). Defence Intelligence has advised that currently *** of its All Source analysts spend more than 50% of their time on Russia and a further *** spend less than 50% of their time on Russia.[84]

Did HMG take its eye off the ball?

72. Following the end of the Cold War, the West aspired to partner with Russia. The threat posed by Russia was considered to be diminished and the proportion of effort allocated to countering the threat decreased accordingly. As can be seen from the figures above, there was a marked drop in allocation of effort. The murder of Alexander Litvinenko in 2006 was perhaps the clearest indication that not only had reconciliation failed, but Russia was once again just as hostile towards the West, and towards the UK. However, by 2006, operational effort was being directed to the fight against international terrorism: in 2006/07, MI5 devoted 92% of its effort to counter-terrorism work,[85] with SIS and GCHQ at 33%.[86] The remaining

---

[79] SIGINT is intelligence gathering through the interception of communications between people, and through the interception of other electronic signals.
[80] Oral evidence – GCHQ, *** December 2018.
[81] Written evidence – GCHQ, 8 March 2019.
[82] Written evidence – GCHQ, 14 December 2018.
[83] Geospatial intelligence (GEOINT) consists of collecting and analysing intelligence on geographical features and the human activities that occur in a geographical context. Measurement and signature intelligence (MASINT) uses technical means to detect and analyse the 'signatures' of targets, in order to locate, analyse and track them.
[84] This represents ***% of Defence Intelligence's current analytical resource being focused on Russia (written evidence – Defence Intelligence, 6 March 2019).
[85] Written evidence – MI5, 31 October 2018.
[86] Written evidence – SIS, 17 December 2018; *Intelligence and Security Committee of Parliament Annual Report 2007–2008* Cm 7542. Defence Intelligence told us that it seconded its analytical effort on counter-terrorism to the Joint Terrorism Analysis Centre (JTAC) when it was established in 2003. This was estimated to be 20 posts by 2006/07 – just 1% of its then workforce (written evidence – Defence Intelligence, 21 March 2019).

resource was thinly spread across a number of areas – Hostile State Activity being just one, and Russia being just one of the hostile states. This is understandable: the threat from international terrorism at that time – just a year after the 2005 terror attacks which claimed the lives of 52 people – had to be the primary focus.

73. If we consider the Russian threat to have been clearly indicated in 2006 with the murder of Alexander Litvinenko, and then take events such as the annexation of Crimea in 2014 as firmly underlining Russian intent on the global stage, the question is whether the Intelligence Community should – and could – have reacted more quickly and increased operational effort on Russia. On figures alone, it could be said that they took their eye off the ball; nevertheless, the Heads of MI5, SIS, GCHQ and Defence Intelligence all sought to defend against this suggestion. MI5 was clear that there was an inevitable reprioritisation due to the terrorist threat:

> *… back then it's how can we possibly do enough to get ahead of this appalling terrorism problem which … back then was larger than we could see the edges of and one of the things we used to say about it, at exactly the time you're talking about, was we haven't yet found the edges of this problem.*[87]

Defence Intelligence viewed it similarly:

> *So in terms of relative prioritisation, rather than losing focus … our coverage of Russia undoubtedly suffered as a consequence of that prioritisation, which was necessary for the conduct of military operations.*[88]

By comparison, SIS and GCHQ saw it as due to the longer lead time required for work on Russia. SIS said:

> *I don't think we did take our eye off the ball. I think the appetite for work against the Russian threat has sort of waxed and waned. ***.*[89]

And GCHQ agreed:

> *A bit like* [SIS's] *point, some of the kind of hardcore capabilities that were necessary to keep in the business we maintained and then, really, as the reviews and the discussion around what happened in Crimea really brought minds more to the fore again on Russia, that then led us to move in ramping up again.*[90]

74. We fully recognise the very considerable pressures on the Agencies since 9/11, and that they have a finite amount of resource, which they must focus on operational priorities. Nevertheless, reacting to the here and now is inherently inefficient and – in our opinion – until recently, the Government had badly underestimated the Russian threat and the response it required.[91]

---

[87] Oral evidence – MI5, *** December 2018.
[88] Oral evidence – Defence Intelligence, *** December 2018.
[89] Oral evidence – SIS, *** December 2018.
[90] Oral evidence – GCHQ, *** December 2018.
[91] We note that the Agencies 'horizon scan' and that this is a matter of prioritisation of resources.

75. Accepting the counter-terrorism pressures on the operational organisations, there is nevertheless a question over the approach taken by the policy departments. We have previously discussed the extent to which economic policy dictated the opening up of the UK to Russian investment. This indicates a failure of the security policy departments to engage with this issue – to the extent that the UK now faces a threat from Russia within its own borders. What appears to have been a somewhat laissez-faire policy approach is less easy to forgive than the response of the busy Agencies. We welcome the fact that this has now been recognised and appears to be changing.

Future resourcing

76. The recent changes in resourcing to counter Russian Hostile State Activity are not (or not only) due to a continuing escalation of the threat – but appear to be an indicator of playing catch-up. SIS and GCHQ planned to change their operational effort against Russia still further – to ***% and ***% respectively by 2020.[92] MI5 is *** and seeking to *** on Hostile State Activity. All three organisations were clear that this was about relative priorities. For example, MI5 told us that:

> *We quite frequently find ourselves quarter on quarter taking *** decisions about … how we will *** across these different subject areas and at the moment we have stuck with some of the resourcing that's surged towards hostile state work after Salisbury, despite the fact that our CT* [Counter-Terrorism] *investigations suspensions rate remains higher than we want it to be.*[93]

In this respect, it must be a matter for Ministers. The Home Secretary told us that, in his view, resourcing on Russia *** and that there "*needs to be more resources in … countering the Hostile State Activity*".[94] He did, however, caution that the threat is wider than Russia alone and the growth in Russia-focused resources cannot be at the expense of efforts on other escalating threats. The Foreign Secretary similarly recognised the importance of not ignoring other priorities:

> *One of my concerns is that some of the short-term problems that Russia is causing us that we are having to address is actually crowding out thinking that we need to be doing on the longer-term changes to the international order, namely the rise of China. So I have been trying to make sure that we find time to actually look at what is changing in the world in its entirety.*[95]

77. With pressures from International Counter-Terrorism work, the Chinese threat, Iran and the Democratic People's Republic of Korea, we recognise that it is difficult to single out the Russian threat as deserving greater allocation of effort. It is therefore essential that the strategy is right – enabling smarter working and effective co-ordination.

---

[92] Written evidence – HMG, 3 April 2018.
[93] Oral evidence – MI5, *** November 2018.
[94] Oral evidence – Home Secretary, 31 January 2019.
[95] Oral evidence – Foreign Secretary, 7 February 2019.

STRATEGY, CO-ORDINATION AND TASKING

The cross-Whitehall Russia Strategy

78. In 2016, the National Security Council approved a cross-Whitehall Russia Strategy. The latest iteration of the Strategy – in March 2019 – has an overarching long-term 'vision' of "*A Russia that chooses to co-operate, rather than challenge or confront*",[96] ***.

79. The Strategy is ordered under five pillars – Protect, Constrain, Engage, Keep Open and Build.[97] Responsibility for this implementation falls to the National Security Strategy Implementation Group for Russia, which comprises 14 departments and agencies. This Implementation Group is co-ordinated by the HMG Russia Unit in the Foreign and Commonwealth Office (FCO), and chaired by the Senior Responsible Owner for implementing the Strategy (currently the FCO's Director-General Consular and Security). All seven organisations that we oversee are represented in the Implementation Group.

80. It is apparent that the cross-Whitehall Russia Strategy has certain similarities – both in format and more fundamentally – to the CONTEST counter-terrorism strategy. However, we understand that no direct lessons have been drawn from CONTEST in drawing up and implementing the Strategy.

81. There also appear to be certain similarities between the struggle against terrorism and Hostile State Activity – particularly in terms of public awareness – and more could be done to leverage the Government's experience on the former in relation to the latter. In particular, it is our view that, whilst MI5 already works with the police regional Counter-Terrorism Units (which have responsibility for Hostile State Activity), there is scope for them to work more closely together in this area.

Ministerial responsibility

82. The Home Secretary holds ministerial responsibility for MI5, the Foreign Secretary for SIS and GCHQ, and the Defence Secretary for Defence Intelligence. All three Secretaries of State have wide portfolios and busy diaries, and there will be natural limits to the extent to which they can devote time to Russia. However, it is clear that Russia is a high ministerial priority: the Home Secretary has informed us that he meets the Director-General of MI5 "*at least once a week, sometimes more, and … in … *** … there has been some discussion around Russia*",[98] and, when asked about how much he speaks to the Chief of SIS and the Director of GCHQ about Russia, the Foreign Secretary replied "***",[99] explaining his concern that Russia-related problems – whilst serious – risk crowding out broader global issues.

83. Policy responsibility for Hostile State Activity sits in the National Security Secretariat in the Cabinet Office. This appears unusual: the Home Office might seem a more natural home for it, as it would allow the Office for Security and Counter-Terrorism's (OSCT) experience on counter-terrorism matters to be brought to bear against the hostile state threat. We understand

[96] We note that the long-term vision of the previous iteration of the Russia Strategy was "*a constrained Russia co-operating with the West, rather than challenging and confronting us*" (the word 'constrained' has now been removed).
[97] Beneath each pillar sits a number of cross-Government 'campaigns' which aim to implement the Strategy.
[98] Oral evidence – Home Secretary, 31 January 2019.
[99] Oral evidence – Foreign Secretary, 7 February 2019.

that Government's view is that Hostile State Activity is a cross-cutting threat and therefore it makes sense for the Cabinet Office to hold responsibility; we nonetheless suggest that it is kept under review.

The Fusion Doctrine and joint working

84. The Committee has heard a great deal over the past year about the Fusion Doctrine, which aims "*to deploy security, economic and influence capabilities to protect, promote and project our national security, economic and influence goals*".[100] In principle, this makes sense in response to a threat as broad as that posed by Russia. We note, however, that Russia's own version of this 'joined-up working' approach is far more developed: given the amount of power centralised in the Kremlin, the lack of strong public institutions, the close connections between big business and the state, and – crucially – its operation outside the Rules Based International Order, Russia is easily able to combine its political, economic, military and intelligence power to achieve its objectives.

85. In relation to the Agencies and Defence Intelligence, given the difficulties in working against Russia (explored in the next section), it is particularly important that all sources – HUMINT, SIGINT, MASINT, GEOINT,[101] open source and others – are used to complement each other as much as possible, and that they are used across all aspects of the co-ordinated Russian threat (***). Given the combined nature of the Russian threat, it is essential that the Agencies' and Defence Intelligence's work on *** is not viewed separately from wider Russian foreign policy and influence efforts. In some cases, we have noted that it has not been clear ***: this must be addressed. It is essential that HMG takes a broader view of the full extent of the Russian threat as the cross-Whitehall Russia Strategy develops and the use of the Fusion Doctrine increases.

The intelligence contributions to the Russia Strategy

86. The Intelligence Coverage and Effects (ICE) process is the method by which SIS and GCHQ are tasked by the Government.[102] The ICE Plan for Russia requires *** coverage outcomes and *** effects outcomes, which are prioritised at five levels: 'non-negotiable', high, medium, low and 'opportunity only'. The intention is to ensure that the Agencies' outputs accord with the intelligence coverage and effects the National Security Council and its 'customer' departments across Government need. On Russia, the ICE requirements represent SIS and GCHQ's tasking in relation to the cross-Whitehall Russia Strategy.

87. In contrast to SIS and GCHQ, MI5 is self-tasking: it prioritises its work against threats to the UK based on its assessment of their severity. This is appropriate given the defensive focus of MI5's role. We have been informed that MI5 does, however, align its work on Russia with that of SIS and GCHQ in an agreed tri-Agency approach.[103]

---

[100] HMG, *National Security Capability Review*, March 2018.
[101] Human intelligence (HUMINT), signals intelligence (SIGINT), measurement and signature intelligence (MASINT), geospatial intelligence (GEOINT).
[102] Intelligence coverage is the collection of information (or acquisition of information from allied intelligence services) by the Agencies and Defence Intelligence. Intelligence effects describe the Agencies' and Defence Intelligence's engagement in activities that have real-life outcomes.
[103] ***

88. Defence Intelligence is tasked by a separate Ministry of Defence process. Given the differences between Defence Intelligence's work and that of the Agencies – including the fact that, in its assessment function, it is a customer for SIS and GCHQ intelligence products – this may make sense. The Chief of Defence Intelligence recognised that "*there is an absolute need for Defence Intelligence to be closely co-ordinated and potentially synchronised with the activity that is going on in ICE*" but caveated that "w*hether we go fully into the ICE process I think is a much harder question to deal with*".[104] We recognise that it may not be appropriate for Defence Intelligence to be covered by ICE, but we were surprised to discover that Defence Intelligence is not included in the tri-Agency approach: ***.

Less talk, more action?

89. There appears to be a plethora of plans and strategies with direct relevance to the work on Russia by the organisations we oversee: the cross-Whitehall Russia Strategy, the ICE Plan requirements for Russia, the tri-Agency joint approach for Russia, a separate tasking and prioritisation process for Defence Intelligence, and the Fusion Doctrine overlaying them all. Whilst we appreciate that there may be good reasons for the existence of each of these documents, it has nonetheless taken some time to understand the purposes behind each one and how they interlink: this suggests that the overall strategy framework is not as simple as it might be. Whilst we do not advocate any immediate overhaul of this framework in relation to Russia (which could serve to worsen the situation by diverting resources away from the Intelligence Community's core work in this area), we nonetheless recommend that, in future, the Government ensures that the plans and priorities are as streamlined as possible. Time spent strategising is only useful if done efficiently, and without getting in the way of the work itself.

Measuring performance

90. We asked the Agencies and Defence Intelligence to assess their current performance against the strategic objectives and plans in place in relation to the Russian threat. Defence Intelligence clearly explained that "*we survey our customers of our product, on a scale that we set out from zero to nine, at the moment … the score that we have aggregated across all of our Russia work is* ***".[105] However, the Agencies could not provide an equally clear assessment. It does not appear that they measure their performance in quite such a developed way: GCHQ and SIS informed us that their assessment of their performance against the ICE Plan was in a comparatively less granular format (which broadly assesses whether or not they had exceeded, met or not met each requirement) and SIS told us that "*the question of performance management and metrication … this is a process which is in evolution*".[106] The Agencies should measure their performance in greater detail – we accept that this is not an exact science, but they must seek a full picture of how successful their work on Russia is.

91. We have sought to establish for ourselves a picture of the quality of the Agencies' current coverage of Russia. However, this has, to a certain extent, been hampered by the organisations we oversee referring frequently in oral evidence to the exemption (in the Justice and Security Act 2013) for information that relates to ongoing operations. We remind the Government

[104] Oral evidence – Defence Intelligence, *** December 2018.
[105] Oral evidence – Defence Intelligence, *** January 2019.
[106] Oral evidence – SIS, *** December 2018.

that the Justice and Security Act 2013 does not oblige it to withhold information relevant to ongoing operations but merely provides the option of doing so. The Agencies and departments are able to provide any information relating to an ongoing intelligence or security operation voluntarily. Whilst we would not expect to receive highly sensitive current operational material in most cases, it is disappointing that in relation to a subject of such public interest this option has been exercised quite so broadly.

A HARD TARGET

92. As already noted, the Russian government is an accomplished adversary with well-resourced and world-class offensive and defensive intelligence capabilities. The well-publicised mistakes Russian operatives made in Salisbury, and later in trying to infiltrate the Organisation for the Prohibition of Chemical Weapons (OPCW), have led to public speculation about the competence of the Russian Intelligence Services (RIS), and the GRU in particular. Whilst these attacks demonstrate that the RIS are not infallible, it would be foolhardy to think that they are any less dangerous because of these mistakes. Indeed, the likelihood is that the RIS will learn from their errors, and become more difficult to detect and protect against as a result.

A unique challenge

93. All witnesses agreed that Russia is one of the hardest intelligence challenges that there is. There are a number of reasons for this. While some are generic problems that are heightened by Russian ability to exploit them (for example, ***), others are unique to Russia (for example, ***).

(i) Structure

94. The Russian decision-making apparatus is concentrated on Putin and a small group of trusted and secretive advisers (many of whom share Putin's background in the RIS). The limited number of individuals who are 'in the know' makes decision-making hard to understand, compared with systems where power and influence are dispersed among a great number of political players. Moreover, the President can make swift decisions that even his inner circle are not aware of – further complicating any ability to understand or predict Russian government intent.

95. This centralised decision-making allows the Russian government to carry out decisions at speed. Putin's inner circle appear to be willing and able to make and enact major decisions (for example, on the deployment of troops) within days, and they retain tight command and control over the whole government infrastructure – which can be put in the service of Russia's foreign policy goals at a moment's notice. It is difficult for the UK's democratic and consensus-based structures to match this pace. Putin appears to value surprise and the unexpected, and has therefore consciously retained and cultivated this 'decision-advantage' as a way of outmanoeuvring adversaries.

96. It is not clear to the Committee whether HMG and our allies have yet found an effective way to respond to the pace of Russian decision-making. This has severely undermined the West's ability to respond effectively to Russian aggressions in the past – for example, the annexation of Crimea in 2014.[107] By contrast, the pace of the response to the Salisbury attack was impressive. However, ***: a way must be found to maintain this momentum across Government.

[107] This is, partly, a result of the inherent differences between Russian and Western political systems.

(ii) Technology and data

97. Advancements in technology and data analytics present a range of challenges for all of the organisations the Committee oversees. In relation to signals intelligence (SIGINT), increasing privacy protection – including ubiquitous encryption – presents particular problems for GCHQ, and in the case of Russia it faces a real SIGINT challenge with the use by the Russian government of ***.

98. In terms of human intelligence (HUMINT) operations, technological advancements that gather and analyse data on individuals have generally increased the difficulty ***. The expansion of smart city technology (such as CCTV, smart sensors and mobile device tracking), and the capability that this provides, has increased the ability of ***.[108] ***.

(iii) The risk of escalation

99. Covert activity against any state carries the potential for conflict, and action against a nuclear hostile state even more so given the risk of escalation into diplomatic, economic or even military conflict. The Agencies and Defence Intelligence must therefore be particularly discerning ***.

100. In the case of Russia, the potential for escalation is particularly potent: the Russian regime is paranoid about Western intelligence activities and "*is not able to treat objectively*" international condemnation of its actions.[109] It views any such moves as Western efforts to encourage internal protest and regime change. The risk is compounded by limitations on UK engagement with the Russian government at official and political levels, making deciphering Russian leadership intent even more difficult.

Rising to the challenge

(i) Focus

101. Due to the difficulty of ***, the Intelligence Community have focused their effort on *** main strategic targets, which they assess will provide insight on the most important strategic topics, with intelligence on the lowest priorities collected on an 'opportunity-only' basis. These key targets are ***.

102. ***.[110]

103. SIS told us that this means operating with "*strategic patience*" in terms of both recruiting agents and increasing staff.[111] Whilst there are a *** group of staff working on this issue, SIS was clear that a sudden surge in numbers would not yield results more quickly.[112] It is the difficulty of recruiting Russian agents with the right accesses, and the careful planning, tradecraft and operational security around any prospective agents – so as to ensure their safety

---

[108] Oral evidence – GCHQ, *** December 2018.
[109] Oral evidence – MI5, *** November 2018.
[110] Written evidence – 2018 ICE Plan requirements for Russia.
[111] Oral evidence – SIS, *** December 2018.
[112] Oral evidence – SIS, *** December 2018; we note that SIS *** and has a "*series of protections*" around the people who do go into the team.

and minimise any political risk to HMG – which means that it takes a relatively long time for intelligence efforts to produce results.

(ii) Using a range of capabilities

104. Russia is a particularly hard operating environment for other countries' intelligence officers, so ***.[113] ***.[114] As a result, HUMINT opportunities need to be sought elsewhere. This may be ***.[115]

105. Due to the difficulties in finding and operating HUMINT sources on Russia, the Intelligence Community rely on the "*bringing together of a range of intelligence disciplines*" in order to get the best possible picture of the Russian threat.[116] In relation to SIGINT, GCHQ has focused on not only deploying a broad range of capabilities against Russia, but in joining up with others to use their capabilities in tandem, allowing them to ***.

106. Defence Intelligence brings to the table a range of specialised geospatial intelligence (GEOINT) and measurement and signature intelligence (MASINT) capabilities, which can be used to observe Russian targets at a distance, with a focus on military capabilities and organisations. Defence Intelligence has sought to *** "*try to understand how they think and why they think*".[117] Defence Intelligence is also involved in the expansion of HMG's open source intelligence capabilities (i.e. the analysis of information that can be accessed freely on the internet, or bought through commercial providers) through the Defence Intelligence Open Source Hub. Analysis of open source information is being increasingly used by the Agencies and Defence Intelligence to enhance their overall situational awareness, and can be fused with a smaller proportion of secret intelligence to provide a richer picture.

(iii) Real-world threat, real-world outcomes

107. The Committee was struck by the relatively small proportion of *** work that is carried out by the Agencies in relation to Russia, compared with the intelligence coverage of Russia that is undertaken. For example, SIS usually deploys only *** of its overall operational Russia effort in support of ***, whilst GCHQ uses approximately ***.[118]

108. We were told that, since the overall cross-Whitehall Russia Strategy aim, in relation to Russia, is to develop "*a Russia that chooses to co-operate, rather than challenge or confront*", any work must be proportionate to this outcome – notably HMG does not deploy effects with the goal of effecting organisational collapse, in the way that they might be deployed against international terrorist groups, for example.[119] However, of equal concern, it appears, is the need to tread carefully so as not to provoke unexpected escalation. As a result, the Agencies' effects work primarily concentrates on ***; capability-building (the sharing of knowledge and capabilities with partners); and counter-intelligence work to disrupt *** operations.

---

[113] GCHQ and Defence Intelligence staff working on Russia are UK based.
[114] Oral evidence – SIS, *** December 2018.
[115] ***
[116] Oral evidence – Defence Intelligence, *** December 2018.
[117] Oral evidence – Defence Intelligence, *** December 2018.
[118] Oral evidence – SIS and GCHQ, *** January 2019.
[119] More information on this is included in the Strategy, Co-ordination and Tasking section of this Report.

109. We note that the focus on *** work increased significantly following the events in Salisbury as HMG *** engaged in a substantive and concerted diplomacy effort to co-ordinate a strong international response to the use of chemical weapons against civilians on UK soil.[120] This raises the question of whether return now to a 'normal', relatively low, level of *** effort against Russia would undermine this, or whether it would now be more appropriate for HMG to capitalise on its strengthened international relationships and push forward with greater emphasis on exposing Russian Hostile State Activity multilaterally; in our view it must be the latter.

[120] The international response to Salisbury is discussed in more detail in the International Partnerships section of this Report.

110. Given the difficulties inherent in seeking to counter Russian Hostile State Activity, it is essential that the Intelligence Community have the legislative powers and tools they need. However, the Home Secretary was quite clear that "*we don't have all the powers yet*".[121]

Counter-espionage

111. The current legislation enabling action against foreign spies is acknowledged to be weak. In particular, the Official Secrets Acts are out of date – crucially, it is not illegal to be a foreign agent in this country.[122] The Director-General of MI5 told us that:

> *... there are things that compellingly we must investigate, everybody would expect us to address, where there isn't actually an obvious criminal offence because of the changing shape of the threat and that for me is fundamentally where this doesn't make sense.*[123]

112. In 2017, the Law Commission ran a consultation which considered options for updating the Official Secrets Acts and replacing them with a new 'Espionage Act'. The outcome of the consultation is still awaited. In the meantime, the Prime Minister, in March 2018, asked the Home Secretary to "*consider whether there is a need for new counter-espionage powers to clamp down on the full spectrum of hostile activities of foreign agents in our country*".[124]

113. In evidence to us, the Home Secretary accepted that the Official Secrets Acts were "*completely out of date*".[125] The Director-General of MI5 echoed this, saying:

> *The purpose of* [a potential new Espionage Act] *is to be able to tighten up on the powers that have become, you know, dusty and largely ineffective since the days of the Official Secrets Act, half of which was drafted for First World War days and was about sketches of naval dockyards, etc., and then there was a 1989 ... addition to it, but we are left with something which makes it very hard these days to deal with some of the situations we are talking about today in the realm of the economic sphere, cyber, things that could be, you know, more to do with influence.*[126]

114. One specific issue that a new Espionage Act might address is individuals acting on behalf of a foreign power and seeking to obfuscate this link. The US, in 1938, introduced the US Foreign Agents Registration Act (FARA), which requires anyone other than accredited diplomats – including both US and non-US citizens – who represents the interests of foreign powers in a "*political or quasi-political capacity*" to register with the Department of Justice, disclosing their relationship with the foreign government and information about related activities and finances. Additionally, US legislation requires agents, other than diplomats, performing non-political activities under the control of foreign governments or foreign officials, to notify the Attorney General (registration under FARA serves as the requisite

[121] Oral evidence – Home Secretary, 31 January 2019.
[122] There are four separate Acts: 1911, 1920, 1939 and 1989.
[123] Oral evidence – MI5, *** February 2019.
[124] Oral evidence – Home Secretary, 31 January 2019.
[125] Oral evidence – Home Secretary, 31 January 2019.
[126] Oral evidence – MI5, *** January 2019.

notification).[127] Anyone who should have registered but who has not done so can be prosecuted and, in the case of non-US citizens, deported.

115. The UK has no equivalent legislation to FARA – which would clearly be valuable in countering Russian influence in the UK. The Director-General of MI5 explained that FARA-type legislative provisions would create:

> *... the basis therefore of being able to pursue under criminal means somebody not declaring, thereby being undercover. So if somebody was a Russian illegal, or something like that, today it is not an offence in any sense to be a covert agent of the Russian Intelligence Services in the UK – just to be that, to be in covert contact, to be pursuing a brief – unless you acquire damaging secrets and give them to your masters.*[128]

116. We note that new powers to stop, question, search or detain any person entering the UK gained Royal Assent in February 2019; it is not necessary for there to be suspicion of engagement in hostile activity in order to use these powers.[129] This is a good first step, but more than a year on from the Prime Minister's commission there is still no sign of broader legislation being brought forward. The Home Secretary explained:

> *It is, by definition, a complex area. The Law Commission has been doing work in this area as well, quite rightly independently and they will be reporting back and I think it makes sense to take into account what they have got to say as well before we rush out some legislative proposal.*[130]

117. We recognise the need to get legislation right. Nevertheless, it is very clear that the Official Secrets Act regime is not fit for purpose and the longer this goes unrectified, the longer the Intelligence Community's hands are tied. It is essential that there is a clear commitment to bring forward new legislation to replace it (and a timetable within which it will be introduced) that can be used by MI5 to defend the UK against agents of a hostile foreign power such as Russia.

Tackling crime

118. In terms of tackling the criminal activities of Russian expatriates and those who enable such activities, Unexplained Wealth Orders came into force in January 2018 through the Criminal Finances Act 2017.[131] These require an individual with unexplained wealth in assets over £50,000 to provide information as to the legitimacy of these assets. Failure to respond or comply with the order may lead to a presumption that the assets are recoverable property in any subsequent civil recovery proceedings before the High Court.

---

[127] Title 18 of the United States Code (Crimes and Criminal Procedure), paragraph 951.
[128] Oral evidence – MI5, *** January 2019.
[129] The provisions in the Counter-Terrorism and Border Security Act 2019 are closely modelled on the 'Schedule 7 port stop' power under the Terrorism Act 2000.
[130] Oral evidence – Home Secretary, 31 January 2019.
[131] Contained in the Proceeds of Crime Act 2002, as amended by the Criminal Finances Act 2017.

119. The National Crime Agency (NCA) can obtain an Unexplained Wealth Order in relation to anyone who is either a Politically Exposed Person[132] from outside the European Economic Area (EEA), someone involved in serious crime, or an individual or entity connected to such people. The Security Minister told the Committee that Unexplained Wealth Orders were acting as a deterrent:

> *We know from both intelligence and open source that people are approaching financial advisers about how to get their money out of Britain as a result of these Unexplained Wealth Orders, and I think you will see them being used more going forward.*[133]

However, the Director-General of the NCA cautioned that:

> *… unexplained wealth does have to be unexplained and, unfortunately … Russians have been investing for a long period of time … you can track back and you can see how they will make a case in court that their wealth is not unexplained, it is very clearly explained.*[134]

As a result, it appears that Unexplained Wealth Orders may not be that useful in relation to the Russian elite. Moreover, there are practical issues around their use, as the NCA explained:

> *We are, bluntly, concerned about the impact on our budget, because these are wealthy people with access to the best lawyers and the case that we have had a finding on … has been through every bit of court in the land, and I've got a very good legal team based within the National Crime Agency but they had a lot of resource dedicated out of my relatively small resource envelope on that work.*[135]

120. There appear to be similar concerns in relation to sanctions. The NCA told us that sanctions have "*a powerful impact*" on members of the Russian elite and their professional enablers, and "*provide a significant primary disruption when imposed, and also open up a range of effective secondary disruptions through sanctions evasion offences*".[136] However, the NCA also underlined that there are several ways in which the Sanctions and Anti-Money Laundering Act 2018 is too restrictive. The NCA outlined changes that it would wish to see to the legislation:

- including serious and organised crime as grounds for introducing sanctions;[137] and

---

[132] A Politically Exposed Person (PEP) is a term used in financial regulation to denote an individual who has been entrusted with a prominent public function. In the UK, this includes any foreign person who has held at any time in the preceding year a prominent public function outside the UK in a state or international institution: ambassadors; high-ranking military officers; Members of Parliament; members of the boards of central banks and members of supreme courts. PEP status also extends to relatives and close associates.
[133] Oral evidence – Security Minister, 31 January 2019.
[134] Oral evidence – NCA, 24 January 2019.
[135] Oral evidence – NCA, 24 January 2019.
[136] Written evidence – NCA, 6 November 2018.
[137] While the current sanctions regime does not encompass serious crime, it does allow for gross human rights violation as a reason for imposing sanctions on a person or entity. These provisions in the Sanctions and Anti-Money Laundering Act 2018 were introduced following the attack in Salisbury. The Proceeds of Crime Act 2002 was also amended by the Criminal Finances Act 2017 (this provision coming into force in January 2018) to expand the definition of 'unlawful conduct' to include gross human rights abuse (such that proceeds of crime, including gross human rights abuses, may be confiscated). These provisions are sometimes referred to as the UK's 'Magnitsky' legislation: the so-called US 'Magnitsky Act' was passed in 2012 in order to punish Russian officials responsible for the death of Russian tax accountant Sergei Magnitsky in a Moscow prison in 2009. This has provisions allowing the US government to act globally to freeze the assets of individual human rights offenders, and to ban them from entering the US. Since then a number of other countries, including Canada and the Baltic states, have implemented analogous legislation.

- providing for Closed Material Proceedings to protect sensitive intelligence in the granting of, and any appeal against, sanctions (the Special Immigration Appeals Commission procedures offer a useful model for this).

We note that the Foreign Secretary stated that he is "*quite enthusiastic about sanctions against individuals because we are all quite sceptical that sanctions against countries have a huge effect and they often hurt the very people that you are trying to help*".[138] We agree and strongly support the NCA's suggested amendments to the legislation.

121. The one remaining area raised with us as requiring action is in relation to the Computer Misuse Act 1990. The NCA explained:

> *The Computer Misuse Act … is very outdated legislation. It was designed for a time when we all didn't carry six phones and computers and let alone have criminals who do the same.*[139]

The Computer Misuse Act should be updated to reflect modern use of personal electronic devices.

Protecting democracy

122. The Digital, Culture, Media and Sport (DCMS) Select Committee has already asked the Government "*whether current legislation to protect the electoral process from malign interference is sufficient. Legislation should be in line with the latest technological developments*". We note that physical interference in the UK's democratic processes is less likely given the use of a paper-based system – however, we support the DCMS Select Committee's calls for the Electoral Commission to be given power to "*stop someone acting illegally in a campaign if they live outside the UK*".[140]

123. Separately, there is the question of influence over our democratic processes. Questions have been raised over whether electoral law is sufficiently up to date, given "*the move from physical billboards to online, micro-targeted political campaigning*".[141] We note – and, again, agree with the DCMS Select Committee – that "*the UK is clearly vulnerable to covert digital influence campaigns*".[142] In this respect, we have already questioned whether the Electoral Commission has sufficient powers to ensure the security of democratic processes where hostile state threats are involved; if it is to tackle foreign interference, then it must be given the necessary legislative powers.

124. We also emphasise the need to ensure that the focus is not solely on national events and bodies. It is important to include local authorities ***.[143] We were encouraged that this issue seems to have been recognised and that action is being taken.

---

[138] Oral evidence – Foreign Secretary, 7 February 2019.
[139] Oral evidence – NCA, 24 January 2019.
[140] DCMS Select Committee, *Disinformation and 'Fake News'*, HC 1791, 18 February 2019.
[141] DCMS Select Committee, *Disinformation and 'Fake News'*, HC 1791, 18 February 2019.
[142] DCMS Select Committee, *Disinformation and 'Fake News'*, HC 1791, 18 February 2019.
[143] Oral evidence – GCHQ, *** February 2019.

Working with others

125. The Intelligence Community must equip themselves to tackle the Russian threat, but we must also look beyond the UK itself. The Kremlin has shown a willingness and ability to operate globally to undermine the West, seeking out division and intimidating those who appear isolated from the international community. The West is strongest when acting in coalition, and therefore the Agencies and Defence Intelligence have a role to play in encouraging their international partners to draw together.

126. In responding to the Russian threat, the UK's long-standing partnership with the US is important. It is clear that this partnership provides valuable capabilities that *** to the UK, and avoids the duplication of coverage through effective burden-sharing. However, there remains a question as to whether ***. This is important given the relative priority of work on Russia among the Five Eyes partnership.

127. The Agencies and Defence Intelligence are increasingly working with *** on the Russian threat. Their perspectives are particularly useful: whilst UK and Western resources were diverted towards the threat from international terrorism in the early 2000s, ***. As well as providing a wealth of *** intelligence on Russia, they also share the UK's approach to the Russian threat, and have been willing to stand alongside the UK in taking an increasingly assertive approach to Russian activities.

128. Others do not share the UK's concerns about Russia – or even if they do they are not willing to take such an assertive approach towards Russia's malign activities. Whilst there appear to be increasing signs that others in Europe are taking the threat from Russia more seriously *** there has clearly been less success in translating this into building public support for the UK's diplomatic approach to attribution and condemnation of Russia's cyber activities. In particular, we note that France does not appear to have publicly condemned Russian cyber activities, and it has been widely reported that other European governments, such as Austria and Italy, have appeared publicly to move closer to the Kremlin in the last few years.[144] We also note reporting that Israel *** has welcomed Russian oligarchs and their investment, and has thus far been unwilling to challenge the Kremlin openly.[145]

129. NATO remains at the heart of strategic thought: the Kremlin considers that any further enlargement of NATO would constitute a breach of the 1997 NATO–Russia Founding Act, and an unacceptable encroachment into its perceived 'sphere of influence'. Diminishing the strength of NATO is therefore a key aim of the Kremlin, as is undermining the credibility of Article V of the 1949 North Atlantic Treaty,[146] and "*delivering NATO and non-NATO deterrence*" therefore forms a key part of the 2019 cross-Whitehall Russia Strategy.

130. We are encouraged to note that Defence Intelligence shares its intelligence assessments with NATO, which we were told aim to try "*to ensure as common an understanding of the*

[144] 'Rise of far-right in Italy and Austria gives Putin some friends in the west', *The Guardian*, 7 June 2018.
[145] 'Russian oligarchs in Israel: Welcome to the Promised Land', *The Economist*, 17 September 2015.
[146] Article V of the 1949 North Atlantic Treaty concerns the principle of 'collective self-defence', and states that an armed attack against one or more NATO Members will be considered an attack against them all, and that all NATO Members will act to repel the attack against the affected Member State(s).

nature of the Russian threat and situation that we face". Defence Intelligence highlighted several "*really important part*[s] *of how we feed into the NATO system*", including "*working very closely with NATO colleagues, putting assessments into NATO,* [and] *working very closely with the NATO Intelligence Fusion Cell at RAF Molesworth*".[147]

Helping others to help us

131. However, some partners with whom the UK might wish to work closely do not have the requisite intelligence capacity. ***.

132. In terms of its 'near abroad', Russia clearly intends keeping these countries within its 'sphere of influence', and conducts cyber activity and pursues economic policy to that end in ***. HMG initiatives *** are therefore essential. However, we note that this is not a short-term project: continuing investment and a long-term strategy are required *** against Russian influence.

The international response to Salisbury

133. Following the GRU attack in Salisbury, the UK's goal was to respond quickly, and – understanding that Russia is not overly concerned about individual reprisal – to 'internationalise' any action against Russia by building as broad a coalition as possible.[148] The UK Government (***) embarked on a diplomacy effort to provide allies with the evidence related to the attack, and to persuade them to join the UK in taking action in the form of expulsions and strengthened sanctions.

134. As mentioned previously, the resulting expulsion of 153 Russian intelligence officers and diplomats from 29 countries and NATO was an unprecedented international response.[149] Whilst the fact that chemical weapons were used – in clear breach of international law and attracting the opprobrium of the international community – was undoubtedly a factor in persuading countries to join forces with the UK, the quick and co-ordinated response from *** HMG more widely, which provided evidence and reassurance to partners, made it easier for them to join in the public condemnation.

135. This diplomatic response, and the subsequent exposure of the responsible GRU agents, sent a strong message to Russia that such actions would not be tolerated, and provides a platform for the future. We were told that:

> [Salisbury] *has changed the dynamic …* [and] *there is a growing sense amongst countries who feel threatened by Russia that there is an opportunity both through intelligence and security cooperation and at a diplomatic level to deliver real-world effects against Russia and that feels quite different. That feels like a very positive outcome from what was a crisis.*[150]

---

[147] Oral evidence – Defence Intelligence, *** January 2019.
[148] ***
[149] It presents a stark comparison with HMG's slow and isolated response to Russian aggression after the murder of Alexander Litvinenko in 2006 (despite the use of a radioactive substance in that case).
[150] Oral evidence – SIS, *** December 2018. Defence Intelligence also observed that the impact of the Salisbury attack on the NATO intelligence community had "*been significant in terms of bolstering individuals*", noting that *** (oral evidence – Defence Intelligence, *** February 2019).

We recognise the amount of effort that went into achieving this and we commend all involved for their hard work.

Maintaining momentum

136. Salisbury must not be allowed to become the high water mark in international unity over the Russia threat: coherent and sustained strategy is needed in order to build on this success, and to make sure these lessons are internalised for similar events, be they targeted towards the UK or its allies. It is clear that restraining Russian activities in the future will rely on making sure that the price the Russians pay for such interference is sufficiently high. The Intelligence Community must ensure that private collaboration supports and complements continued public exposure of Russian activities, and the building of a broad international coalition that is willing to act quickly and decisively against Russian aggression.

Is Russia seeking alliances?

137. By contrast to the West, Russia has traditionally been suspicious of building significant international partnerships. However, we note that in recent years it has been proactive in seeking 'alliances of convenience' across the world. This has included deepened defence and security co-operation with China, as a useful partner against the US (going so far as to conduct joint military exercises), increased influence in South America, and substantive engagement in several African countries, including widespread trade campaigns.[151]

138. Russia has also sought to expand its influence in the Middle East. Despite agreement that Russia's exploitation of the power vacuum in Syria was "*one of the biggest setbacks*"[152] for UK foreign policy in 2018, we still do not consider that the UK has a clear approach to this issue. Russia views its intervention in support of the Assad regime as a success, and it is clear that its presence in Syria presents the West with difficulty in supporting peace in the region. Russia's increased links with Iran, and trade initiatives with a range of countries in the Gulf area, complicate the situation further. If HMG is to contribute to peace and security in the Middle East, the Intelligence Community must ***, and the UK must have a clear strategy as to how this should be tackled.

[151] In September 2018, Russia held its 'VOSTOK 2018' military exercises jointly with Chinese and Mongolian forces.
[152] Oral evidence – Foreign Secretary, 7 February 2019.

ENGAGEMENT WITH RUSSIA

Russian disengagement

139. As we have already noted, following the end of the Cold War and dissolution of the USSR, there was a concerted effort by the West to engage Russia as a potential future partner in the Rules Based International Order. Following the election of Putin as President in 2000, the Russian government has increasingly shown itself instead to be actively hostile towards the UK and the West, and fundamentally unwilling to adhere to international laws and norms.

140. The Russian government is looking for engagement on its terms alone: paying lip-service to notions of better relations with the UK and seeking more economic co-operation, whilst flouting UK sovereignty and – in the Skripal attack – the most essential of international principles around the prohibition of chemical weapons.

The purpose of communication

141. The question is how the UK responds, and in this it is important to differentiate between public 'messaging', and 'back channels' of communication which are essential to enabling de-escalation in times of crisis.

142. Following a break in relations in 2007 after the assassination of Alexander Litvinenko, communication channels with Russia were re-opened in 2013 to allow for the exchange of information regarding the terrorist threat to the Sochi Olympics.[153] These were subsequently closed in 2014 after the Games, but re-opened in 2016 ahead of the Euro 2016 tournament and kept open in the run-up to the 2018 Football World Cup, to ensure the security of Russian citizens visiting the UK and UK citizens visiting Russia respectively. *** more proactive engagement, or relationship-building, has been frozen recently, as has planned ministerial engagement.

143. Having limited channels of communication with the Russian government can be beneficial. The ability to have direct conversations enables an understanding of the intentions of both sides in times of crisis – ***. Having such channels in place can therefore reduce the risk of miscommunication and escalation of hostilities. It can also provide opportunities to de-conflict military activities in areas where both the UK and Russia have active military presences.

Sending the right message

144. It is nevertheless striking that two out of the five 'pillars'[154] of the cross-Whitehall Russia Strategy are still focused on proactive engagement and relationship-building with Russia, beyond essential communication.[155] Whilst it is possible that an improved relationship between Russia and the UK may one day reduce the threat to the UK, it is unrealistic to think that that might happen under the current Russian leadership. It would have to be dependent on Russia ceasing its acts of aggression towards the UK, such as the use of chemical weapons

[153] ***

[154] We note, however, that these two pillars only make up a very small part of the overall action.

[155] The cross-Whitehall Russia Strategy seeks engagement with Russian civil society as well as the Russian government.

on UK soil. The UK, as a Western democracy, cannot allow Russia to flout the Rules Based International Order without there being commensurate consequences. Any public move towards a more allied relationship with Russia at present would severely undermine the strength of the international response to Salisbury, and the UK's leadership and credibility within this movement.

WITNESSES

Ministers

The Rt Hon. Jeremy Hunt MP – then Foreign Secretary

The Rt Hon. Sajid Javid MP – then Home Secretary

The Rt Hon. Ben Wallace MP – then Security Minister

Officials

CABINET OFFICE

Ms Madeleine Alessandri CMG – then Deputy National Security Adviser

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

Other officials

DEFENCE INTELLIGENCE

Lt Gen. Jim Hockenhull OBE – Chief of Defence Intelligence

Other officials

FOREIGN AND COMMONWEALTH OFFICE

Sir Philip Barton KCMG OBE – then Director-General Consular and Security, FCO, and cross-Government Senior Responsible Owner for Russia

Other officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Mr Jeremy Fleming – Director, GCHQ

Other officials

NATIONAL CRIME AGENCY

Ms Lynne Owens CBE QPM – Director-General, NCA

Other officials

OFFICE FOR SECURITY AND COUNTER-TERRORISM

Mr Tom Hurd OBE – Director-General, OSCT

Other officials

SECRET INTELLIGENCE SERVICE (MI6)

Sir Alex Younger KCMG – Chief, SIS

Other officials

SECURITY SERVICE (MI5)

Sir Andrew Parker KCB – then Director-General, Security Service

Other officials

Expert external witnesses

Professor Anne Applebaum – Institute of Global Affairs

Mr William Browder – Head of the Global Magnitsky Justice Movement

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

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

Mr Christopher Steele – Director, Orbis Business Intelligence Ltd

ANNEX

***

CLASSIFIED ORAL AND WRITTEN EVIDENCE

***

CCS0221966010
978-1-5286-1686-7