Government Response to the Intelligence and Security Committee of Parliament Report 'Russia'

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

JULY 2020

CP 275

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at publiccorrespondence@cabinetoffice.gov.uk

ISBN 978-1-5286-2092-5

CCS0720885888 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.

INTELLIGENCE AND SECURITY COMMITTEE REPORT 'RUSSIA' GOVERNMENT RESPONSE

The Government is grateful to the Intelligence and Security Committee (ISC) for their report on Russia. As the final report says, this was a major Inquiry spanning eight months and numerous evidence sessions. Both the Committee and the Government devoted considerable time and resource to it and we are grateful for the detailed report the Committee has produced. We would like to take this opportunity to thank the former Members of the Committee for their vital work over the course of the last Parliament and we look forward to working with the new Committee as they continue their independent oversight of the UK's Intelligence Community.

The Committee notes that Russia presents a serious threat to the United Kingdom. As NATO leaders agreed at their meeting in London on 3-4 December 2019, Russia's aggressive actions also constitute a threat to Euro-Atlantic security. The Government has made clear to the Kremlin that an improvement in relations is only possible if Russia desists from its attacks on the UK and its allies. Meanwhile we will be resolute in defending our country, our democracy, and our values from such Hostile State Activity.

We do this through a cross-Government Russia Strategy and structures that combine the UK's diplomatic, intelligence, and military capabilities, its hard and soft power, to maximum effect. We act in concert with our allies, seeking to lead the West's collective response to hybrid threats to our societies and values. This includes concerted campaigns to counter disinformation, as well as to bear down on illicit finance, combat influence operations, and fend off cyber-attacks.

We are grateful to the Committee for their commendation of the hard work of the community of Government officials and others who are engaged in this effort, including in mounting the UK's response to the Salisbury attack in 2018, and for its recommendations on how to sustain it going forward.

The former Committee has made a number of recommendations within the text of their report as well as drawing out some cross-cutting themes. We have not addressed each and every recommendation individually in this response, but have instead addressed the key themes which we have grouped together under the headings: cross-Government focus and strategy; defending democracy; and legislation, making reference to some specific recommendations where appropriate. For those recommendations where the Committee has requested specific updates, we will respond to those directly in the timeframes they have set out. A further, private response will be provided to the Committee in due course, on aspects of the Committee's report which are too sensitive to respond to in a published response.

CROSS-GOVERNMENT FOCUS AND STRATEGY

"[Paragraph 12] 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."

"[Paragraph 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)."

As the Committee notes, delivery of the Government's Russia Strategy is coordinated through the Government's Russia Unit, based in the Foreign and Commonwealth Office (FCO), and governance of the Strategy is led by the Russia and Ukraine National Security Implementation Group (NSIG) and kept under review by the National Security Council (NSC). Philip Barton has now been replaced by Tom Drew as Director General Consular and Security in the FCO and the cross-Government senior responsible officer for Russia.

There is a clear line of accountability for HMG's policy on Russia: the Russia and Ukraine NSIG reports to the National Security Advisor and to Ministers on the National Security Council. Ultimate ministerial oversight is provided by the Prime Minister. The Foreign Secretary retains an important role in overseeing the work of GCHQ and SIS (which is the case for all geographical areas).

Delivering the ambition of the National Cyber Security Strategy requires a whole of Government and whole of society response, as it is about both national security and economic prosperity. Implementation of the National Cyber Security Strategy is overseen by the Paymaster General, who is accountable to Parliament for the Strategy and the accompanying £1.9 billion investment. Ministerial responsibilities are clearly defined and necessarily distributed given the various departmental equities. This is brought together under the NSC, where priority activity and the balance of investment across the Strategy are agreed.

"[Paragraph 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."

"[Paragraph 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 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 that of the busy Agencies. We welcome the fact that this has now been recognised and appears to be changing."

"[Paragraph 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."

"[Paragraph 85] …It is essential that HMG takes a broader view of the full spectrum of the Russian threat as the cross-Whitehall Russia Strategy develops and the use of the Fusion Doctrine increases."

The Government has long recognised there is an enduring and significant threat posed by Russia to the UK and its allies, including conventional military capabilities, disinformation, illicit finance, influence operations, and cyber-attacks. As such, Russia remains a top national security priority for the Government. This is why in 2017 the Government implemented the NSC-endorsed Russia Strategy, and in 2017 established the cross-Government Russia Unit which brings together the UK's diplomatic, intelligence and military capabilities to maximum effect. The Government's Russia Strategy does not just respond to the here and now; it is a 30 year strategy, designed in the long-term to move from a relationship of confrontation and challenge, which currently threatens our collective security and values, to a relationship where Russia chooses to work alongside the international community. The integrated and established nature of the Strategy and the Russia Unit was paramount to the immediate nature of the effective and coherent Salisbury response. We have shown in recent years that the UK takes the threat from Russia extremely seriously and will respond to and call out Russian aggression wherever it occurs.

The Committee doubts whether the Russia Strategy has learned any direct lessons from the CONTEST strategy. However, what has been fundamental to the delivery of the Government's Russia Strategy is the application of 'fusion doctrine', which aims to deploy security, economic and influence capabilities to protect, promote and protect our national security, economic and influence interests. This approach to cross-Government coordination was an important part of the lessons learned over the last fifteen years since the London terror attacks in 2005. In particular, the NSIG structure enables decisions to be taken in consultation with a broad range of Government departments that hold a stake in the policy on Russia; and in doing so allow balanced recommendations to be made to Ministers. This is one element of 'fusion doctrine'

that the Committee's report recognises is vital to how HMG delivers policy using all available levers and the Government will continue to adopt this approach.

"[Paragraph 81] There 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 while 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."

The Government notes this recommendation and agrees with the benefits of closer join up. MI5 has already developed closer working with Police and Home Office partners in tackling the threat posed by Hostile State Activity, including working together closely on a number of Hostile State Activity cases. The Salisbury response and investigations in 2018 were led by Counter Terrorism Command, drawing on its expertise in investigating matters that pertain to national security. The Agencies continue to collaborate closely and productively with Police on all relevant Hostile State Activity cases. MI5 welcomes the Home Office's ongoing work on new legislation to counter Hostile State Activity, which will update existing criminal offences and introduce new powers to support the Police's work on Hostile State Activity.

"[Paragraph 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] experience on counter-terrorism matters to be brought to bear against the hostile state threat. We understand 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."

As the report notes, our adversaries adopt a whole of state approach to hybrid and malign activity. Tackling it therefore requires a cross-Government and cross-society response, drawing on the skills, resources and remits of different departments, agencies and non-Government organisations. Accordingly, this activity is coordinated by the Cabinet Office with individual Government departments and the Security and Intelligence Agencies playing a key role in all relevant areas. However, the NSC will keep this and all aspects of the Government's approach to Hostile State Activity under review.

"[Paragraph 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. 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."**

The Committee notes that the Russian leadership has shown to have an ability to make decisions quickly and unexpectedly, demonstrated by the annexation of Crimea in 2014 (although, as the Committee has noted, the Kremlin operates without democratic or consensus-

based decision-making structures or culture and outside the rules-based international order). The Government agrees with the Committee on the importance of being able to act decisively and with appropriate speed as was demonstrated in the response to the Salisbury attack. The structures put in place to implement the Government's Russia Strategy enable the Government to respond at pace to Russia's actions, most notably in the aftermath of the Salisbury attack in 2018. These have been maintained since.

"[Paragraph 125] The UK intelligence and security community must equip itself 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 DI have a role to play in encouraging its international partners to draw together."

"[Paragraph 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."**

"[Paragraph 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 UK intelligence and security 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."

The Government agrees with the Committee that it would be appropriate for the Government to capitalise on its strengthened international relationships and push forward with a greater emphasis on exposing Russian Hostile State Activity multilaterally.

The UK has a record of taking strong action against Russian wrongdoing and will continue to work closely with allies to fully and robustly respond to the challenges Russia presents. We are grateful for the Committee's recognition of the Government's effective response to the Salisbury attack, expelling 23 undeclared intelligence officers with support from 28 countries and NATO, who expelled a further 130 Russian diplomats. This is clear evidence that, when necessary, the UK and its allies are able to act quickly and decisively together.

Specifically the UK has worked with international partners to call out the malign influence and activities of Russia's Military Intelligence (widely known as the GRU). Eleven countries joined the UK in attributing its 'NotPetya' attack in 2018, 19 countries plus the EU and NATO joined HMG in exposing the hacker-group APT28 as the GRU in 2018, and 20 countries plus the EU (a joint statement from all 27 Member States) joined the UK in condemning the GRU's cyber-

attack on Georgia in 2020. The UK also operates at the heart of the international community's engagement on Ukraine: shaping international sanctions against Russia for its illegal annexation of Crimea; leading efforts in the UN to hold Russia to account; deepening NATO's partnership with Ukraine; and launching the Ukraine Reform Conference series.

The adoption of a cyber sanctions regime by the EU in 2019, now also enshrined in UK legislation, increases our capabilities to respond to cyber-attacks. In addition, the Foreign Secretary announced in Parliament on 6 July that HMG is launching the UK Global Human Rights sanctions regime that enables HMG to sanction individuals involved in serious human rights abuses. Among the first listings, twenty five Russian Government officials have been sanctioned for their involvement in the death of Sergey Magnitsky whilst in detention. The Sanctions and Anti-Money Laundering Act (2018) also includes relevant provisions that would allow for sanctions in the interests of national security, in the interests of international peace and security and to further a foreign policy objective of the UK government.

The Government will continue to increase our understanding of what the GRU is doing against the UK and our allies, to shine a light on their activities, to expose their methods and share these with our allies. We will deploy the full range of tools to counter the threat posed by the GRU and we will be working closely with our allies to defend ourselves.

"[Paragraph 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 has been "*one of the biggest setbacks*" 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 and security community must * and the UK must have a clear strategy as to how this should be tackled."**

As the Committee notes, Russia has significantly increased its presence in the Middle East as a consequence of its intervention in the ongoing Syrian conflict. We have been clear that Russia must use its influence to persuade the Assad regime to end its military campaign and engage in a meaningful political process. In addition, the UK has called on Russia to use its relationship with the Iranian government to ensure Iran complies with its obligations under the Joint Comprehensive Plan of Action (JPCOA) and end its malign activity in the region.

"[Paragraph 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."**

The Committee notes that two of the five strategy pillars concern 'proactive engagement and relationship-building', both with the Russian Government and the Russian people. Official channels for dialogue are necessary for the national security reasons set out in the Committee's report, as well as to engage Russia on matters of international security as fellow P5 members. The Prime Minister met President Putin in January 2020 at the Libya conference in Berlin. The Foreign Secretary spoke to his counterpart Foreign Minister Lavrov in May regarding Syria and Ukraine. Senior officials meet regularly on bilateral and international issues.

The Government has also fostered cultural and educational links with Russia, and sustained support for human rights defenders and other civil society actors who are under increased pressure from the Russian authorities.

DEFENDING UK DEMOCRACY FROM FOREIGN INTERFERENCE

"[Paragraph 33] Protecting our democratic discourse and processes from hostile foreign interference is a central responsibility of Government, and should be a ministerial priority."

The UK's free and open democracy is one of our nation's greatest strengths. However, we know that certain states seek to exploit our open system to sow division and undermine trust in our democracy, and those of our allies, through disinformation, cyber-attacks and other methods. We have made clear that any foreign interference in the UK's Democratic processes is completely unacceptable. It is, and always will be, an absolute priority to protect the UK against foreign interference, whether from Russia or any other state.

We have worked with industry, civil society and international partners to implement robust systems to secure our Democratic processes and deter attempts to interfere in it. This work is undertaken with the utmost regard for the freedom of the press, political and parliamentary discourse and freedom of speech. We will always balance the need to secure our Democracy with our duty to uphold our values.

Protecting UK democratic processes

Since the Committee took evidence in January 2019, the Government has established the Defending Democracy programme, strengthened cross-Government counter disinformation capability and established frameworks to counter state sponsored influence campaigns, and oversee election security. The Cabinet Office established the Defending Democracy programme to bring together our work to safeguard our democratic processes and to make sure that our democracy remains safe and inclusive, now and into the future. The Programme was formally announced in July 2019. It brings together capabilities and expertise from Government departments, the Security and Intelligence Agencies and civil society to ensure UK democracy remains open and vibrant as well as secure. Given the cross cutting nature of

this task, the Minister for the Cabinet Office, supported by Cabinet Office Officials, coordinates work to secure UK Democracy. The programme has four priorities:

- **Protect** and secure UK democratic processes, systems and institutions from interference, including from cyber, personnel and physical threats.
- **Strengthen** the integrity of UK elections.
- Encourage **Respect** for open, fair and safe democratic participation.
- **Promote** fact-based and open discourse, including online.

Through the "Protect" elements of the programme, we have taken steps to ensure our institutions and core electoral mechanics are secured against interference, including information operations and direct attacks on electoral infrastructure. Cabinet Office, the National Cyber Security Centre (NCSC, a part of GCHQ) and the Centre for the Protection of National Infrastructure (CPNI) continue to work closely with Political Parties and Government departments as well as local and devolved Government to update and disseminate security advice and raise awareness of threats, including foreign interference.

During the May 2019 European Elections and the December 2019 General Election, we stood up a cross-Government election security cell to monitor and respond to emerging issues during election periods. This brought together staff from Government departments and agencies to share information and coordinate responses to threats and hazards relating to the election, from severe weather through to foreign interference.

During the UK General Election 2019, and as part of their ongoing work, CPNI and NCSC provided cyber and protective security guidance for local authorities and political parties as well as individuals such as candidates. The NCSC meets regularly with the UK's Parliamentary Parties, and works closely with those responsible for core parts of the UK's electoral infrastructure such as the Cabinet Office's 'Register to Vote' service. This work was prioritised during the pre-election period.

The use of NCSC's network reporting service, by local authorities and the UK's Parliamentary Parties, enables greater understanding of both security vulnerabilities and threats affecting electoral infrastructure and campaigns. NCSC responded to several incidents during the 2019 General Election including distributed denial of service attacks against political parties, and suspicious emails received by candidates.

"[Paragraph 12] 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 momentum is not lost."

"[Paragraph 20] … When attacks can be traced back – and we accept that this is in itself resource-intensive – Government must always consider 'naming and shaming.'"

"[Paragraph 25] …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."

"[Paragraph 26] … 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 DPRK). 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."

The UK Government has been at the forefront of demonstrating that there are consequences including through public attribution, co-ordinating use of existing deterrence tools and working to put in place new tools such as EU and UK cyber sanctions regimes. We have set out clearly how international law and norms of responsible state behaviour apply in cyber space. We and our allies will continue to expose those that aim to do us and our institutions harm. No longer can they act with impunity in the shadows. We will continue to do so where we believe it is in the best interests of the UK to do so. Sometimes this is in public, sometimes we have private conversations with the country concerned. We consider ever case on its merits.

As cyber space is essentially borderless, our response needs to be international – it is a foreign policy issue as much as a technical one. Working with international partners to deter and publicly expose those states, including Russia, responsible for malicious cyber activity has been a core component of the government's work as set out in the 2016 National Cyber Security Strategy. Over the last four year, the UK has played a leading role internationally in developing a co-ordinated approach to cyber deterrence, sharing our own cyber deterrence toolkit with over twenty countries and holding workshops on how to politically attribute and use all the tools of government to respond to state-directed malicious cyber activity. This work has included China, Iran and DPRK – the Government has made political statements publicly exposing the role of actors from all three countries in carrying out malicious cyber activity, as well as raising concerns directly with countries in private and increasing awareness of the threat with international partners.

On 16 July, the Foreign Secretary, supported by the US and Canada, publicly exposed that the Russian Intelligence Services are collecting information on vaccine development and research into the COVID-19 virus.

The Committee will also be aware that following extensive analysis, the Government has concluded that it is almost certain that Russian actors sought to interfere in the 2019 General Election through the online amplification of illicitly acquired and leaked Government documents.

Whilst there is no evidence of a broad spectrum Russian campaign against the election, any attempt to interfere in our democratic processes is completely unacceptable. There is an ongoing criminal investigation and it would be inappropriate for us to say anything further at this point.

"[Paragraph 122] The Digital, Culture, Media and Sport 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*"."

"[Paragraph 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*". We note – and, again, agree with the DCMS Select Committee – that "*the UK is clearly vulnerable to covert digital influence campaigns*". 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."

"[Paragraph 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, *. We were encouraged that this issue seems to have been recognised and that action is being taken."**

Through the 'Strengthen' pillar of the Defending Democracy programme the Government is reinforcing the overall integrity of our electoral processes by increasing transparency in digital campaigning, in line with the Committee's recommendation. In summer 2019, the Government announced that it will implement an imprints regime for digital election material. This will ensure greater transparency and make it clearer to the electorate who has produced and promoted online political materials.

The Cabinet Office is working closely with the Department for Digital, Culture, Media and Sport (DCMS) and other stakeholders to confirm the details of how such regulations will be put in place. The Government is planning to bring forward the technical proposals on the regime and further detail will be announced in due course.

The Government notes the Committee's comments on the Electoral Commission and we continue to consider the recommendations from the Electoral Commission itself to enhance their powers. The Commission has civil sanctioning powers that apply to referendums and elections. More serious criminal matters can and are referred to the police, and then considered by a court of law. The courts have the power to levy unlimited fines. We must ensure that regulation is proportionate. Political parties vary considerably in size and professionalism and it is important to ensure that regulation of them is fair and proportionate so as not to undermine local democracy or discourage engagement.

Disinformation

"[Paragraph 37] The aim [*of the Government's Defending Democracy programme*] 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 only signed off by the National Security Council 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."

The Government's aim is to reduce the potential impact of disinformation on UK democracy, society, economic and national security interests, in line with our democratic values. While the Cabinet Office leads the 'Defending Democracy' programme, it is clear that the threat posed by disinformation is not to democratic principles alone, as evidenced by COVID-19 disinformation.

DCMS holds the lead responsibility for the Government's overall counter-disinformation policy, including setting the direction, focus and principles of domestic policy; leading the Government's engagement with social media companies and the media; working with external partners in industry, academia, and civil society to further the aims of the strategy; and representing and promoting our domestic approach amongst our international partners and the public. The department is uniquely positioned to consider the cross-cutting threats to the information environment. While Hostile State Activity from states such as Russia poses a significant threat, there are a range of other malign actors the UK must tackle.

Since evidence was provided to the Committee by DCMS in January 2019, the department has taken a number of steps to progress the Government's policy and operational response to address this important issue. Over the last year, DCMS has introduced robust structures for the Government's counter-disinformation operational response. This includes the establishment of a cross-Whitehall Counter-Disinformation Unit (CDU), which brings together cross-Government capabilities, including monitoring, analysis and strategic communications with teams from DCMS, the Home Office, the FCO and the Cabinet Office providing a comprehensive picture of the extent, scope and potential impact of disinformation.

The CDU previously stood up in support of the European Parliamentary and General Elections in 2019, and has been contributing to the Government's COVID-19 response. COVID-19 disinformation (and misinformation; i.e. the inadvertent sharing of false information) has presented a sustained and evolving threat to the information environment. Given the range of poor quality and potentially harmful information that we have seen in relation to the pandemic, the COVID-19 response has reaffirmed the need to take an actor-agnostic approach. It is vitally important that at this or any other time of increased vulnerability, the public has accurate information.

Through the world-leading Online Harms framework, DCMS is developing potential regulatory and non-regulatory interventions to help make the UK the safest place to be online. The Online Harms framework will establish a new duty of care on companies which will require them to put appropriate systems and processes in place to improve the safety of their users. The regulation will establish differentiated expectations on companies for illegal content and activity, versus conduct that may not be illegal but has the potential to cause harm to individuals. Companies will be able to determine what type of legal content or behaviour is acceptable on their services, and will need to set this out clearly in their terms and conditions and enforce these effectively, consistently and transparently. Alongside the proposed regulatory framework, we are committed to implementing a number of non-legislative measures in order to ensure a holistic response to online harms, including a media literacy strategy, to be published later this year, which will support users to spot risks and think critically about the content they see online.

Engaging with Content Service Providers

"[Paragraph 35] …The Government must now seek to establish a protocol with the social media providers 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."

We recognise that one of the most important levers to tackle disinformation and other forms of online manipulation is through building strong relationships with the social media companies to ensure that appropriate action is being taken to address issues on their platforms. As the departmental lead for Digital policy, DCMS leads these relationships.

Through the DCMS-led CDU, the Government has established strong relationships with the companies, and have been given access to accelerated reporting portals. This allows the Government to quickly identify content which is in breach of platform terms and conditions, to ensure that platforms can take appropriate action such as removal of content or suspension of accounts.

In addition, the Home Office already works closely with social media companies to prevent terrorist use of the internet. In 2010, the Government set up the police Counter-Terrorism Internet Referral Unit (CTIRU), based in the Metropolitan Police. To date, in excess of 310,000 individual pieces of terrorist content referred by CTIRU have been removed by companies and the Unit has also informed the design of the EU Internet Referral Unit based at Europol. The Government has pressed companies to increase the use of technology to automate the detection and removal of content where possible. The Government is also working in partnership with UK Data Science companies to develop technical solutions to aid in quicker detection and

removal of terrorist content and offer these free of charge, to enable companies to take quicker action on terrorist content.

The Government's relationship with the social media companies continues to evolve. In the context of the COVID-19 response, we are learning valuable lessons which will be applied to our future approach to countering disinformation and other forms of online manipulation. While the Government welcomes the actions taken by social media companies thus far, including the cooperation they have shown in tackling these issues together, there still issues to be addressed. DCMS will continue pushing platforms to take the actions necessary to improve and safeguard the information environment.

"[Paragraph 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 their recommendation that all online political adverts should include an imprint stating who is paying for it. We would add to that a requirement for social media providers to cooperate with MI5 where it is suspected that a hostile foreign state may be covertly running a campaign."

The Government remains committed to ensuring elections and campaigning rules are fit for the modern age. Following the 2019 General election, we are considering how best to take forward our work in this area. Further details will be announced in due course.

Government has committed to increasing transparency over who is promoting material online. This will be addressed as part of our proposed digital imprints regime. Through new imprints on digital election material, we will strengthen trust and ensure people are informed about who is behind online election material. We will continue to strive to uphold transparency in the digital campaigning framework. The Cabinet Office is taking forward work in this area.

As set our above, DCMS is working closely with the social media companies to ensure that there are appropriate systems in place to quickly identify and respond to manipulative behaviour on their platforms.

UK elections and EU Referendum

"[Paragraph 47] …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 and security community should produce an analogous assessment of potential Russian interference in the EU referendum and that an unclassified summary of it be published."

We have seen no evidence of successful interference in the EU Referendum.

The Intelligence and Security Agencies produce and contribute to regular assessments of the threat posed by Hostile State Activity, including around potential interference in UK democratic processes. We keep such assessments under review and, where necessary, update

them in response to new intelligence, including during democratic events such as elections and referendums. Where new information emerges, the Government will always consider the most appropriate use of any intelligence it develops or receives, including whether it is appropriate to make this public. Given this long standing approach, a retrospective assessment of the EU Referendum is not necessary.

Illicit Finance

"[Paragraph 49] …The UK welcomed Russian money, and few questions – if any – were asked, regarding 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."

"[Paragraph 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'. […] 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."

"[Paragraph 53] … 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."**

The Government is clear that tackling illicit finance and driving dirty money and money launderers out of the UK is a priority. The UK has one of the world's largest and most open economies. These factors make the UK attractive for legitimate business, but also expose the UK to money laundering risks. The Financial Action Task Force praised the UK as a "global leader in promoting corporate transparency" with a "comprehensive legal framework", and that the UK "aggressively identifies, pursues and prioritises money laundering investigations and prosecutions". However, we are not complacent and we will ensure the full weight of law enforcement bears down on dirty money. In recent years through ground-breaking legislation such as the Criminal Finances Act 2017, the Government has introduced new powers and tools making it easier to seize criminals' money from bank accounts with billions taken from criminals, set up the National Economic Crime Centre within the National Crime Agency (NCA), expanded civil recovery powers, led the world on introducing public registers of beneficial ownership of companies and, crucially, we have ramped up law enforcement capabilities to specifically tackle illicit finance with over £48 million funding in 2019 to 2020.

Post Salisbury, the Government made its intentions clear that we will crack down on dirty money in the UK. Led by the NCA, we continue to bring the full capabilities of law enforcement to bear against serious criminals, corrupt elites, and their assets. The Foreign Secretary reaffirmed this stance when he announced the UK's new Global Human Rights

sanctions, which will target those individuals involved in human rights abuses, be they linked to the state or not, who seek to siphon dirty money through British banks or other financial institutions.

"[Paragraph 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 Registry 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."

The Government agrees that the transparency of information about political donations is important. The rules on registration and declaration of donations received by Members of the House of Lords are set out in the Code of Conduct for Members of the House of Lords and the Guide to the Code, which also incorporates the rules surrounding bullying, harassment and sexual misconduct. The Code is the responsibility of the House itself. It is kept under regular review by the Conduct Committee; a committee made up of 5 Members of the House of Lords and 4 lay members. The Government is confident that the Conduct Committee with give due consideration to the recommendations.

LEGISLATION

"[Paragraph 12] The clearest requirement for immediate action is for new legislation: the intelligence and security community must be given the tools they need and be put in the best possible position if they are 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."

"[Paragraph 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 security and 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."

The Government is grateful for the Committee's recommendations on legislation to counter hostile activity by foreign states. The Government committed in the December 2019 Queen's

Speech to introduce legislation to provide the security services and law enforcement agencies with the tools they need to disrupt this hostile activity. The Home Office leads on this and is considering several measures for introduction via new primary legislation to make the UK a harder environment for adversaries to operate in.

The Law Commission is currently reviewing the Official Secrets Acts (OSAs) as part of their report on the Protection of Official Data. The OSAs are the only pieces of UK legislation that currently exist to specifically address hostile activity by foreign states, other than the ports stop power the Government introduced in the Counter-Terrorism and Border Security Act 2019. The Government will carefully consider the recommendations for reform post publication.

In terms of Foreign Agent Registration, the Home Office is considering like-minded international partners' legislation as part of its ongoing work on new legislative proposals to identify the benefits for adopting a similar approach in the UK.

The Committee will be kept up to date on the Government's proposals for new legislation to counter hostile activity by foreign states.

The Government is also considering legislation which, when implemented, would strengthen the UK's defences against illicit finance in general, and not specifically in relation to Russian elites. This includes reforms to strengthen the powers of Companies House; to the law governing Limited Partnerships, to make them less open to abuse in money laundering; as well as to establish a register of beneficial ownership information of foreign companies owning UK property.

"[Paragraph 121] …The Computer Misuse Act should be updated to reflect modern use of personal electronic devices."

The Computer Misuse Act (CMA) has undergone several amendments to ensure it keeps pace with the evolving threat, including most recently in 2015. The Home Office keeps the CMA under regular review to determine any potential benefits and drawbacks of legislative change, including through engagement with the cyber security sector.

"**[Paragraph 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*". 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 they would wish to see to the legislation**

- **including serious and organised crime as grounds for introducing sanctions; and**
- **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*." We agree and strongly support NCA's suggested amendments to the legislation."

As mentioned in our response to paragraphs 125, 132 and 136 above, the Government has introduced new legislation – the UK Global Human Rights sanctions regime – that enables the UK to sanction individuals for serious human rights abuses. Among the first listings, twenty five Russian Government officials have been sanctioned for their involvement in the death of Sergey Magnitsky whilst in detention. The Sanctions and Anti-Money Laundering Act (2018) also includes relevant provisions that would allow for sanctions in the interests of national security, in the interests of international peace and security and to further a foreign policy objective of the Government.

CCS0720885888

978-1-5286-2092-5