Ausschuss für Nachrichtendienste und Sicherheit des Parlaments

Russland

HC 632

Nachrichtendienst- und Sicherheitsausschuss des Parlaments

Russland

Dem Parlament gemäß Abschnitt 3 des Justiz- und Sicherheitsgesetzes von 2013 vorgelegt

Auf Anordnung des Unterhauses am 21. Juli 2020 gedruckt

HC 632

Anfragen zu dieser Veröffentlichung richten Sie bitte über unser Webformular an isc.independent.gov.uk/contact

Diese Veröffentlichung ist auch auf unserer Website unter isc.independent.gov.uk

verfügbar. ISBN 978-1-5286-1686-7

CCS1019402408 07/20

Gedruckt auf Papier mit einem Recyclinganteil von mindestens 75 %.

Gedruckt im Vereinigten Königreich von der APS Group im Auftrag des Controllers of Her Majesty’s Stationery Office

DER AUSSCHUSS FÜR NACHRICHTENDIENSTE UND SICHERHEIT DES PARLAMENTS

Dr. Julian Lewis, MP (Vorsitzender) *Chris Grayling, MP*
Der Abgeordnete Kevan Jones
Der Abgeordnete Sir John Hayes CBE
Mark Pritchard, MP
Stewart Hosie, MP
Die sehr geehrte Theresa Villiers, MP
Dame Diana Johnson, DBE, MP
Der sehr geehrte Admiral Lord West of Spithead GCB DSC

Dieser Bericht ist das Ergebnis einer Untersuchung, die vom vorherigen Ausschuss durchgeführt wurde, der von November 2017 bis November 2019 tagte:

Der Abgeordnete Dominic Grieve QC (Vorsitzender)
Der Abgeordnete Richard Benyon
Der sehr geehrte Lord Janvrin GCB GCVO QSO
Die sehr geehrte Caroline Flint MP
Der sehr geehrte Kevan Jones MP
Der sehr geehrte David Hanson MP
Der sehr ehrenwerte Marquess of Lothian QC PC
Stewart Hosie MP
Der sehr geehrte Keith Simpson, Mitglied des britischen Parlaments

Der Geheimdienst- und Sicherheitsausschuss des Parlaments (ISC) ist ein gesetzlich vorgeschriebener Ausschuss des Parlaments, der für die Aufsicht über die britischen Geheimdienste zuständig ist. Der Ausschuss wurde ursprünglich durch den Intelligence Services Act 1994 eingerichtet und durch den Justice and Security Act 2013 reformiert und in seinen Befugnissen gestärkt.

Der Ausschuss überwacht die nachrichtendienstlichen und sicherheitspolitischen Aktivitäten der britischen Nachrichtendienste, einschließlich der Politik, Ausgaben, Verwaltung und Operationen des MI5 (Sicherheitsdienst), des MI6 (Geheimdienst oder SIS) und des GCHQ (Government Communications Headquarters)* sowie die Arbeit der Joint Intelligence Organisation (JIO) und des National Security Secretariat (NSS) im Kabinettsamt; des Verteidigungsnachrichtendienstes (DI) im Verteidigungsministerium und des Amtes für Sicherheit und Terrorismusbekämpfung (OSCT) im Innenministerium.

Der Ausschuss besteht aus neun Mitgliedern, die aus beiden Kammern des Parlaments stammen. Die Mitglieder werden vom Parlament ernannt, nachdem sie vom Premierminister in Absprache mit dem Oppositionsführer nominiert wurden. Der Vorsitzende des Ausschusses wird von dessen Mitgliedern gewählt.

Die Mitglieder des Ausschusses unterliegen Abschnitt 1(1)(b) des Gesetzes über Staatsgeheimnisse von 1989 und erhalten im Rahmen ihrer Tätigkeit regelmäßig Zugang zu streng geheimen Informationen. Der Ausschuss legt seine eigene Tagesordnung und sein Arbeitsprogramm fest und hört bei Bedarf Regierungsminister, die Leiter der Nachrichten- und Sicherheitsdienste, hochrangige Beamte, Experten und Wissenschaftler an. Seine Untersuchungen konzentrieren sich in der Regel auf aktuelle Ereignisse und Themen von Interesse und befassen sich daher vor allem mit operativen und politischen Fragen, während seine Jahresberichte sich mit Verwaltungs- und Finanzfragen befassen.

Die Berichte können streng geheimes Material enthalten, dessen Veröffentlichung die operativen Fähigkeiten der Geheimdienste beeinträchtigen würde. Daher gibt es einen gut etablierten und langwierigen Prozess, um die Berichte des Ausschusses für die Veröffentlichung vorzubereiten. Der Bericht wird überprüft, um sicherzustellen, dass er sachlich korrekt ist (d. h., dass die Fakten und Zahlen in einem sich schnell verändernden Umfeld auf dem neuesten Stand sind). Die Geheimdienstgemeinschaft kann dann im Namen des Premierministers die Schwärzung von Material im Bericht beantragen, wenn sie der Ansicht ist, dass

dass die Veröffentlichung ihrer Arbeit schaden würde, beispielsweise durch die Offenlegung ihrer Ziele, Methoden, Quellen oder operativen Fähigkeiten. Der Ausschuss verlangt von den Nachrichtendiensten einen klaren Nachweis dafür, inwiefern die Veröffentlichung des betreffenden Materials schädlich wäre, da der Ausschuss darauf bedacht ist, dass nur ein Minimum an Text aus einem Bericht geschwärzt wird. Lehnt der Ausschuss einen Antrag auf Schwärzung von Material ab und ist die Organisation der Ansicht, dass die Veröffentlichung des Materials die nationale Sicherheit ernsthaft gefährden würde, muss der Leiter dieser Organisation vor dem Ausschuss erscheinen, um den Fall zu vertreten. Nach Abschluss dieser Schritte wird der Bericht dem Premierminister zur Prüfung vorgelegt. Gemäß dem Justiz- und Sicherheitsgesetz von 2013 kann der Ausschuss seine Berichte erst dann dem Parlament vorlegen, wenn der Premierminister bestätigt hat, dass sie keine Informationen enthalten, die die Erfüllung der Aufgaben der Behörden beeinträchtigen würden, oder – wenn der Premierminister der Ansicht ist, dass der Bericht solche Informationen enthält – wenn der Premierminister den Ausschuss konsultiert hat und dieser die betreffenden Informationen aus dem Bericht entfernt hat.

Der Ausschuss hält es für wichtig, dass das Parlament und die Öffentlichkeit sehen können, wo Informationen geschwärzt werden mussten: Schwärzungen sind im Bericht durch *** deutlich gekennzeichnet. Das bedeutet, dass der veröffentlichte Bericht mit der vertraulichen Fassung, die dem Premierminister übermittelt wurde, identisch ist (abgesehen von den Schwärzungen).

INHALT

EINLEITUNG **1**
Was will Russland? 1
Warum Großbritannien? 2
Der Bericht 2

Die Bedrohung

CYBER **5**
Ein raffinierter Akteur 5
Führend bei der Reaktion 6
Attribution: ein neuer Ansatz 6
HMG als Akteur: Offensive Cyber 7
Internationale Maßnahmen 7

DESINFORMATION UND BEEINFLUSSUNG **9**
Ein „heißes Eisen“ 10
Das Programm „Defending Democracy“ 11
Politische Werbung in sozialen Medien 12
Fallstudie: Das EU-Referendum 12

RUSSLANDISCHE AUSWANDERER **15**
Oligarchen mit offenen Armen empfangen 15
Der Versuch, das Scheunentor zu schließen 16
Russland in Gefahr 17

Die Reaktion

VERTEILUNG DER ANSTRENGUNGEN **19**
Berichterstattung 19
Hat die britische Regierung den Blick für das Wesentliche verloren? 21
Zukünftige Ressourcen 23

STRATEGIE, KOORDINATION UND AUFGABENVERTEILUNG **25**
Die Russland-Strategie der britischen Regierung 25
Ministerielle Verantwortung 25
Die Fusionsdoktrin und die gemeinsame Arbeit 26
Die Beiträge der Nachrichtendienste zur Russland-Strategie 26
Weniger reden, mehr handeln? 27
Leistungsmessung 27

EIN SCHWIERIGES ZIEL **29**
Eine einzigartige Herausforderung 29
Die Herausforderung meistern 30

GESETZGEBUNG **33**
Spionageabwehr 33
Bekämpfung von Kriminalität 34
Schutz der Demokratie 36

INTERNATIONALE PARTNERSCHAFTEN **37**
Zusammenarbeit mit anderen 37
Anderen helfen, uns zu helfen 38
Die internationale Reaktion auf Salisbury 38
Die Dynamik aufrechterhalten 39

Strebt Russland Allianzen an?....39

ENGAGEMENT MIT RUSSLAND....41
Russlands Rückzug....41
Zweck der Kommunikation....41
Die richtige Botschaft senden....41

ZEUGEN....43

ANHANG....45

GEHEIME MÜNDLICHE UND SCHRIFTLICHE BEWEISE....47

EINLEITUNG

1. Die Auflösung der UdSSR war für den Westen eine Zeit der Hoffnung. In den 1990er und frühen 2000er Jahren ging es im Westen darum, Russland, wenn schon nicht vollständig zu integrieren, so doch zumindest zu einem Partner zu machen. Mitte der 2000er Jahre war klar, dass dies nicht gelungen war. Die Ermordung von Alexander Litwinenko im Jahr 2006 zeigte, dass Russland unter Präsident Putin sich von einem potenziellen Partner zu einer etablierten Bedrohung gewandelt hatte. Seitdem gab es eine Reihe von Versuchen, die Beziehungen zwischen den westlichen Ländern und Russland wiederherzustellen (zum Beispiel der „Russian Reset" der USA im Jahr 2009 und der Besuch des Premierministers in Moskau im Jahr 2011, bei dem er den Wunsch zum Ausdruck brachte, die Beziehungen wieder aufzubauen), aber die Ereignisse der letzten Jahre zeigen, dass keiner dieser Versuche einen Einfluss auf die Absichten Russlands und damit auf die von Russland ausgehende Sicherheitsbedrohung hatte.

2. Russland ist gleichzeitig sehr stark und sehr schwach. Die Stärken, die Russland noch hat, sind größtenteils ein Erbe der UdSSR und seines Status als Sieger des Zweiten Weltkriegs: Atomwaffen, eine Präsenz in der Raumfahrt und ein ständiger Sitz im UN-Sicherheitsrat. Demgegenüber steht eine im Vergleich zum Westen geringe Bevölkerungszahl, ein Mangel an verlässlichen Partnern und kulturellem Einfluss außerhalb der Länder der ehemaligen UdSSR, ein Mangel an starken öffentlichen und demokratischen Institutionen, einschließlich Rechtsstaatlichkeit, und natürlich eine schwache Wirtschaft.

3. Trotz seiner wirtschaftlichen Schwäche stellt es dennoch erhebliche Ressourcen für seine Geheimdienste und Streitkräfte bereit, die unverhältnismäßig groß und mächtig sind. Darüber hinaus versteht es Russland, seine offensichtlichen Schwächen zu seinem Vorteil zu nutzen: So scheinen beispielsweise sein schlechtes nationales Image und der Mangel an langfristigen globalen Freunden seine enorme Risikobereitschaft zu fördern – vielleicht auf der Grundlage, dass es glaubt, nichts zu verlieren zu haben. Der Mangel an Demokratie und Rechtsstaatlichkeit ermöglicht es seinen Geheimdiensten, schnell, ohne Einschränkungen oder Rücksichtnahmen zu handeln. Das Fehlen starker unabhängiger öffentlicher Einrichtungen und die Verschmelzung von Regierung und Wirtschaft ermöglichen es ihm, seine gesamte nachrichtendienstliche, militärische und wirtschaftliche Macht gleichzeitig einzusetzen, um eine allumfassende Sicherheitsbedrohung darzustellen.

Was will Russland ?

4. Die von Russland ausgehende Sicherheitsbedrohung ist für den Westen schwer zu bewältigen, da sie unserer Ansicht nach und nach Ansicht vieler anderer grundlegend nihilistisch erscheint. Russland scheint Außenpolitik als Nullsummenspiel zu betrachten: Jede Maßnahme, die dem Westen schadet, ist grundsätzlich gut für Russland. Dies scheint auch durch Paranoia genährt zu werden, da Russland glaubt, dass westliche Institutionen wie die NATO und die EU ihm gegenüber eine weitaus aggressivere Haltung einnehmen, als dies in Wirklichkeit der Fall ist. Es besteht auch der Eindruck, dass Russland glaubt, eine undemokratische Weltordnung nach dem Prinzip „Macht geht vor Recht" spiele seinen Stärken in die Hände, was es dazu veranlasst, die regelbasierte internationale Ordnung zu untergraben – während es dennoch von seiner Mitgliedschaft in internationalen politischen und wirtschaftlichen Institutionen profitiert.

5. Die eigentlichen Ziele Russlands sind jedoch relativ begrenzt: Es möchte als wiedererstarkte „Großmacht" wahrgenommen werden – insbesondere als dominierende Macht über die Länder der ehemaligen UdSSR – und sicherstellen, dass die privilegierte Position seiner Führungsclique nicht beschädigt wird.

Warum das Vereinigte Königreich „ “?

6. Es scheint, dass Russland das Vereinigte Königreich als eines seiner wichtigsten westlichen Geheimdienstziele betrachtet: Auch wenn wir möglicherweise nicht das Ausmaß und die Art der Bedrohung erleben, unter der die an Russland angrenzenden Länder leiden, deuten Zeugenaussagen darauf hin, dass wir in jeder Prioritätenliste direkt hinter den USA und der NATO stehen würden. Dies hängt wahrscheinlich mit den engen Beziehungen des Vereinigten Königreichs zu den USA zusammen und mit der Tatsache, dass das Vereinigte Königreich als zentraler Akteur der westlichen antirussischen Lobby angesehen wird. [1]

7. Diese Wahrnehmung dürfte durch die entschlossene Haltung Großbritanniens angesichts der jüngsten Aggressionen Russlands noch verstärkt worden sein: Nach der von Großbritannien angeführten internationalen Reaktion auf den Anschlag von Salisbury – in deren Folge 153 russische Geheimdienstmitarbeiter und Diplomaten aus 29 Ländern und der NATO ausgewiesen wurden – scheint Putin nach Ansicht des Ausschusses Großbritannien als einen wichtigen diplomatischen Gegner zu betrachten. Die Bedrohung für das Vereinigte Königreich – und etwaige Änderungen dieser Bedrohung nach den Maßnahmen, die als Reaktion auf den Anschlag von Salisbury ergriffen wurden – werden in diesem Bericht beschrieben, zusammen mit den Maßnahmen, die die britischen Geheimdienste zur Abwehr dieser Bedrohungen ergreifen. [2]

Der Bericht „ ”

8. Es handelte sich um eine umfangreiche Untersuchung, die sich über acht Monate erstreckte und neben einer Vielzahl schriftlicher Beweise auch eine Reihe von Anhörungen mit einer Vielzahl von Zeugen umfasste. Wir sind den Personen außerhalb der Geheimdienstgemeinschaft – insbesondere Anne Applebaum, William Browder, Christopher Donnelly, Edward Lucas und Christopher Steele – dankbar, dass sie uns freiwillig ihr umfangreiches Fachwissen über Russland zur Verfügung gestellt haben, das uns eine unschätzbare Grundlage für die geheimen Anhörungen bot.

9. Wir möchten auch dem verstorbenen Sir Charles Farr, der während eines Großteils unserer Untersuchung Vorsitzender des Gemeinsamen Geheimdienstausschusses war, unseren besonderen Dank aussprechen. Die von ihm direkt vorgelegten Beweise und seine umfassende Unterstützung bei der Durchführung unserer Untersuchung waren sehr hilfreich. Wir möchten diese Gelegenheit nutzen, um ihm für sein lebenslanges außergewöhnliches Engagement für die Geheimdienstgemeinschaft unsere Anerkennung auszusprechen.

10. Die von unserer Untersuchung behandelten Themen sind äußerst sensibel. Uns wurde wiederholt mitgeteilt, dass die russischen Geheimdienste alles analysieren werden, was wir öffentlich machen, und daher war in diesem Bereich mehr als in jedem anderen die Gefahr, die Fähigkeiten der Geheimdienste, Sicherheitsbehörden und des Militärgeheimdienstes zu beeinträchtigen, sowohl real als auch erheblich. Es war daher klar, dass jeder Bericht umfangreichen Schwärzungen unterzogen werden müsste und Gefahr lief, unlesbar zu werden. Um überhaupt einen Bericht veröffentlichen zu können, haben wir uns daher entschlossen, einen kürzeren Bericht als üblich zu erstellen, der in Form einer Zusammenfassung der wichtigsten Punkte, die wir während der Untersuchung festgestellt haben, auf hoher Ebene verfasst ist, ohne die zugrunde liegenden Details preiszugeben. Wir haben diesen Bericht durch einen umfangreichen Anhang ergänzt, der sowohl detailliertere Informationen zu den von uns angesprochenen Punkten als auch weitere Begründungen für die von uns getroffenen Entscheidungen enthält. Dieser Anhang wird angesichts der aktuellen Bedrohung durch Russland zum jetzigen Zeitpunkt nicht veröffentlicht.

---

[1] Natürlich gibt es auch eine lange Geschichte feindseliger Auseinandersetzungen zwischen den russischen – und früher sowjetischen – Geheimdiensten und ihren britischen Pendants.

[2] In diesem Bericht wird der Begriff „Geheimdienstgemeinschaft“ verwendet, um die sieben Organisationen zu bezeichnen, die der Ausschuss beaufsichtigt: die Geheimdienst- und Sicherheitsbehörden (MI5, SIS und GCHQ), den Militärgeheimdienst im Verteidigungsministerium, das Amt für Sicherheit und Terrorismusbekämpfung (OSCT) im Innenministerium sowie das Nationale Sicherheitssekretariat (NSS) und die Gemeinsame Geheimdienstorganisation (JIO) im Kabinettsamt.

11. Der Bericht behandelt Aspekte der russischen Bedrohung für das Vereinigte Königreich (Cyber, Desinformation und Einflussnahme sowie russische Auswanderer) und untersucht anschließend, wie die britische Regierung – insbesondere die Behörden und der Militärgeheimdienst – darauf reagiert hat (Aufgabenzuweisung, Strategie, Koordination und Aufgabenstellung, ein hartes Ziel, Gesetzgebung, internationale Partnerschaften und Zusammenarbeit mit Russland).

12. Als Ergebnis unserer Prüfung sind wir zu Schlussfolgerungen gekommen, was gut funktioniert, wo mehr oder andere Anstrengungen erforderlich sind oder wo eine Strategie möglicherweise aktualisiert werden muss, und wir haben eine Reihe von Maßnahmen in Auftrag gegeben. Diese sind im gesamten Bericht enthalten. Wir stellen jedoch fest, dass sich im Laufe unserer Arbeit eine Reihe von übergreifenden Themen herauskristallisiert haben:

- Am überraschendsten war vielleicht, in welchem Umfang sich ein Großteil der Arbeit der Geheimdienste auf *** konzentriert. Zu Beginn unserer Untersuchung waren wir davon ausgegangen, dass sie einen eher breiteren Blickwinkel einnehmen würden, da allgemein anerkannt ist, dass die Russen einen gesamtstaatlichen Ansatz verfolgen.

- Dieser Fokus hat uns zu der Frage veranlasst, wer für umfassendere Maßnahmen gegen die russische Bedrohung zuständig ist und ob diese Organisationen ausreichend befugt sind, um einer feindlichen staatlichen Bedrohung wie Russland entgegenzutreten. In einigen Fällen haben wir daher eine Verlagerung der Zuständigkeiten empfohlen. In anderen Fällen haben wir eine Vereinfachung empfohlen: Es gibt eine Reihe unnötig komplizierter Schaltpläne, die nicht die erforderlichen klaren Zuständigkeiten vorgeben.

- Die offensichtlichste Notwendigkeit für sofortiges Handeln ist eine neue Gesetzgebung: Die Geheimdienste müssen mit den erforderlichen Mitteln ausgestattet und in die bestmögliche Position gebracht werden, um diesen sehr fähigen Gegner bekämpfen zu können. Dies bedeutet einen neuen gesetzlichen Rahmen zur Bekämpfung von Spionage, illegalen Finanzgeschäften der russischen Elite und den „Helfern“, die diese Aktivitäten unterstützen.

- Allgemeiner gesagt liegt der Weg nach vorne darin, gemeinsam mit unseren Verbündeten Maßnahmen zu ergreifen; es bedarf eines anhaltenden internationalen Konsenses gegen das aggressive Vorgehen Russlands. Der Westen ist am stärksten, wenn er gemeinsam handelt, und auf diese Weise können wir Putins Handlungen am besten mit Kosten belegen. Das Vereinigte Königreich hat gezeigt, dass es die internationale Reaktion gestalten kann, wie es dies bei den Anschlägen von Salisbury getan hat. Es muss nun darauf aufbauen, um sicherzustellen, dass die Dynamik nicht verloren geht.

CYBER

Ein hochentwickelter Akteur im Bereich der Cyber

13. Nach Einschätzung des GCHQ ist Russland ein hochkompetenter Cyberakteur mit nachgewiesener Fähigkeit, Operationen durchzuführen, die eine Reihe von Auswirkungen auf alle Sektoren haben können:

- Seit 2014 führt Russland böswillige Cyberaktivitäten durch, um sich in einer Reihe von Bereichen aggressiv zu behaupten, darunter auch Versuche, die demokratischen Wahlen anderer Länder zu beeinflussen – so wurde beispielsweise vielfach berichtet, dass Russland hinter der cybergestützten „Hack-and-Leak"-Operation stand, mit der im Vorfeld der französischen Wahlen 2017 die Konten von Mitgliedern der französischen Partei *En Marche!* kompromittiert wurden.

- Russland hat auch Cyber-Vorbereitungsmaßnahmen[4] gegen die kritische nationale Infrastruktur (CNI) anderer Länder durchgeführt.[5] Das National Cyber Security Centre (NCSC) hat darauf hingewiesen, dass es *** russische Cyber-Einbrüche in die CNI des Vereinigten Königreichs gibt – insbesondere in den *** Sektoren.

- Das GCHQ hat außerdem darauf hingewiesen, dass Akteure der russischen GRU[6]Phishing-Versuche[7]gegen Regierungsbehörden orchestriert haben – so gab es beispielsweise Versuche gegen ***,[8]das Außenministerium (FCO) und das Verteidigungswissenschafts- und Technologielabor (DSTL) in der Anfangsphase der Ermittlungen zu den Anschlägen von Salisbury.[9]

14. Russland hat versucht, organisierte kriminelle Gruppen einzusetzen, um seine Cyberfähigkeiten zu ergänzen: Der SIS hat beobachtet, dass *„dies zu einer sehr undurchsichtigen Verflechtung zwischen Wirtschaft, Korruption und Staatsmacht in Russland führt*".[10] Der GCHQ teilte dem Ausschuss *mit*, dass es *„derzeit eine beträchtliche Menge an Informationen* gibt*, die Verbindungen zwischen schweren und organisierten kriminellen Gruppen und russischen Staatsaktivitäten* belegen" und dass *„wir weitere Hinweise darauf gefunden haben*, *dass *** schwere und organisierte Kriminalität *** mit hohen Ebenen des russischen Staates und des russischen Geheimdienstes in Verbindung* steht", was als *„symbiotische* Beziehung" beschrieben wurde. [11]

15. Die Cyberfähigkeiten Russlands in Verbindung mit seiner Bereitschaft, diese in böswilliger Absicht einzusetzen, geben Anlass zu großer Sorge und stellen eine unmittelbare und dringende Bedrohung für unsere nationale Sicherheit dar.

---

[3] „Hack and Leak" bezieht sich auf das Erlangen privater Informationen durch Hacking und deren Veröffentlichung.

[4] Vorpositionierung im Zusammenhang mit Cyberaktivitäten ist der Prozess der Erkundung und Sicherung eines Einstiegspunkts in ein Netzwerk, der jetzt oder in Zukunft für disruptive Zwecke genutzt werden könnte. Es ist nicht immer sofort ersichtlich, ob das Eindringen zu Spionagezwecken oder zur Vorpositionierung erfolgt.

[5] Kritische nationale Infrastruktur (CNI) umfasst die Einrichtungen, Systeme, Standorte, Informationen, Personen, Netzwerke und Prozesse, die für das Funktionieren eines Landes notwendig sind und von denen das tägliche Leben abhängt. Im Vereinigten Königreich gibt es 13 CNI-Sektoren: Chemie, zivile Kernenergie, Kommunikation, Verteidigung, Rettungsdienste, Energie, Finanzen, Lebensmittel, Regierung, Gesundheit, Raumfahrt, Verkehr und Wasser.

[6] Die GRU ist die Hauptnachrichtendienstdirektion des Generalstabs der russischen Streitkräfte.

[7] Phishing – die betrügerische Praxis, E-Mails zu versenden, die angeblich von seriösen Organisationen stammen, um persönliche Informationen wie Passwörter und Kreditkartennummern zu erlangen.

[8] ***

[9] GCHQ, *Quartalsbericht an den ISC*, Juli–September 2018.

[10] Mündliche Aussage – SIS, *** Februar 2019.

[11] Mündliche Aussage – GCHQ, *** Februar 2019.

Leitung der Reaktion auf „ “

16. Das NCSC – Teil des GCHQ – ist federführend beim Schutz des Vereinigten Königreichs vor Cyberangriffen und als Behörde für Cybersicherheit im Vereinigten Königreich für den Wissensaustausch und die Behebung systemischer Schwachstellen zuständig. Es ist die Schnittstelle der Regierung zur Industrie im Bereich Cybersicherheit und federführend bei der Reaktion auf Vorfälle (z. B. im Falle eines Cyberangriffs auf die kritische Infrastruktur des Vereinigten Königreichs).

17. Es ist jedoch klar, dass der Cyberbereich ein überfülltes Feld – oder eine *„komplexe Landschaft“* – ist.[12] Es gibt eine Reihe von Behörden und Organisationen innerhalb der Intelligence Community, die eine Rolle bei der Bekämpfung der russischen Cyberbedrohung spielen, und es war nicht sofort ersichtlich, wie diese verschiedenen Behörden und Organisationen koordiniert werden und sich tatsächlich ergänzen. Die nächste Fassung der Nationalen Cybersicherheitsstrategie muss diesem Bedarf an größerer Kohäsion Rechnung tragen.

18. Insbesondere die Zuständigkeit ist ein Problem: Während der Außenminister für das NCSC verantwortlich ist, das für die Reaktion auf Vorfälle zuständig ist, leitet der Innenminister die Reaktion auf größere Cybervorfälle. Tatsächlich gibt es eine Reihe weiterer Minister, die in irgendeiner Form für Cyberfragen zuständig sind: Der Verteidigungsminister trägt die Gesamtverantwortung für offensive Cybermaßnahmen als „Kriegsführungsinstrument“ und für das nationale offensive Cyberprogramm, während der Minister für Digitales, Kultur, Medien und Sport (DCMS) für digitale Angelegenheiten zuständig ist und der Kanzler des Herzogtums Lancaster für die nationale Cybersicherheitsstrategie und das nationale Cybersicherheitsprogramm verantwortlich ist. Dies führt zu einem unnötig komplizierten Verantwortungsgeflecht, das vom Nationalen Sicherheitsrat (NSC) regelmäßig überprüft werden sollte.

Attribution: ein neuer Ansatz für die „ “

19. Aus der Reaktion der Regierung geht klar hervor, dass sie nun begonnen hat, einen entschlosseneren Ansatz zu verfolgen. Cyber-Attribution ist der Prozess der Identifizierung und anschließenden Schuldzuweisung an den Urheber eines Cyberangriffs. Das Vereinigte Königreich hat sich in der Vergangenheit bei der Zuordnung von Cyberangriffen zurückhaltend gezeigt – noch 2010 wurde dieser Ausschuss aus diplomatischen Gründen gebeten, die Erwähnung Russlands als Urheber von Cyberangriffen zu streichen.

20. Dieser neue Ansatz zeigte sich zunächst in der Reaktion auf den WannaCry-Angriff im November 2017 (mit einer Erklärung des Außenministers Lord Ahmad, in der er den Angriff verurteilte) und der anschließenden Reaktion auf den NotPetya-Angriff im Februar 2018, dann kürzlich, als der Außenminister am am 3. Oktober 2018 öffentlich bekannt gab, dass das Vereinigte Königreich und seine Verbündeten eine Kampagne des GRU mit wahllosen und rücksichtslosen Cyberangriffen auf öffentliche Einrichtungen, Unternehmen, Medien und Sport[14] identifiziert hatten – einschließlich der Zuordnung des versuchten Hackerangriffs auf die Organisation für das Verbot chemischer Waffen (OPCW) in Den Haag.[15] Dies muss der richtige Ansatz sein; solche Aktivitäten müssen nun mit Kosten verbunden sein. Wenn Angriffe zurückverfolgt werden können – und wir akzeptieren, dass dies an sich ressourcenintensiv ist –, muss die Regierung immer eine „Naming and Shaming“-Strategie in Betracht ziehen.

---

[12] Mündliche Aussage – NSS, *** Februar 2019.

[13] Der Ausschuss lehnte diesen Antrag ab und veröffentlichte die Informationen.

[14] NCSC, *Reckless campaign of cyber attacks by Russian military intelligence service exposed*, 3. Oktober 2018, (www.ncsc.gov. uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed).

([15]) Am 4. Oktober 2018 gaben die Premierministerin, Theresa May MP, und der niederländische Ministerpräsident Mark Rutte eine gemeinsame Erklärung ab.

HMG als Akteur: Offensive Cyber

21. Nichtsdestotrotz leben wir in einer Zeit hybrider Kriegsführung, in der offensive Cyberfähigkeiten unverzichtbar sind. Die Regierung kündigte im September 2013 ihre Absicht an, offensive Cyberfähigkeiten zu entwickeln, und 2014 wurde das Nationale Offensive Cyberprogramm (NOCP) ins Leben gerufen – eine Partnerschaft zwischen dem Verteidigungsministerium und dem GCHQ.

22. Das Vereinigte Königreich baut seine offensiven Cyberfähigkeiten weiter aus. Das Verteidigungsministerium und das GCHQ haben dies als *„echte gemeinsame* Anstrengung" bezeichnet.[17] Dies hat uns zu der Frage veranlasst, ob es klare Zuständigkeiten gibt. Der Ausschuss wurde vom Chef des Verteidigungsnachrichtendienstes versichert, dass

> *Durch die Durchführung einer gemeinsamen Mission können wir* [das Verteidigungsministerium und das GCHQ] *nahtlos zwischen verschiedenen Genehmigungen wechseln und so sicherstellen, dass wir angemessen handeln, während diejenigen, die die Fähigkeiten verwalten, in der Lage sind, diesen Wechsel vorzunehmen und die Operationen effektiv durchzuführen.*[18]

Wir erwarten, dass wir über die Funktionsweise des dualen Genehmigungsverfahrens auf dem Laufenden gehalten werden, während die Kapazitäten selbst weiter ausgebaut werden.

23. Das GCHQ und das Verteidigungsministerium haben in den letzten Jahren eine offenere Haltung gegenüber offensiven Cyberoperationen eingenommen [19], beispielsweise durch öffentliche Verweise auf die erfolgreiche Verfolgung einer groß angelegten offensiven Cyberkampagne gegen Daesh. Das Thema offensive Cyberoperationen wird im vertraulichen Anhang zu diesem Bericht ausführlicher behandelt.

24. *** – Das GCHQ räumte ein, dass *** es seine Rekrutierungsbasis erweitern und den Schwerpunkt eher auf die Eignung als auf bereits vorhandene Fähigkeiten legen müsse. Interessant war auch zu hören, dass der Militärische Nachrichtendienst Maßnahmen ergreift, um diese Fähigkeiten durch eine Überarbeitung des militärischen Ressourcenmodells zu entwickeln und zu erhalten, was bedeutet, dass Militärangehörige länger als derzeit ein bis zwei Jahre in Cyber-Funktionen bleiben werden. Der Ausschuss unterstützt die Verlängerung der Amtszeit als allgemeiner Grundsatz, nicht nur im Verteidigungsnachrichtendienst und nicht nur im Cyberbereich. Durch solche kurzen Rotationen gehen in der gesamten Regierung kontinuierlich Unternehmenswissen und -erfahrung verloren, und es stellt sich die Frage, wie lange eine Person in einer Position bleiben muss, um einen Beitrag leisten zu können, oder ob sie gerade dann weiterzieht, wenn sie sich eingearbeitet hat. Wir loben den Verteidigungsnachrichtendienst dafür, dass er dieses Problem als erster erkannt und Maßnahmen ergriffen hat.

Internationale Maßnahmen zur „ "

25. Das Vereinigte Königreich muss zwar über eigene defensive und offensive Fähigkeiten verfügen, aber auch bereit sein, internationale Maßnahmen zu leiten. Was die Zuordnung von Verantwortung angeht, so ist offensichtlich, dass nicht alle bereit sind, diesen neuen Ansatz zu übernehmen und Russland wegen böswilliger Cyberaktivitäten zur Rechenschaft zu ziehen. Die Regierung muss nun ihre diplomatischen Beziehungen nutzen, um einen gemeinsamen internationalen Ansatz für die Zuordnung von böswilligen Cyberaktivitäten durch Russland und andere zu entwickeln.

26. Auch in Bezug auf offensive Cyberaktivitäten ist ein gemeinsamer internationaler Ansatz erforderlich. Es besteht eindeutig dringender Bedarf an der Einführung einer Doktrin oder einer Reihe von

---

[16] Die Ankündigung des damaligen Verteidigungsministers Philip Hammond umfasste auch die Einrichtung einer Cyber-Reserveeinheit.
[17] Mündliche Aussage – GCHQ, *** Februar 2019.
[18] Mündliche Aussage – Verteidigungsnachrichtendienst, *** Februar 2019.
[19] Der Direktor des GCHQ verwies in einer Rede auf der CyberUK am 21. April 2018 auf die Cyberkampagne gegen Daesh.

Protokolle, um einen gemeinsamen Ansatz für offensive Cyberangriffe sicherzustellen. Die Vereinten Nationen haben zwar vereinbart, dass das Völkerrecht und insbesondere die Charta der Vereinten Nationen im Cyberspace gelten, doch besteht nach wie vor Bedarf an einem besseren globalen Verständnis dafür, wie dies in der Praxis funktionieren soll. Der Ausschuss hat diese Empfehlung vor über zwei Jahren in seinem Jahresbericht 2016–2017 ausgesprochen.[20]Angesichts der zunehmenden Bedrohung durch Russland (und andere Länder, darunter China, Iran und die Demokratische Volksrepublik Korea) sind nun konkrete Fortschritte in diesem Bereich unerlässlich. Die Erzielung eines Konsenses über diesen gemeinsamen Ansatz wird ein schwieriger Prozess sein, aber als führender Befürworter der regelbasierten internationalen Ordnung ist es unerlässlich, dass das Vereinigte Königreich in Zusammenarbeit mit seinen Verbündeten zur Förderung und Gestaltung von Einsatzregeln beiträgt.

[20] *Jahresbericht 2016–2017 des Geheimdienst- und Sicherheitsausschusses des Parlaments*, HC 655.

[21] Die Position des Vereinigten Königreichs zur Anwendung des Völkerrechts im Cyberspace wurde in einer Rede mit dem Titel *„Cyber and International Law in the 21st century*" dargelegt, die der Generalstaatsanwalt, Rt Hon. Jeremy Wright QC MP, am 23. Mai 2018 im Chatham House hielt.

DESINFORMATION UND EINFLUSS VON „ “

27. Die Verbreitung von Desinformation (damit meinen wir die Förderung absichtlich falscher, verzerrender oder ablenkender Darstellungen) und die Durchführung von „Einflusskampagnen“ sind separate, aber miteinander verbundene Themen. Eine Einflusskampagne im Zusammenhang mit einer Wahl kann beispielsweise die Verbreitung von Desinformation nutzen, aber auch andere Taktiken wie illegale Finanzierung, Störung des Wahlmechanismus oder direkte Angriffe auf eine der Kampagnen (z. B. „Hack and Leak”) umfassen. Ebenso zielt die Verbreitung von Desinformation nicht unbedingt darauf ab, ein bestimmtes Ergebnis zu beeinflussen, sondern kann einfach allgemeine Ziele wie die Schaffung einer Atmosphäre des Misstrauens oder die Spaltung der Gesellschaft verfolgen. [22]

28. Russlands Förderung von Desinformation und seine Versuche, seinen politischen Einfluss im Ausland auszuweiten, sind vielfach dokumentiert worden.[23]Beispiele hierfür sind:

- Nutzung staatlicher traditioneller Medien: Open-Source-Studien haben erhebliche Verzerrungen in der Berichterstattung russischer staatlicher internationaler Sender wie RT und Sputnik aufgezeigt;[24]

- „Bots” und „Trolle”: Open-Source-Studien haben erhebliche Aktivitäten in den sozialen Medien festgestellt;

- „Hack and Leak“: Die USA haben öffentlich erklärt, dass Russland im Zusammenhang mit den Präsidentschaftswahlen 2016 „Hack and Leak“-Operationen durchgeführt hat, und es wird weithin vermutet, dass Russland für einen ähnlichen Angriff auf die französischen Präsidentschaftswahlen 2017 verantwortlich war.

- „Real Life“-politische Einmischung: Es wurde vielfach berichtet, dass mit dem Kreml verbundene Einrichtungen dem (damaligen) *Front National* in Frankreich „zinsgünstige Darlehen“ gewährt haben, offenbar zumindest teilweise als Belohnung dafür, dass die Partei die Annexion der Krim durch Russland unterstützt hatte,[25] und dass der GRU im Oktober 2016 einen gescheiterten Putsch in Montenegro[26] – ein erstaunlich gewagter Schritt in einem Land, das nur wenige Monate vor seinem Beitritt zur NATO stand.

29. Russland mag Desinformation verbreiten oder versuchen, politische Ereignisse für eine Vielzahl von Zwecken zu beeinflussen, aber alles dient der Unterstützung seiner grundlegenden außenpolitischen Ziele:

- direkte Unterstützung einer pro-russischen Darstellung bestimmter Ereignisse (auch wenn einige der offen vorgebrachten Unwahrheiten vielleicht nicht allgemein geglaubt werden, können sie dennoch erfolgreich Zweifel an der wahren Darstellung der Ereignisse säen: *„Wenn Menschen*

---

[22] Die Verbreitung von Desinformation führt nach britischem Recht in der Regel nicht zu einer straf- oder zivilrechtlichen Haftung, aber eine Einflusskampagne, die in einen demokratischen Prozess eingreift, könnte dies bewirken (dies wird im Abschnitt *„Gesetzgebung“* dieses Berichts näher erläutert).

[23] Wir stellen fest, dass die Desinformationsbemühungen Russlands gegenüber dem Westen im Vergleich zu denen, die der russische Staat gegenüber seiner eigenen Bevölkerung unternimmt, verblassen.

[24] Eine Übersicht über einige dieser Studien findet sich im Bericht des Sonderausschusses für Digitales, Kultur, Medien und Sport *„Desinformation und ‚Fake News‘“*, HC 1791, 18. Februar 2019. Im Fall von RT teilte Edward Lucas dem Ausschuss mit, dass die direkten *„Auswirkungen von RT ... gering sind ... Zu jedem beliebigen Zeitpunkt ... sehen durchschnittlich 1.300 Menschen in diesem Land RT ... Der eigentliche Sinn von RT besteht darin, in Elitekreisen an Legitimität zu gewinnen und nicht zuletzt Abgeordneten und Peers zu sagen: „Hier sind [sagen wir] 2.000 £ in bar, wenn Sie in unserer* Sendung *auftreten*.” Christopher Donnelly erklärte, dass *„im Vereinigten Königreich die Hauptwirkung ... über die sozialen Medien erzielt wird. Sie verbreitet ihre Botschaft zu allen wichtigen Aktivitäten, die* [in den sozialen Medien] *innerhalb von 20 Minuten stattfinden ...*“ (mündliche Aussage – 12. Juli 2018).

[25] ***

[26] Schriftliche Beweismittel – HMG, 29. Juni 2018.

Wenn man anfängt zu sagen: „Man weiß nicht, was man glauben soll" oder „Die sind alle gleich schlecht", dann gewinnen die Desinformanten" [27]);

- direkte Unterstützung des von Russland bevorzugten Ergebnisses in Bezug auf eine ausländische Wahl oder ein politisches Thema; und

- allgemeine Vergiftung der politischen Debatte im Westen durch die Schürung von politischem Extremismus und „Spaltungsthemen"[28] sowie durch „Astroturfing"[29] der westlichen öffentlichen Meinung; und allgemeine Diskreditierung des Westens.[30]

30. Was die direkte Bedrohung für Wahlen angeht, wurde uns mitgeteilt, dass die Mechanismen des britischen Wahlsystems als weitgehend sicher gelten: Die Verwendung eines stark verstreuten papierbasierten Wahl- und Auszählungssystems macht jede nennenswerte Manipulation schwierig, und wir gehen davon aus, dass der GCHQ umfangreiche Maßnahmen ergriffen hat, um die Sicherheit des Online-Wählerregistrierungssystems zu gewährleisten.[31] Dennoch teilte uns das GCHQ mit, dass „***",[32] und der stellvertretende nationale Sicherheitsberater merkte an, dass *„viel Arbeit* [in Bezug auf die Wahlmechanismen] *geleistet wird, um die End-to-End-Prozesse abzubilden … *** und um sicherzustellen, dass wir die Risiken dort, wo es möglich ist, mindern*".[33] Dies spiegelte sich in der Einschätzung des Joint Intelligence Committee (JIC) vom Mai 2017 wider, dass *„das papierbasierte Wahlverfahren im Vereinigten Königreich vor Cyberangriffen geschützt ist, aber ***"*.[34]
***. Der Ausschuss erwartet in sechs Monaten einen aktuellen Bericht zu diesem Thema.

Ein „heißes Eisen" in der „Hot "

31. Das Vereinigte Königreich ist eindeutig ein Ziel für Russlands Desinformationskampagnen und politische Einflussnahme[35] und muss sich daher rüsten, um solchen Bemühungen entgegenzuwirken. Die Behörden haben betont, dass sie ihre Rolle dabei darin sehen, geheime Informationen[36] als Kontext für andere Organisationen bereitzustellen, als Teil einer umfassenderen Reaktion der britischen Regierung:[37] Sie sehen sich nicht in erster Linie dafür verantwortlich, die demokratischen Prozesse des Vereinigten Königreichs aktiv vor feindlichen ausländischen Einmischungen zu schützen, und zeigten sich im Laufe unserer Untersuchung entschlossen, sich von jeglicher Andeutung zu distanzieren, sie könnten eine herausragende Rolle in Bezug auf den demokratischen Prozess selbst spielen, wobei sie auf die Vorsicht hinwiesen, die im Zusammenhang mit Eingriffsbefugnissen im Kontext eines demokratischen Prozesses geboten sei. Sie teilten uns mit, dass das Ministerium für Digitales, Kultur, Medien und Sport (DCMS) die Hauptverantwortung für Desinformation trägt.

---

[27] *Leitfaden der Integrity Initiative zur Bekämpfung russischer Desinformation*, 2018 (die Integrity Initiative ist ein Projekt des Institute for Statecraft, einer in Großbritannien ansässigen Denkfabrik und Wohltätigkeitsorganisation, die sich zum Ziel gesetzt hat, russischen Desinformationskampagnen entgegenzuwirken).

[28] „Wedge Issues" sind Themen, die die Bevölkerung eines Landes stark spalten, oft (aber nicht immer) in sozial liberale und sozial konservative Lager, und die häufig zumindest bis zu einem gewissen Grad über die traditionellen Parteigrenzen hinausgehen. Beispiele für „Wedge Issues" sind Abtreibung und Waffenkontrolle in den USA und der Brexit im Vereinigten Königreich.

[29] „Astroturfing" ist eine Propagandatechnik, bei der eine Meinung fälschlicherweise als die Meinung einer bestimmten Gruppe dargestellt wird. In diesem Fall können sich Mitarbeiter des russischen Staates und von Russland kontrollierte Bots in sozialen Medien als normale britische Bürger ausgeben und britischen Politikern, Journalisten und anderen Personen, die Macht und Einfluss haben, allein durch die schiere Menge der Beiträge den Eindruck vermitteln, dass die vertretenen Ansichten tatsächlich denen der Mehrheit der Bevölkerung ihres Landes entsprechen.

[30] Während der Zweck dieser Art von Kampagnen manchmal darin besteht, westlichen Positionen direkt zu schaden, zielen einige dieser Bemühungen darauf ab, sicherzustellen, dass die Natur der herrschenden Elite Russlands nicht aufgedeckt wird. Mit den Worten von Edward Lucas in seiner Aussage vor dem Ausschuss: *„Wenn man glaubt, dass der Westen von heuchlerischen, inkompetenten und gierigen Politikern regiert wird, dann wird es viel schwieriger, gegenüber Russland, das tatsächlich von sehr, sehr schlechten Menschen regiert wird, eine moralische Überlegenheit einzunehmen*."

[31] Mündliche Aussage – GCHQ, *** Dezember 2018; mündliche Aussage – NSS, *** Februar 2019.

[32] Mündliche Aussage – GCHQ, *** Februar 2019.

[33] Mündliche Aussage – NSS, *** Februar 2019.

[34] JIC(17)053.

[35] Wir stellen fest, dass die formelle Bewertung der britischen Regierung das Vereinigte Königreich als „***" Ziel für politische Einflussnahme einstuft.

[36] Zusätzlich zur Bereitstellung geheimer Informationen können die Behörden ***.

[37] Wir stellen fest, dass das Centre for the Protection of National Infrastructure (CPNI) und das National Cyber Security Centre (NCSC) ebenfalls die Sicherheitsarchitektur der Regierung unterstützen und eine Rolle beim Schutz der Wahlmechanismen spielen, unter anderem durch Informationen zu Verbesserungen der Wahlverwaltungssoftware und durch Sicherheitsempfehlungen an politische Parteien.

Kampagnen, und dass die Wahlkommission für die allgemeine Sicherheit demokratischer Prozesse verantwortlich ist.

32. Das DCMS teilte uns jedoch mit, dass seine Funktion weitgehend auf die allgemeine Politik der britischen Regierung hinsichtlich der Verwendung von Desinformation beschränkt ist und nicht die Bewertung oder Bekämpfung feindlicher staatlicher Kampagnen umfasst. Es war überraschend schwierig festzustellen, wer für was zuständig ist. Insgesamt scheint die Frage der Verteidigung der demokratischen Prozesse und Diskurse im Vereinigten Königreich eine Art „heißes Eisen" zu sein, da keine Organisation bereit ist, die Gesamtverantwortung zu übernehmen.

33. Wir verstehen zwar die Nervosität, die mit jedem Hinweis auf eine mögliche Beteiligung der Geheimdienste und Sicherheitsbehörden an demokratischen Prozessen einhergeht – eine Befürchtung, die in anderen Ländern sicherlich weit verbreitet ist –, doch kann dies nicht gelten, wenn es um den Schutz dieser Prozesse geht. Und ohne in irgendeiner Weise unterstellen zu wollen, dass das DCMS nicht fähig oder die Wahlkommission kein entschiedener Verteidiger der Demokratie ist, ist dies eine Frage des Umfangs und des Zugangs. Das DCMS ist eine kleine Politikabteilung in Whitehall, und die Wahlkommission ist eine unabhängige Einrichtung; keine der beiden ist in der zentralen Position, die erforderlich ist, um einer großen feindlichen Bedrohung unserer Demokratie durch einen anderen Staat entgegenzuwirken. Der Schutz unseres demokratischen Diskurses und unserer demokratischen Prozesse vor feindlichen ausländischen Einmischungen ist eine zentrale Aufgabe der Regierung und sollte eine Priorität des Ministeriums sein.

34. Unserer Meinung nach muss die operative Rolle in erster Linie beim MI5 liegen, entsprechend seiner gesetzlichen Verantwortung für *„den Schutz der nationalen Sicherheit und insbesondere deren Schutz vor Bedrohungen durch Spionage, Terrorismus und Sabotage, vor den Aktivitäten von Agenten ausländischer Mächte und vor Handlungen, die darauf abzielen, die parlamentarische Demokratie zu stürzen oder zu untergraben …".*[38] Die politische Rolle sollte beim Amt für Sicherheit und Terrorismusbekämpfung (OSCT) liegen – vor allem aufgrund seiner zehnjährigen Erfahrung in der Bekämpfung terroristischer Bedrohungen und seiner engen Zusammenarbeit mit dem MI5 innerhalb der zentralen Regierungsapparate. Dies hätte auch den Vorteil, dass die Beziehungen zu Social-Media-Unternehmen, die dazu dienen, diese zur Zusammenarbeit bei der Bekämpfung der Nutzung sozialer Medien durch Terroristen zu bewegen, auch gegen die Bedrohung durch feindliche Staaten genutzt werden könnten; uns ist nicht klar, warum die Regierung dies nicht bereits tut.

35. Vor diesem Hintergrund stellen wir fest, dass – wie bei so vielen anderen aktuellen Themen – die Social-Media-Unternehmen den Schlüssel in der Hand halten, aber dennoch ihrer Verantwortung nicht nachkommen. Das DCMS teilte uns mit, dass ***.[39] Die Regierung muss nun versuchen, ein Protokoll mit den Social-Media-Unternehmen zu vereinbaren, um sicherzustellen, dass diese die verdeckte Nutzung ihrer Plattformen durch feindliche Staaten ernst nehmen und klare Fristen festlegen, innerhalb derer sie sich zur Entfernung solcher Inhalte verpflichten. Die Regierung sollte diejenigen, die nicht handeln, öffentlich anprangern. Ein solches Protokoll könnte sinnvollerweise auf andere Bereiche ausgeweitet werden, in denen Maßnahmen von den Social-Media-Unternehmen erforderlich sind, da dieses Problem nicht nur für feindliche staatliche Aktivitäten gilt. Diese Angelegenheit ist unserer Ansicht nach dringend, und wir erwarten, dass die Regierung so bald wie möglich über die Fortschritte in diesem Bereich berichtet.

Das Programm „Defending Democracy" ( )

36. Die oben genannten Probleme hinsichtlich der Rollen und Verantwortlichkeiten könnten durch das Programm „Defending Democracy" der Regierung angegangen werden, das öffentlich angekündigt wurde in

---

[38] Abschnitt 1(2), Sicherheitsdienstgesetz von 1989; Der MI5 hat uns mitgeteilt, dass er derzeit folgende Aufgaben hat: (i) „Hinweise auf solche geheimen Aktivitäten ausländischer Staaten zu untersuchen"; (ii) „die gewonnenen Erkenntnisse in Schutzempfehlungen zur Verteidigung unserer Systeme umzusetzen" und (iii) „bewertete Geheimdienstberichte an das politische System zu liefern, um die Politikgestaltung zu unterstützen" (mündliche Aussage – MI5, *** Dezember 2018).

[39] Schriftliche Aussage – DCMS, 13. Februar 2019.

Juli 2019. Uns wurde mitgeteilt, dass dies die Arbeit der Regierung zum Schutz des demokratischen Diskurses und der demokratischen Prozesse vor Einmischung unter der Leitung des Kabinettsbüros koordinieren wird, wobei der Kanzler des Herzogtums Lancaster[40] und der stellvertretende nationale Sicherheitsberater die Gesamtverantwortung auf Minister- bzw. Beamtenebene tragen.

37. Das Ziel ist gut, aber die vorgeschlagene Reaktion ist noch recht fragmentiert (mindestens zehn verschiedene Teams innerhalb der Regierung sind beteiligt, ebenso wie die Wahlkommission und das Amt des Informationsbeauftragten). Darüber hinaus scheint ihr eine eher geringe Priorität eingeräumt worden zu sein: Sie wurde erst im Februar 2019 vom Nationalen Sicherheitsrat verabschiedet, fast drei Jahre nach der EU-Referendumskampagne und den US-Präsidentschaftswahlen, die diese Themen in den Vordergrund gerückt hatten. Nach Ansicht des Ausschusses darf eine ausländische Macht, die versucht, sich in unsere demokratischen Prozesse einzumischen – unabhängig davon, ob sie damit Erfolg hat oder nicht –, nicht auf die leichte Schulter genommen werden. Unsere Demokratie ist für den Erfolg und das Wohlergehen unseres Landes von grundlegender Bedeutung, und jede Bedrohung derselben muss von denjenigen, die mit unserer Verteidigung betraut sind, als ernstes Problem der nationalen Sicherheit behandelt werden.

Politische Werbung in sozialen Medien

38. Die Regulierung politischer Werbung fällt nicht in den Zuständigkeitsbereich dieses Ausschusses. Wir stimmen jedoch mit der Schlussfolgerung des DCMS-Sonderausschusses überein, dass der Rechtsrahmen dringend überarbeitet werden muss, damit er im Zeitalter der weit verbreiteten sozialen Medien seinen Zweck erfüllen kann. Insbesondere nehmen wir die Empfehlung des Sonderausschusses zur Kenntnis und bekräftigen sie, dass alle politischen Online-Anzeigen einen Impressumsvermerk enthalten sollten, aus dem hervorgeht, wer für sie bezahlt. [41] Wir würden hinzufügen, dass Social-Media-Unternehmen verpflichtet werden sollten, mit dem MI5 zusammenzuarbeiten, wenn der Verdacht besteht, dass ein feindlicher ausländischer Staat heimlich eine Kampagne durchführt.

Fallstudie: Das Referendum über den EU-

39. Es gab weit verbreitete öffentliche Vorwürfe, dass Russland versucht habe, das Referendum über die EU-Mitgliedschaft Großbritanniens im Jahr 2016 zu beeinflussen. Die Auswirkungen solcher Versuche wären schwer – wenn nicht gar unmöglich – zu beurteilen, und wir haben auch nicht versucht, dies zu tun. Es ist jedoch wichtig festzustellen, ob ein feindlich gesinnter Staat bewusst Maßnahmen ergriffen hat, um einen demokratischen Prozess im Vereinigten Königreich zu beeinflussen, unabhängig davon, ob diese erfolgreich waren oder nicht.

40. Open-Source-Studien haben auf die Überzahl von Pro-Brexit- oder Anti-EU-Berichten auf RT und Sputnik sowie auf den Einsatz von „Bots" und „Trollen" als Beweis für russische Versuche hingewiesen, den Prozess zu beeinflussen. [42] Wir haben versucht festzustellen, ob es geheime Informationen gibt, die diese Studien stützen oder darauf aufbauen. Auf unsere Anfrage nach schriftlichen Beweisen zu Beginn der Untersuchung lieferte der MI5 zunächst nur sechs Zeilen Text. Darin hieß es, dass ***, bevor auf akademische Studien verwiesen wurde.[43] Bemerkenswert war dabei die Formulierung (***) und der Verweis auf öffentlich zugängliche Studien ***. Die Kürze war für uns erneut ein Hinweis auf die extreme Vorsicht der Geheimdienste und Sicherheitsbehörden angesichts der Vorstellung, dass sie eine Rolle im Zusammenhang mit den demokratischen Prozessen im Vereinigten Königreich spielen könnten, insbesondere bei einem so umstrittenen Thema wie dem EU-Referendum. Wir wiederholen, dass diese Haltung unlogisch ist; es geht hier um die

---

[40] Der Kanzler des Herzogtums Lancaster delegiert die Aufgaben gegebenenfalls an den Minister für Verfassungsfragen.
[41] DCMS-Sonderausschuss, *Desinformation und „Fake News",* HC 1791, 18. Februar 2019.
[42] Der Bericht des DCMS-Sonderausschusses *„Desinformation und Fake News"* (HC 1791, 18. Februar 2019) untersucht einige dieser Studien und kommentiert sie.
[43] Schriftliche Stellungnahme – HMG, 3. April 2018.

Schutz des Prozesses und des Mechanismus vor feindlichen staatlichen Eingriffen, was Aufgabe unserer Geheimdienste und Sicherheitsbehörden sein sollte.

(i) Versäumnisse bei der Vorbereitung

41. Es gibt glaubwürdige Kommentare aus offenen Quellen, die darauf hindeuten, dass Russland im Zusammenhang mit dem schottischen Unabhängigkeitsreferendum 2014 Einflusskampagnen durchgeführt hat. [44] Zu diesem Zeitpunkt ***. Es scheint, dass ***, was einige Kommentatoren als möglicherweise erste postsowjetische Einmischung Russlands in einen westlichen demokratischen Prozess bezeichnet haben. Wir stellen fest, dass – fast fünf Jahre später – ***. [45]

42. Erst als Russland eine „Hack-and-Leak"-Operation gegen das Democratic National Committee in den USA durchgeführt hatte – wobei die gestohlenen E-Mails einen Monat nach dem EU-Referendum veröffentlicht wurden –, schien die Regierung verspätet zu erkennen, welche Bedrohung Russland in diesem Bereich darstellen könnte, da sich die Risikoschwellen im Kreml eindeutig verschoben hatten und die „Hack-and-Leak"-Operation in den USA als *„Game* Changer" bezeichnet wurde[46] und einräumte, dass *„vor den Ereignissen in den Vereinigten Staaten* [die russische Einmischung] *im Allgemeinen nicht als große Bedrohung für* [Wahl-]*Prozesse angesehen wurde*".[47]

43. Es scheint, dass die Geheimdienste aus den Erfahrungen der USA gelernt haben und die britische Regierung die russische Bedrohung für die demokratischen Prozesse und den politischen Diskurs im Vereinigten Königreich erkannt hat. Im Mai 2017 kam der Gemeinsame Geheimdienstausschuss (Joint Intelligence Committee, JIC) zu dem Schluss, dass „***" und dass „ ***".[48]Hätten die zuständigen Stellen der Geheimdienste vor dem Referendum eine ähnliche Bedrohungsanalyse durchgeführt, wäre es unvorstellbar, dass sie nicht zu dem gleichen Schluss hinsichtlich der Absichten Russlands gekommen wären, was sie dann möglicherweise dazu veranlasst hätte, Maßnahmen zum Schutz des Prozesses zu ergreifen.

(ii) Begrenzte Berichterstattung

44. Die uns vorgelegten schriftlichen Beweise schienen darauf hinzudeuten, dass die britische Regierung keine Beweise für eine erfolgreiche Einmischung in die demokratischen Prozesse des Vereinigten Königreichs oder für Aktivitäten gesehen oder gesucht hatte, die einen wesentlichen Einfluss auf eine Wahl hatten, beispielsweise durch Beeinflussung der Ergebnisse.[49] ,[50] ***. ***.[51]

45. Diese Fokussierung auf *** deutet darauf hin, dass öffentlich zugängliches Material (z. B. die Studien zu Versuchen, das Referendum mithilfe von RT und Sputnik zu beeinflussen, oder die zuvor erwähnten Social-Media-Kampagnen) nicht vollständig berücksichtigt wurde. Angesichts der Tatsache, dass der Ausschuss zuvor

---

[44] So wurde beispielsweise kurz nach dem Referendum vielfach berichtet, dass russische Wahlbeobachter auf Unregelmäßigkeiten bei der Durchführung der Abstimmung hingewiesen hätten, und diese Position wurde von den russischen Staatsmedien breit propagiert. Wir gehen davon aus, dass die britische Regierung dies in erster Linie als Versuch ansah, das Vereinigte Königreich in den Augen der russischen Öffentlichkeit zu diskreditieren. In jüngerer Zeit verweisen wir auf die Studie von Ben Nimmo – *#ElectionWatch: Scottish Vote, Pro-Kremlin Trolls*, 12. Dezember 2017.

[45] Mündliche Aussage – GCHQ, *** Dezember 2018 ***.

[46] ***

[47] ***

[48] JIC-Schlüsselurteil, ***, 26. Mai 2017.

[49] *** (schriftliche Aussage – HMG, 29. Juni 2018).

[50] Wir stellen fest, dass Arron Banks mit seiner Spende von 8 Millionen Pfund an die Leave.EU-Kampagne zum größten Spender in der britischen Politikgeschichte wurde. Im Oktober 2018 verwies die Wahlkommission, die die Herkunft dieser Spende untersucht hatte, den Fall an die National Crime Agency, die ihn untersuchte ***. Im September 2019 gab die National Crime Agency bekannt, dass sie die Ermittlungen abgeschlossen habe, da sie keine Hinweise darauf gefunden habe, dass eine der von der Wahlkommission an sie verwiesenen Personen oder Organisationen gegen das Gesetz über politische Parteien, Wahlen und Referenden von 2000 oder gegen das Gesellschaftsrecht verstoßen habe.

[51] ***

Da uns mitgeteilt wurde, dass Open-Source-Material nun vollständig in der Einschätzung der Bedrohungslage durch die Regierung berücksichtigt wird, war es für uns überraschend, dass dies in diesem Fall nicht der Fall war.

46. Zwar mag es zutreffen, dass einige in Open-Source-Quellen hervorgehobene Probleme keine geheimen Ermittlungsfähigkeiten der Geheimdienste und Sicherheitsbehörden erforderten oder am Rande ihres Zuständigkeitsbereichs lagen, doch verfügen die Behörden dennoch über Fähigkeiten, die es ihnen ermöglichen, auf den Erkenntnissen aus Open-Source-Quellen aufzubauen: So könnte beispielsweise könnte das GCHQ versuchen, hinter die verdächtigen Social-Media-Konten zu blicken, die durch die Analyse öffentlich zugänglicher Quellen identifiziert wurden, um ihre wahren Betreiber aufzudecken (und sogar ihre Nutzung zu unterbinden), oder der SIS könnte einen Agenten speziell damit beauftragen, Informationen über das Ausmaß und die Art russischer Einflusskampagnen zu beschaffen. [52] Wir haben jedoch *** gefunden, was darauf hindeutet, dass ***. ***.

(iii) Fehlende rückblickende Bewertung

47. Uns liegt keine Bewertung der russischen Einmischungsversuche nach dem Referendum vor, ***.[53] Diese Situation steht in krassem Gegensatz zum Umgang der USA mit den Vorwürfen der russischen Einmischung in die Präsidentschaftswahlen 2016, wo innerhalb von zwei Monaten nach der Wahl eine Bewertung der Geheimdienste[54] erstellt und eine nicht klassifizierte Zusammenfassung veröffentlicht wurde. Auch wenn die Fragen, um die es in der EU-Referendumskampagne geht, weniger eindeutig sind, ist der Ausschuss dennoch der Ansicht, dass die britischen Geheimdienste eine ähnliche Bewertung der potenziellen russischen Einmischung in das EU-Referendum erstellen und eine nicht klassifizierte Zusammenfassung davon veröffentlichen sollten.[55]

48. ***. Selbst wenn eine solche Bewertung zu dem Ergebnis käme, dass nur minimale Eingriffe stattgefunden haben, würde dies dennoch eine hilfreiche Beruhigung für die Öffentlichkeit darstellen, dass die demokratischen Prozesse im Vereinigten Königreich relativ sicher geblieben sind.

---

52 ***

53 ***

54 Amt des Direktors der Nationalen Nachrichtendienste, *Bewertung der Aktivitäten und Absichten Russlands bei den jüngsten Wahlen in den USA,* 6. Januar 2017.

55 Wir stellen fest, dass der DCMS-Sonderausschuss die Regierung aufgefordert hat, eine unabhängige Untersuchung zu ausländischer Einflussnahme, Desinformation, Finanzierung, Wählermanipulation und Datenaustausch im Zusammenhang mit dem schottischen Unabhängigkeitsreferendum, dem EU-Referendum und den Parlamentswahlen 2017 einzuleiten. Sollte die Regierung diese Empfehlung für eine umfassendere Untersuchung aufgreifen, könnte die von uns empfohlene Bewertung in diese einfließen (DCMS-Sonderausschuss, *Desinformation und „Fake News"*, HC 1791, 18. Februar 2019, Empfehlung 39).

Oligarchen mit offenen Armen empfangen

49. Während die russische Elite in den letzten Jahren Beziehungen zu einer Reihe von Ländern aufgebaut hat, scheint das Vereinigte Königreich für russische Oligarchen und ihr Geld ein besonders attraktives Ziel zu sein. Es ist allgemein bekannt, dass der Schlüssel zur Attraktivität Londons in der Ausnutzung des 1994 eingeführten britischen Investorenvisumsystems lag, gefolgt von der Förderung einer lockeren und begrenzten Regulierung, wobei Londons starke Kapital- und Immobilienmärkte solide Investitionsmöglichkeiten boten. Auch die Rechtsstaatlichkeit und das Justizsystem des Vereinigten Königreichs wurden als Anziehungspunkt angesehen. Das Vereinigte Königreich hieß russisches Geld willkommen, und es wurden – wenn überhaupt – nur wenige Fragen zur Herkunft dieses beträchtlichen Vermögens gestellt. Es scheint, dass die britische Regierung damals der Überzeugung war (vielleicht eher in der Hoffnung als in der Erwartung), dass der Aufbau von Beziehungen zu großen russischen Unternehmen eine gute Regierungsführung fördern würde, indem ethische und transparente Praktiken sowie die Schaffung eines rechtsstaatlichen Wirtschaftsumfelds gefördert würden.

50. Heute ist klar, dass dies in Wirklichkeit kontraproduktiv war, da es ideale Mechanismen bot, mit denen illegale Finanzmittel über die sogenannte Londoner „Wäscherei” recycelt werden konnten. Das Geld wurde auch in die Ausweitung von Patronage und den Aufbau von Einfluss in weiten Bereichen des britischen Establishments investiert – PR-Firmen, Wohltätigkeitsorganisationen, politische Interessengruppen, akademische und kulturelle Einrichtungen waren allesamt willige Nutznießer russischer Gelder und trugen so zu einem Prozess der „Reputationswäsche” bei. Kurz gesagt, der russische Einfluss im Vereinigten Königreich ist „die neue Normalität”, und es gibt viele Russen mit sehr engen Verbindungen zu Putin, die gut in die britische Geschäfts- und Gesellschaftsszene integriert und aufgrund ihres Reichtums akzeptiert sind. Dieser Grad der Integration – insbesondere in „Londongrad” – bedeutet, dass alle Maßnahmen, die derzeit von der Regierung ergriffen werden, nicht präventiv sind, sondern eher der Schadensbegrenzung dienen.

51. Es sind nicht nur die Oligarchen: Das Eintreffen russischer Gelder führte zu einem Boom der Branche der „Enabler“ – Personen und Organisationen, die für die russische Elite in Großbritannien tätig sind und Lobbyarbeit für sie betreiben. Rechtsanwälte, Wirtschaftsprüfer, Immobilienmakler und PR-Fachleute haben wissentlich oder unwissentlich zur Ausweitung des russischen Einflusses beigetragen, der oft mit der Förderung der ruchlosen Interessen des russischen Staates verbunden ist. Im Vereinigten Königreich hat sich eine große private Sicherheitsbranche entwickelt, um den Bedürfnissen der russischen Elite gerecht zu werden. Britische Unternehmen schützen die Oligarchen und ihre Familien, suchen nach *Kompromat*[56] über Konkurrenten und helfen gelegentlich dabei, Geld über Offshore-Briefkastenfirmen zu waschen und „Due-Diligence”-Berichte zu fälschen, während Anwälte Unterstützung bei Rechtsstreitigkeiten leisten. William Browder erklärte gegenüber dem Ausschuss:

> *Russische Staatsinteressen, die mit kriminellen privaten Interessen zusammenarbeiten und durch diese umgesetzt werden, haben eine „Pufferzone” aus Westlern geschaffen, die de facto zu russischen Staatsagenten werden, viele davon unwissentlich, andere jedoch mit dem Wissen, was sie tun und für wen sie arbeiten. Infolgedessen müssen britische Akteure sich mit russischen kriminellen Interessen auseinandersetzen, die als Staatsinteressen getarnt sind, sowie mit russischen Staatsinteressen, die durch ihre westlichen Agenten verschleiert werden.*[57]

[56] *Kompromat* – kompromittierende Informationen, die gesammelt werden, um jemanden zu erpressen, zu diskreditieren oder zu manipulieren, in der Regel zu politischen Zwecken.
[57] Schriftliche Beweise – William Browder, 14. September 2018.

Der Versuch, die Tür zum Stall zu schließen

52. Die Verbindungen der russischen Elite zum Vereinigten Königreich – insbesondere in den Bereichen Wirtschaft und Investitionen – ermöglichen den Zugang zu britischen Unternehmen und Politikern und damit einen weitreichenden Einfluss Russlands im Vereinigten Königreich. Bis zu einem gewissen Grad lässt sich dies nicht entwirren, und die Priorität muss nun darin bestehen, das Risiko zu mindern und sicherzustellen, dass bei Aufdeckung feindlicher Aktivitäten Instrumente zur Verfügung stehen, um diese an der Quelle zu bekämpfen.

53. Das Ausmaß, in dem russische Auswanderer ihren Zugang zu britischen Unternehmen und Politikern nutzen, um Einfluss in Großbritannien auszuüben, ist ***: Es ist allgemein bekannt, dass russische Geheimdienste und Wirtschaft vollständig miteinander verflochten sind. Die Regierung muss *** die notwendigen Maßnahmen ergreifen, um dieser Bedrohung entgegenzuwirken und die Straffreiheit der mit Putin verbundenen Eliten in Frage zu stellen. Die Gesetzgebung ist ein wichtiger Schritt und wird später in diesem Bericht behandelt.

54. Mehrere Mitglieder der russischen Elite, die eng mit Putin verbunden sind, stehen in Verbindung mit gemeinnützigen und/oder politischen Organisationen im Vereinigten Königreich, haben Spenden an politische Parteien geleistet und verfügen über ein öffentliches Profil, das sie in die Lage versetzt, russische Einflussnahme zu unterstützen. Bemerkenswert ist, dass eine Reihe von Mitgliedern des House of Lords geschäftliche Interessen in Russland haben oder direkt für große russische Unternehmen arbeiten, die mit dem russischen Staat verbunden sind – diese Beziehungen sollten sorgfältig geprüft werden, da der russische Staat sie potenziell ausnutzen könnte. Es ist wichtig, dass der Verhaltenskodex für Mitglieder des House of Lords und das Register der Interessen der Lords, einschließlich finanzieller Interessen, die erforderliche Transparenz gewährleisten und durchgesetzt werden. In diesem Zusammenhang stellen wir fest, dass der Verhaltenskodex für Mitglieder des Parlaments vorschreibt, dass Abgeordnete einzelne Zahlungen von mehr als 100 £ registrieren müssen, die sie für eine Beschäftigung außerhalb des Oberhauses erhalten – dies gilt nicht für das Oberhaus, und es sollte erwogen werden, eine solche Vorschrift einzuführen. Ein „Gesetz zur Registrierung ausländischer Agenten" (ein Thema, das im Abschnitt über Gesetzgebung behandelt wird) wäre in dieser Hinsicht ebenfalls hilfreich.

55. Die Bemühungen der Regierung zur Unterbindung illegaler russischer Finanzaktivitäten im Vereinigten Königreich werden von der National Crime Agency (NCA) geleitet und koordiniert.[58] Ihre Arbeit umfasst auch die Untersuchung von im Vereinigten Königreich ansässigen professionellen Mittelsmännern im Finanz- und Immobiliensektor mit dem Ziel, die britischen Finanz- und Immobilienmärkte gegen Erträge aus Straftaten zu wappnen und der Auffassung entgegenzuwirken, dass das Vereinigte Königreich ein sicherer Hafen für illegale Gelder sei. Das Ausmaß, in dem dieses Geld inzwischen investiert und reinvestiert wurde, stellt die Wirksamkeit der kürzlich eingeführten Unexplained Wealth Orders (UWO) in Frage, wenn sie auf die Untersuchung von Personen angewendet werden, die seit langem etablierte – und in jeder Hinsicht offenbar mittlerweile legitime – finanzielle Interessen im Vereinigten Königreich haben. Zwar scheinen die Anordnungen der NCA mehr Einfluss und größere Befugnisse zu verleihen, doch in Wirklichkeit ist es sehr wahrscheinlich, dass die Oligarchie über die finanziellen Mittel verfügt, um sicherzustellen, dass ihre Anwälte – eine wichtige Gruppe von professionellen Unterstützern – Wege finden, diese Gesetzgebung zu umgehen (wir kommen später in diesem Bericht auf dieses Thema zurück). Im Gegensatz dazu mangelt es der NCA an den erforderlichen Ressourcen in Form von Finanzermittlern, technischen Experten und juristischem Fachwissen – dies muss korrigiert werden. [59]

56. Die inhärente Spannung zwischen der Wohlstandsagenda der Regierung und der Notwendigkeit, die nationale Sicherheit zu schützen, die zur aktuellen Situation geführt hat, hat sich in ganz

---

[58] Der Ausschuss dankt der NCA für die Bereitstellung von Beweismaterial für diese Untersuchung. Der Ausschuss beaufsichtigt die NCA nicht; ihre Arbeit und ihre Tätigkeiten fallen in der Regel nicht in den Zuständigkeitsbereich des ISC.

[59] In der am 1. November 2018 veröffentlichten Strategie zur Bekämpfung schwerer und organisierter Kriminalität wurde die Einrichtung eines behördenübergreifenden National Assessment Centre (NAC) und des National Economic Crime Centre innerhalb der NCA angekündigt.

Whitehall-Ministerien. Die Gründung der neuen Gruppe für schwere und organisierte Kriminalität (Serious and Organised Crime, SOC) innerhalb des Innenministeriums Ende 2018 war jedoch eine konkrete Anerkennung der Wirtschaftskriminalität als Frage der nationalen Sicherheit. Die SOC-Gruppe hat einen weitreichenden Aufgabenbereich – es bleibt zu hoffen, dass sie mit den notwendigen Ressourcen ausgestattet wird und der Bekämpfung der Bedrohung durch illegale russische Finanzaktivitäten ausreichende Priorität einräumt. Eine wichtige Maßnahme wäre eine Überarbeitung des Tier-1-Visaprogramms (Investorenvisum)[60] – das Genehmigungsverfahren für diese Visa muss strenger gestaltet werden.

Russische Staatsangehörige mit „ ”-Risiko

57. Während die Oligarchen und ihr Geld der sichtbarste Teil der russischen Diaspora sind, haben die jüngsten Ereignisse gezeigt, dass es in Großbritannien auch viele Russen gibt, die auf der gegnerischen Seite stehen. Seit Putin 1999 an die Macht kam, haben zahlreiche Kritiker Putins und der russischen Regierung aus Angst vor politisch motivierten Strafanzeigen und Schikanen Zuflucht im Vereinigten Königreich gesucht. [61]Sie sind für die russischen Geheimdienste (RIS) von Interesse, die möglicherweise versuchen werden, sie auf verschiedene Weise ins Visier zu nehmen:

- Es ist möglich, dass der RIS versuchen wird, einige dieser Personen mithilfe menschlicher Quellen (d. h. Agenten) und technischer Mittel zu überwachen, beispielsweise durch das Abhören von Telefonaten und das Hacken ihrer persönlichen elektronischen Geräte.

- Die vom RIS gesammelten Informationen könnten auch zur Unterstützung von „Einflussoperationen” verwendet werden, mit dem Ziel, die Fähigkeit einer Person zu beeinträchtigen, internationale oder innenpolitische russische Opposition gegen Putin und seine Regierung zu fördern.

- Der RIS könnte versuchen, Möglichkeiten zu identifizieren oder zu schaffen, um die Verhaftung einer Person und ihre Überstellung nach Russland zu veranlassen, wo sie vor Gericht gestellt wird oder sogar ein schlimmeres Schicksal ereilt.

58. Am 15. Juni 2017 veröffentlichte BuzzFeed News die Ergebnisse seiner Untersuchung zu 14 Todesfällen in Großbritannien, bei denen es sich um russische Geschäftsleute und mit ihnen in Verbindung stehende britische Staatsbürger handelte.[62] Der Mordversuch an Sergei und Yulia Skripal im März 2018 führte zu Forderungen an die Regierung, die in dem BuzzFeed-Bericht erhobenen Vorwürfe zu untersuchen, und am 6. März 2018 schrieb der Vorsitzende des Innenausschusses an den Innenminister und forderte eine Überprüfung der 14 Todesfälle, da die *„erheblichen besorgniserregenden* Beweise“ von BuzzFeed *„Fragen zur Solidität der polizeilichen* Ermittlungen“ aufwerfen würden. [63]

59. Der Ausschuss hat Beweise zu diesen Angelegenheiten gesammelt. Uns wurde mitgeteilt, dass ***. ***.[64]

60. Wir haben in Frage gestellt, ob der Schutz der gefährdeten Personen im Vereinigten Königreich ausreichend Priorität eingeräumt wurde. Uns wurde versichert, dass alle gefährdeten Personen – ob russischer oder anderer Herkunft – entsprechend dem Grad der Gefährdung durch ein von der Polizei geleitetes Verfahren Schutz erhalten ***.[65]

61. Wir haben diesen Prozess begrüßt, aber die Frage gestellt, ob die Geheimdienste ein klares Bild davon haben, wie viele Russen sich im Vereinigten Königreich in Gefahr befinden – würde beispielsweise

---

[60] Ein Tier-1-Visum (Investorenvisum) berechtigt den Inhaber zu einem Aufenthalt von drei Jahren und vier Monaten im Vereinigten Königreich im Austausch für eine Investition von 2 Millionen Pfund im Vereinigten Königreich.

[61] Dazu gehören so bekannte Persönlichkeiten wie ***.

[62] „From Russia with Blood“, *BuzzFeed News*, 15. Juni 2017.

[63] Schreiben des Vorsitzenden des Innenausschusses an den Innenminister, 6. März 2018.

[64] ***

[65] Mündliche Aussage – *** Februar 2019.

MI5 oder eine andere zuständige Behörde ***? Dies scheint ein unmittelbarer und naheliegender Ansatz für dieses Problem zu sein, und die ***, sodass es machbar erscheint. Als Antwort wurde uns mitgeteilt, dass ***.

62. Die Ereignisse vom 4. März 2018 haben gezeigt, dass nicht nur Personen, die Putin offen kritisieren, hier in Großbritannien gefährdet sind. Der Anschlag von Salisbury hat die Gefährdung ehemaliger russischer Geheimdienstmitarbeiter, die sich in Großbritannien niedergelassen haben, deutlich gemacht. Diese Frage wurde vom Ausschuss im Rahmen seiner Untersuchung geprüft und wird im vertraulichen Anhang zu diesem Bericht behandelt.

63. Es ist offensichtlich, dass Russland derzeit in vielerlei Hinsicht eine erhebliche Bedrohung für das Vereinigte Königreich darstellt – von Spionage über Einmischung in demokratische Prozesse bis hin zu schwerer Kriminalität. Die Frage ist, wie es dazu gekommen ist – und was die Geheimdienste nun unternehmen, um dagegen vorzugehen.

Berichterstattung

64. In seinem Jahresbericht 2001–2002 äußerte der Ausschuss die Besorgnis, dass durch die Umschichtung von Ressourcen zur Terrorismusbekämpfung die Abdeckung anderer Bereiche zunehmend eingeschränkt worden sei:

> *Diese Kürzungen führen zu Lücken in der Informationsbeschaffung, was bedeuten könnte, dass im Laufe der Zeit inakzeptable Risiken für die Gewährleistung der nationalen Sicherheit und die Prävention und Aufdeckung schwerer organisierter Kriminalität entstehen. Die Behörden müssen mit ausreichenden Ressourcen ausgestattet werden, damit sie nicht nur die entstandenen Personalengpässe beheben, sondern auch ausreichend expandieren können, um den neuen Anforderungen gerecht zu werden, die nun an sie gestellt werden.* [66]

Die Regierung antwortete darauf:

> *Die Regierung ist sich bewusst, dass die steigende Nachfrage nach Informationen zur Unterstützung der Terrorismusbekämpfung dazu geführt hat, dass unter anderem die Behörden ihre Prioritäten innerhalb ihrer eigenen Budgets überprüfen mussten. Dieser Prozess wurde professionell und sorgfältig durchgeführt, und die Regierung wird die Situation weiterhin beobachten. Es ist unvermeidlich, dass einige Tätigkeitsbereiche für das nationale Interesse relativ an Bedeutung gewinnen, während andere relativ an Bedeutung verlieren und möglicherweise weniger Ressourcen zur Verfügung stehen. Alle Entscheidungen über die Anpassung der Ressourcen an die Aufgaben sind mit einem gewissen Risiko verbunden. Die Identifizierung, Quantifizierung, Steuerung und, soweit möglich, Minderung dieser Risiken gehört zu den grundlegenden Aufgaben der Leitung der Behörden. Die Regierung ist zuversichtlich, dass die bisherigen Entscheidungen richtig waren und dass keine inakzeptablen Risiken für die nationale Sicherheit eingegangen wurden oder werden.* [67]

65. In seinem Jahresbericht 2002–2003 berichtete der Ausschuss, dass sich das Problem der Lücken in der Informationsbeschaffung seiner Meinung nach verschärft habe, und kam zu folgendem Schluss:

> *Der Ausschuss ist der Ansicht, dass durch die Konzentration auf aktuelle Krisen die langfristige Fähigkeit der Behörden, Warnungen auszusprechen, untergraben wird. Diese Situation muss von den Ministern und dem JIC* [Joint Intelligence Committee] *angegangen und bewältigt werden.* [68]

---

[66] *Jahresbericht 2001–2002 des Geheimdienst- und Sicherheitsausschusses des Parlaments*, Cm 5542.
[67] Zitiert im *Jahresbericht 2002–2003* des *Geheimdienst- und Sicherheitsausschusses des Parlaments*, Cm 5837.
[68] *Jahresbericht 2002–2003 des Geheimdienst- und Sicherheitsausschusses des Parlaments*, Cm 5837.

In den Jahren 2003–2004 äußerte der Ausschuss erneut seine Besorgnis:

> *Wir sind weiterhin besorgt, dass aufgrund der notwendigen zusätzlichen Anstrengungen, die der Sicherheitsdienst für die Terrorismusbekämpfung aufwendet, unvermeidlich erhebliche Risiken im Bereich der Spionageabwehr eingegangen werden.* [69]

MI5

66. Der Auftrag des MI5 – wie im Security Service Act 1989 festgelegt – ist der *„Schutz der nationalen Sicherheit und insbesondere deren Schutz vor Bedrohungen durch Spionage, Terrorismus und Sabotage, vor den Aktivitäten von Agenten ausländischer Mächte und vor Handlungen, die darauf abzielen, die parlamentarische Demokratie durch politische, industrielle oder gewalttätige Mittel zu stürzen oder zu untergraben*“.[70]Der MI5 gibt als seine Ziele in diesem Bereich an, *„diejenigen aufzuspüren, die versuchen, sensible Informationen und Ausrüstung des Vereinigten Königreichs an andere Länder weiterzugeben, und sicherzustellen,* dass *sie keinen Erfolg* haben“ sowie *„die Aktivitäten ausländischer Geheimdienstmitarbeiter zu untersuchen und zu unterbinden, wenn diese den Interessen unseres Landes schaden*“.[71]

67. Vor zwanzig Jahren widmete der MI5 etwa 20 % seiner Arbeit der Bekämpfung feindlicher staatlicher Aktivitäten, darunter russische Aktivitäten sowie feindliche Aktivitäten anderer Staaten wie China und Iran. [72] Dieser Anteil ging mit zunehmender terroristischer Bedrohung zurück. Bis 2001/02 sank er auf 16 % und bis 2003/04 auf 10,7 %. Dieser Rückgang setzte sich fort, bis der MI5 2008/09 nur noch 3 % seiner Arbeit für alle Maßnahmen gegen feindliche staatliche Aktivitäten aufwendete (wobei zu beachten ist, dass sich der Rückgang des Anteils an der Gesamtarbeit nicht direkt in einer Veränderung der Ressourcen niederschlägt).[73] Erst 2013/14 begann der Anteil wieder deutlich zu steigen und erreichte 14,5 %[74] – ein Niveau, das laut MI5 bedeutete, dass etwas mehr Mitarbeiter für Russland zuständig waren als während des Kalten Krieges.[75] In den letzten zwei Jahren wurden ***: Derzeit werden *** % für feindliche staatliche Aktivitäten bereitgestellt, davon etwa *** für die Bekämpfung feindlicher staatlicher Aktivitäten Russlands.[76]

SIS und GCHQ

68. Der SIS ist der britische Geheimdienst für menschliche Informationsbeschaffung (HUMINT) mit einer *„globalen verdeckten* Kapazität“ [77], deren Schwerpunkt auf der Informationsbeschaffung liegt. Zu den Bereichen der Informationsbeschaffung, die der SIS in Bezug auf Russland durchführt, gehört die Anwerbung von Agenten, die in der Lage sind, geheime Informationen weiterzugeben, insbesondere in Bezug auf die Fähigkeiten und Absichten der russischen Regierung, und seine Arbeit im Bereich der Informationsbeschaffung umfasst ***. Im Jahr 2001 betrugen die operativen Anstrengungen des SIS gegen Russland *** %. Diese gingen 2007 auf *** % zurück. Erst im Jahr *** begannen sie wieder deutlich anzusteigen und liegen derzeit bei etwa *** %.[78]

---

[69] *Jahresbericht 2003–2004 des Geheimdienst- und Sicherheitsausschusses des Parlaments*, Cm 6240.

[70] Abschnitt 1(2) des Sicherheitsdienstgesetzes von 1989.

[71] www.mi5.gov.uk/espionage

[72] Schriftliche Stellungnahme – MI5, 31. Oktober 2018.

[73] Jahresberichte des Geheimdienst- und Sicherheitsausschusses des Parlaments: 2001–2002, Cm 5542; 2003–2004, Cm 6240; 2008–2009, Cm 7807.

[74] Schriftliche Beweismittel – MI5, 31. Oktober 2018.

[75] *Jahresbericht 2016–2017 des Geheimdienst- und Sicherheitsausschusses des Parlaments*, HC 655.

[76] Schriftliche Beweismittel – MI5, 12. März 2019; Die Gesamtressourcen des MI5 haben in diesem Zeitraum erheblich zugenommen. *** Die Zuweisung von Ressourcen für Aktivitäten feindlicher Staaten hat ***, die Ausgaben für Aktivitäten feindlicher Staaten haben ***. Diese operativen Bemühungen profitieren auch von der Unterstützung durch Unternehmens- und „Enabling“-Dienste im gesamten MI5 (was in diesen Zahlen nicht zum Ausdruck kommt).

[77] www.sis.gov.uk

[78] Schriftliche Beweismittel – SIS, 17. Dezember 2018.

69. Das GCHQ ist die britische Behörde für Fernmeldeaufklärung (SIGINT) und konzentriert sich ebenfalls auf die Informationsbeschaffung. [79]Die nachrichtendienstliche Arbeit des GCHQ umfasst in erster Linie offensive Cybermaßnahmen. Zu den Bereichen der nachrichtendienstlichen Arbeit des GCHQ gehören: die Anwendung von Selektoren auf E-Mails, die durch Massenüberwachung erfasst wurden; die gezielte Überwachung von Telefonaten von Personen von Interesse; das Abfangen von Material, das über militärische Kommunikationssysteme übertragen wird; und das Hacken von Computersystemen, um die darin enthaltenen Informationen zu erhalten.

70. Auf dem Höhepunkt des Kalten Krieges konzentrierten sich 70 % der Aktivitäten des GCHQ auf den Sowjetblock.[80] Bis zum Jahr 2000 war dieser Anteil auf 16 % gesunken, und 2006 erreichte er mit nur noch 4 % einen Tiefpunkt. Im Jahr 2012 stieg dieser Anteil wieder auf 10 % an und blieb bis 2016 relativ konstant, bevor ein weiterer deutlicher Anstieg einsetzte.[81] Etwa *** % der aktuellen operativen Aktivitäten des GCHQ konzentrieren sich auf Russland.[82]

Verteidigungsnachrichtendienst

71. Der Verteidigungsnachrichtendienst hat weitreichende Zuständigkeiten für die Sammlung und Analyse von Informationen und spielt innerhalb der Regierung eine Schlüsselrolle bei der Erstellung von All-Source-Informationen über Russland. Er leitet die Arbeit des Vereinigten Königreichs im Bereich der georäumlichen Aufklärung (GEOINT) sowie der Mess- und Signaturerkennung (MASINT).[83] Er übernimmt auch eine SIGINT-Funktion *** und verfügt über eine HUMINT-Einheit, die in erster Linie zur Unterstützung militärischer Operationen eingesetzt wird. Neben dem GCHQ spielt sie auch eine wichtige Rolle in der Offensive Cyber Capability des Vereinigten Königreichs. Auch die Aktivitäten des Verteidigungsnachrichtendienstes in Bezug auf Russland wurden Anfang der 2000er Jahre erheblich reduziert. Obwohl der Verteidigungsnachrichtendienst keine Zahlen zu seinen Aktivitäten in den letzten 20 Jahren vorlegen konnte, wurde uns mitgeteilt, dass es 2013 relativ wenige All-Source-Analysten im Russland/Eurasien-Team gab (zusätzlich zu den auf Russland spezialisierten Analysten in anderen Teams). Der Verteidigungsnachrichtendienst hat mitgeteilt, dass derzeit *** seiner All-Source-Analysten mehr als 50 % ihrer Zeit mit Russland verbringen und weitere *** weniger als 50 % ihrer Zeit mit Russland verbringen. [84]

Hat die britische Regierung den Ball „ ” aus den Augen verloren?

72. Nach dem Ende des Kalten Krieges strebte der Westen eine Partnerschaft mit Russland an. Die von Russland ausgehende Bedrohung wurde als geringer eingeschätzt, und der Anteil der Anstrengungen zur Abwehr dieser Bedrohung wurde entsprechend reduziert. Wie aus den obigen Zahlen ersichtlich ist, kam es zu einem deutlichen Rückgang der Anstrengungen. Die Ermordung von Alexander Litwinenko im Jahr 2006 war vielleicht das deutlichste Zeichen dafür, dass nicht nur die Aussöhnung gescheitert war, sondern dass Russland gegenüber dem Westen und gegenüber Großbritannien wieder genauso feindselig eingestellt war wie zuvor. Bis 2006 konzentrierten sich die operativen Anstrengungen jedoch auf die Bekämpfung des internationalen Terrorismus: 2006/07 widmete der MI5 92 % seiner Anstrengungen der Terrorismusbekämpfung,[85] während es beim SIS und beim GCHQ 33 % waren.[86] Die restlichen

---

[79] SIGINT ist die Informationsbeschaffung durch das Abhören von Kommunikationen zwischen Personen und durch das Abfangen anderer elektronischer Signale.

[80] Mündliche Aussage – GCHQ, *** Dezember 2018.

[81] Schriftliche Aussage – GCHQ, 8. März 2019.

[82] Schriftliche Aussage – GCHQ, 14. Dezember 2018.

[83] Geospatial Intelligence (GEOINT) umfasst die Sammlung und Analyse von Informationen über geografische Merkmale und menschliche Aktivitäten, die in einem geografischen Kontext stattfinden. Measurement and Signature Intelligence (MASINT) nutzt technische Mittel, um die „Signaturen“ von Zielen zu erkennen und zu analysieren, um diese zu lokalisieren, zu analysieren und zu verfolgen.

[84] Dies entspricht *** % der derzeitigen analytischen Ressourcen des Verteidigungsnachrichtendienstes, die auf Russland konzentriert sind (schriftliche Stellungnahme – Verteidigungsnachrichtendienst, 6. März 2019).

[85] Schriftliche Stellungnahme – MI5, 31. Oktober 2018.

[86] Schriftliche Stellungnahme – SIS, 17. Dezember 2018; *Jahresbericht 2007–2008 des Geheimdienst- und Sicherheitsausschusses des Parlaments,* Cm 7542. Der Verteidigungsnachrichtendienst teilte uns mit, dass er seine analytischen Bemühungen zur Terrorismusbekämpfung an das Joint Terrorism Analysis Centre (JTAC) abgegeben habe, als dieses 2003 gegründet wurde. Dies entsprach schätzungsweise 20 Stellen bis 2006/07 – nur 1 % seiner damaligen Belegschaft (schriftliche Stellungnahme – Verteidigungsnachrichtendienst, 21. März 2019).

Die Ressourcen waren auf eine Reihe von Bereichen verteilt – feindselige Aktivitäten von Staaten waren nur einer davon, und Russland war nur einer der feindseligen Staaten. Das ist verständlich: Die Bedrohung durch den internationalen Terrorismus zu dieser Zeit – nur ein Jahr nach den Terroranschlägen von 2005, bei denen 52 Menschen ums Leben kamen – musste im Vordergrund stehen.

73. Wenn wir davon ausgehen, dass die russische Bedrohung 2006 mit der Ermordung von Alexander Litwinenko deutlich geworden ist, und dann Ereignisse wie die Annexion der Krim im Jahr 2014 als deutlichen Beweis für die Absichten Russlands auf der Weltbühne betrachten, stellt sich die Frage, ob die Geheimdienste schneller hätten reagieren und ihre operativen Anstrengungen in Bezug auf Russland verstärken sollen – und können. Betrachtet man allein die Zahlen, könnte man sagen, dass sie den Blick vom Ball genommen haben; dennoch versuchten die Leiter von MI5, SIS, GCHQ und Defence Intelligence, sich gegen diese Vermutung zu verteidigen. Der MI5 stellte klar, dass es aufgrund der terroristischen Bedrohung zu einer unvermeidlichen Neugewichtung der Prioritäten gekommen sei:

> *… damals ging es darum, wie wir dieses schreckliche Terrorismusproblem, das … damals größer war, als wir es überblicken konnten, in den Griff bekommen könnten, und eine der Aussagen, die wir genau zu der Zeit, von der Sie sprechen, dazu machten, war, dass wir die Grenzen dieses Problems noch nicht erkannt hätten.* [87]

Der Militärgeheimdienst sah das ähnlich:

> *Was also die relative Priorisierung angeht, so hat unsere Berichterstattung über Russland zweifellos unter dieser Priorisierung gelitten, die für die Durchführung militärischer Operationen notwendig war, anstatt den Fokus zu verlieren.* [88]

Im Vergleich dazu sahen der SIS und der GCHQ dies als Folge der längeren Vorlaufzeit, die für die Arbeit zu Russland erforderlich war. Der SIS erklärte:

> *Ich glaube nicht, dass wir den Blick vom Ball genommen haben. Ich denke, dass das Interesse an der Arbeit gegen die russische Bedrohung gewissermaßen gewachsen und wieder geschwunden ist.* ***. [89]

Und GCHQ stimmte zu:

> *Ähnlich wie* [SIS] *argumentiert, waren einige der Hardcore-Fähigkeiten, die notwendig waren, um im Geschäft zu bleiben, die wir aufrechterhalten haben, und dann, als die Berichte und Diskussionen über die Ereignisse auf der Krim die Aufmerksamkeit wieder mehr auf Russland lenkten, hat uns das dazu veranlasst, wieder einen Gang höher zu schalten.* [90]

74. Wir sind uns der enormen Belastungen bewusst, denen die Behörden seit dem 11. September ausgesetzt sind, und dass sie nur über begrenzte Ressourcen verfügen, die sie auf operative Prioritäten konzentrieren müssen. Dennoch ist es von Natur aus ineffizient, nur auf das Hier und Jetzt zu reagieren, und unserer Meinung nach hat die Regierung bis vor kurzem die russische Bedrohung und die erforderliche Reaktion darauf stark unterschätzt. [91]

---

[87] Mündliche Aussage – MI5, *** Dezember 2018.
[88] Mündliche Aussage – Verteidigungsnachrichtendienst, *** Dezember 2018.
[89] Mündliche Aussage – SIS, *** Dezember 2018.
[90] Mündliche Aussage – GCHQ, *** Dezember 2018.
[91] Wir nehmen zur Kenntnis, dass die Behörden einen „Horizontscan“ durchführen und dass es sich hierbei um eine Frage der Priorisierung von Ressourcen handelt.

75. Unter Berücksichtigung des Drucks, der durch die Terrorismusbekämpfung auf die operativen Organisationen ausgeübt wird, stellt sich dennoch die Frage nach dem Ansatz der politischen Abteilungen. Wir haben bereits zuvor erörtert, inwieweit die Wirtschaftspolitik die Öffnung des Vereinigten Königreichs für russische Investitionen diktiert hat. Dies deutet darauf hin, dass die sicherheitspolitischen Abteilungen es versäumt haben, sich mit diesem Thema auseinanderzusetzen – in einem Ausmaß, dass das Vereinigte Königreich nun innerhalb seiner eigenen Grenzen einer Bedrohung durch Russland ausgesetzt ist. Was offenbar ein eher laissez-faire-Ansatz in der Politik war, ist weniger leicht zu verzeihen als die Reaktion der vielbeschäftigten Behörden. Wir begrüßen die Tatsache, dass dies nun erkannt wurde und sich offenbar ändert.

Zukünftige Ressourcen für „ ”

76. Die jüngsten Veränderungen bei der Bereitstellung von Ressourcen zur Bekämpfung feindlicher Aktivitäten Russlands sind nicht (oder nicht nur) auf eine anhaltende Eskalation der Bedrohung zurückzuführen, sondern scheinen vielmehr ein Zeichen dafür zu sein, dass man versucht, den Rückstand aufzuholen. Der SIS und der GCHQ planten, ihre operativen Maßnahmen gegen Russland bis 2020 noch weiter zu verstärken – auf *** % bzw. *** %.[92]Der MI5 ist *** und strebt an, *** in Bezug auf feindliche staatliche Aktivitäten zu erreichen. Alle drei Organisationen machten deutlich, dass es sich hierbei um relative Prioritäten handelte. Der MI5 erklärte uns beispielsweise:

> *Wir treffen ziemlich häufig vierteljährlich *** Entscheidungen darüber, wie wir *** in diesen verschiedenen Themenbereichen vorgehen werden, und derzeit halten wir an einigen der Ressourcen fest, die nach Salisbury für die Arbeit im Bereich feindlicher Staaten bereitgestellt wurden, obwohl die Aussetzungsrate unserer CT-Ermittlungen* (Counter-Terrorism, Terrorismusbekämpfung) *weiterhin höher ist, als wir es uns wünschen.* [93]

In dieser Hinsicht muss dies eine Angelegenheit für die Minister sein. Der Innenminister erklärte uns, dass seiner Ansicht nach die Ressourcen für Russland *** und dass *„mehr Ressourcen für die Bekämpfung feindlicher Aktivitäten von Staaten bereitgestellt werden müssen*“.[94] Er warnte jedoch davor, dass die Bedrohung über Russland hinausgeht und dass die Aufstockung der auf Russland ausgerichteten Ressourcen nicht auf Kosten der Bemühungen zur Bekämpfung anderer eskalierender Bedrohungen gehen darf. Der Außenminister erkannte ebenfalls, wie wichtig es ist, andere Prioritäten nicht zu vernachlässigen:

> *Eine meiner Sorgen ist, dass einige der kurzfristigen Probleme, die Russland uns bereitet und mit denen wir uns befassen müssen, tatsächlich unsere Überlegungen zu den längerfristigen Veränderungen der internationalen Ordnung, nämlich dem Aufstieg Chinas, verdrängen. Deshalb habe ich versucht, sicherzustellen, dass wir uns Zeit nehmen, um tatsächlich zu betrachten, was sich in der Welt insgesamt verändert.*[95]

77. Angesichts des Drucks durch die internationale Terrorismusbekämpfung, die Bedrohung durch China, den Iran und die Demokratische Volksrepublik Korea erkennen wir, dass es schwierig ist, die russische Bedrohung als besonders wichtig herauszustellen und ihr mehr Aufmerksamkeit zu widmen. Daher ist es unerlässlich, dass die Strategie richtig ist – sie muss intelligenteres Arbeiten und eine effektive Koordinierung ermöglichen.

---

[92] Schriftliche Stellungnahme – HMG, 3. April 2018.
[93] Mündliche Aussage – MI5, *** November 2018.
[94] Mündliche Aussage – Innenminister, 31. Januar 2019.
[95] Mündliche Aussage – Außenminister, 7. Februar 2019.

STRATEGIE, KOORDINATION UND RUSSLAND-

Die ressortübergreifende Russland- sstrategie

78. Im Jahr 2016 verabschiedete der Nationale Sicherheitsrat eine ressortübergreifende Russland-Strategie. Die jüngste Fassung der Strategie – vom März 2019 – verfolgt eine übergeordnete langfristige „Vision" von *„einem Russland, das sich für Zusammenarbeit statt für Herausforderung oder* Konfrontation entscheidet"[96] ***.

79. Die Strategie gliedert sich in fünf Säulen: Schützen, Einschränken, Einbinden, Offenhalten und Aufbauen. [97]Die Verantwortung für die Umsetzung liegt bei der National Security Strategy Implementation Group for Russia, die sich aus 14 Ministerien und Behörden zusammensetzt. Diese Umsetzungsgruppe wird von der HMG Russia Unit im Außen- und Commonwealth-Ministerium (FCO) koordiniert und vom Senior Responsible Owner für die Umsetzung der Strategie (derzeit der Generaldirektor für Konsular- und Sicherheitsangelegenheiten des FCO) geleitet. Alle sieben von uns beaufsichtigten Organisationen sind in der Umsetzungsgruppe vertreten.

80. Es ist offensichtlich, dass die Russland-Strategie der britischen Regierung in gewisser Weise – sowohl hinsichtlich ihres Formats als auch grundlegender – Ähnlichkeiten mit der CONTEST-Strategie zur Terrorismusbekämpfung aufweist. Unseres Wissens wurden jedoch bei der Ausarbeitung und Umsetzung der Strategie keine direkten Lehren aus CONTEST gezogen.

81. Es scheint auch gewisse Ähnlichkeiten zwischen der Bekämpfung des Terrorismus und feindlichen Aktivitäten von Staaten zu geben – insbesondere im Hinblick auf die Sensibilisierung der Öffentlichkeit –, und es könnte mehr getan werden, um die Erfahrungen der Regierung im ersten Bereich für den zweiten Bereich zu nutzen. Insbesondere sind wir der Ansicht, dass der MI5 zwar bereits mit den regionalen Anti-Terror-Einheiten der Polizei (die für feindliche Aktivitäten von Staaten zuständig sind) zusammenarbeitet, aber dass es Spielraum für eine engere Zusammenarbeit in diesem Bereich gibt.

Ministerielle Zuständigkeit für „ "

82. Der Innenminister trägt die ministerielle Verantwortung für den MI5, der Außenminister für den SIS und den GCHQ und der Verteidigungsminister für den Verteidigungsnachrichtendienst. Alle drei Minister haben ein umfangreiches Aufgabengebiet und einen vollen Terminkalender, sodass ihnen nur begrenzt Zeit für Russland zur Verfügung steht. Es ist jedoch klar, dass Russland für die Minister eine hohe Priorität hat: Der Innenminister hat uns mitgeteilt, dass er sich *„mindestens einmal pro Woche, manchmal öfter, und … in … *** … es gab einige Diskussionen über* Russland" [98] und auf die Frage, wie oft er mit dem Chef des SIS und dem Direktor des GCHQ über Russland spreche, antwortete der Außenminister „***" [99] und erklärte seine Besorgnis, dass Probleme im Zusammenhang mit Russland – obwohl sie ernst sind – die Gefahr bergen, umfassendere globale Themen zu verdrängen.

83. Die politische Verantwortung für feindliche Aktivitäten von Staaten liegt beim Nationalen Sicherheitssekretariat im Kabinettsamt. Dies erscheint ungewöhnlich: Das Innenministerium scheint dafür eher der natürliche Ort zu sein, da so die Erfahrung des Amtes für Sicherheit und Terrorismusbekämpfung (OSCT) in Fragen der Terrorismusbekämpfung gegen die Bedrohung durch feindliche Staaten genutzt werden könnte. Wir verstehen

---

[96] Wir stellen fest, dass die langfristige Vision der vorherigen Fassung der Russland-Strategie darin bestand, *„ein eingeschränktes Russland, das mit dem Westen kooperiert, anstatt uns herauszufordern und zu* konfrontieren" (das Wort „eingeschränkt" wurde inzwischen gestrichen).

[97] Unter jeder Säule gibt es eine Reihe von regierungsübergreifenden „Kampagnen", die auf die Umsetzung der Strategie abzielen.

[98] Mündliche Aussage – Innenminister, 31. Januar 2019.

[99] Mündliche Aussage – Außenminister, 7. Februar 2019.

Die Regierung vertritt die Ansicht, dass feindliche Aktivitäten von Staaten eine übergreifende Bedrohung darstellen und es daher sinnvoll ist, dass das Kabinettsamt die Verantwortung dafür übernimmt; wir schlagen dennoch vor, dies weiterhin zu überprüfen.

Die Fusionsdoktrin und die gemeinsame Arbeit von „ “

84. Der Ausschuss hat im vergangenen Jahr viel über die Fusionsdoktrin gehört, deren Ziel es ist, *„Sicherheits-, Wirtschafts- und Einflussmöglichkeiten einzusetzen, um unsere nationalen Sicherheits-, Wirtschafts- und Einflussziele zu schützen, zu fördern und zu vertreten*“.[100] Grundsätzlich ist dies als Reaktion auf eine so weitreichende Bedrohung wie die durch Russland sinnvoll. Wir stellen jedoch fest, dass Russlands eigene Version dieses „verbundenen Arbeitsansatzes“ weitaus weiter entwickelt ist: Angesichts der im Kreml zentralisierten Macht, des Mangels an starken öffentlichen Institutionen, der engen Verbindungen zwischen Großunternehmen und Staat und – was entscheidend ist – seiner Tätigkeit außerhalb der regelbasierten internationalen Ordnung ist Russland leicht in der Lage, seine politische, wirtschaftliche, militärische und nachrichtendienstliche Macht zu kombinieren, um seine Ziele zu erreichen.

85. In Bezug auf die Behörden und den Militärgeheimdienst ist es angesichts der Schwierigkeiten bei der Zusammenarbeit mit Russland (die im nächsten Abschnitt näher erläutert werden) besonders wichtig, dass alle Quellen – HUMINT, SIGINT, MASINT, GEOINT,[101] Open Source und andere – so weit wie möglich komplementär genutzt werden und dass sie in allen Aspekten der koordinierten russischen Bedrohung (***) zum Einsatz kommen. Angesichts des kombinierten Charakters der russischen Bedrohung ist es von entscheidender Bedeutung, dass die Arbeit der Geheimdienste und des Verteidigungsnachrichtendienstes zu *** nicht getrennt von der allgemeinen russischen Außenpolitik und den Einflussbemühungen betrachtet wird. In einigen Fällen haben wir festgestellt, dass dies nicht klar war ***: Dies muss angegangen werden. Es ist von entscheidender Bedeutung, dass die britische Regierung im Zuge der Entwicklung der ressortübergreifenden Russland-Strategie und der zunehmenden Anwendung der Fusionsdoktrin eine umfassendere Sichtweise auf das gesamte Ausmaß der russischen Bedrohung einnimmt.

Die Beiträge der Geheimdienste zur Russland- -Strategie

86. Der Prozess „Intelligence Coverage and Effects“ (ICE) ist die Methode, mit der SIS und GCHQ von der Regierung beauftragt werden. [102]Der ICE-Plan für Russland erfordert *** Abdeckungsergebnisse und *** Wirkungsergebnisse, die in fünf Stufen priorisiert werden: „nicht verhandelbar“, hoch, mittel, niedrig und „nur bei Gelegenheit“. Damit soll sichergestellt werden, dass die Ergebnisse der Behörden mit den Anforderungen des Nationalen Sicherheitsrats und seiner „Kunden“ in den verschiedenen Ministerien hinsichtlich der Informationsbeschaffung und deren Auswirkungen übereinstimmen. In Bezug auf Russland entsprechen die ICE-Anforderungen den Aufgaben des SIS und des GCHQ im Zusammenhang mit der Russland-Strategie der britischen Regierung.

87. Im Gegensatz zu SIS und GCHQ ist MI5 selbstständig: Es priorisiert seine Arbeit gegen Bedrohungen für das Vereinigte Königreich auf der Grundlage seiner Einschätzung ihrer Schwere. Dies ist angesichts der defensiven Ausrichtung der Rolle von MI5 angemessen. Uns wurde jedoch mitgeteilt, dass MI5 seine Arbeit zu Russland in einem vereinbarten Ansatz der drei Behörden mit der von SIS und GCHQ abstimmt. [103]

---

[100] HMG, *National Security Capability Review*, März 2018.

[101] Menschliche Nachrichtendienste (HUMINT), Fernmeldeaufklärung (SIGINT), Mess- und Signaturerkennung (MASINT), Geodatenauswertung (GEOINT).

[102] Die nachrichtendienstliche Berichterstattung umfasst die Sammlung von Informationen (oder den Erwerb von Informationen von verbündeten Nachrichtendiensten) durch die Behörden und den Militärischen Nachrichtendienst. Die nachrichtendienstlichen Auswirkungen beschreiben die Beteiligung der Behörden und des Militärischen Nachrichtendienstes an Aktivitäten, die zu konkreten Ergebnissen führen.

[103] ***

88. Die Verteidigungsnachrichtendienst ist mit einem separaten Prozess des Verteidigungsministeriums betraut. Angesichts der Unterschiede zwischen der Arbeit des Verteidigungsnachrichtendienstes und der Arbeit der Behörden – einschließlich der Tatsache, dass er in seiner Bewertungsfunktion Kunde für die Nachrichtendienstprodukte des SIS und des GCHQ ist – mag dies sinnvoll sein. Der Chef des Verteidigungsnachrichtendienstes erkannte an, dass *„es absolut notwendig ist, dass der Verteidigungsnachrichtendienst eng mit den Aktivitäten des ICE koordiniert und möglicherweise synchronisiert wird*", schränkte jedoch ein, dass *„die Frage, ob wir uns vollständig auf den ICE-Prozess einlassen, meiner Meinung nach viel schwieriger zu beantworten ist*".[104] Wir erkennen an, dass es möglicherweise nicht angemessen ist, den Verteidigungsnachrichtendienst in den ICE einzubeziehen, waren jedoch überrascht, als wir feststellten, dass der Verteidigungsnachrichtendienst nicht in den Ansatz der drei Behörden einbezogen ist: ***.

Weniger reden, mehr „ "-Maßnahmen?

89. Es scheint eine Vielzahl von Plänen und Strategien zu geben, die für die Arbeit der von uns beaufsichtigten Organisationen in Bezug auf Russland von unmittelbarer Bedeutung sind: die ressortübergreifende Russland-Strategie, die Anforderungen des ICE-Plans für Russland, der gemeinsame Ansatz der drei Behörden für Russland, ein separater Aufgaben- und Priorisierungsprozess für den Militärgeheimdienst und die Fusion Doctrine, die all diese Dokumente überlagert. Wir sind uns zwar bewusst, dass es gute Gründe für die Existenz jedes dieser Dokumente geben mag, dennoch hat es einige Zeit gedauert, die jeweiligen Ziele und deren Zusammenhänge zu verstehen: Dies deutet darauf hin, dass der strategische Gesamtrahmen nicht so einfach ist, wie er sein könnte. Wir plädieren zwar nicht für eine sofortige Überarbeitung dieses Rahmens in Bezug auf Russland (was die Situation verschlimmern könnte, indem Ressourcen von der Kernarbeit der Intelligence Community in diesem Bereich abgezogen würden), empfehlen jedoch, dass die Regierung in Zukunft dafür sorgt, dass die Pläne und Prioritäten so weit wie möglich gestrafft werden. Die Zeit, die für die Strategieentwicklung aufgewendet wird, ist nur dann sinnvoll, wenn sie effizient genutzt wird und die eigentliche Arbeit nicht behindert.

Messung der Leistung von „ "

90. Wir haben die Behörden und den Militärgeheimdienst gebeten, ihre aktuelle Leistung anhand der strategischen Ziele und Pläne in Bezug auf die russische Bedrohung zu bewerten. Der Militärgeheimdienst erklärte eindeutig: *„Wir befragen unsere Kunden zu unserem Produkt auf einer Skala von null bis neun, die wir derzeit verwenden ... Die Gesamtpunktzahl für unsere gesamte Arbeit in Bezug auf Russland beträgt* ***."[105] Die Behörden konnten jedoch keine ebenso klare Bewertung abgeben. Es scheint, dass sie ihre Leistung nicht auf eine so ausgefeilte Weise messen: GCHQ und SIS teilten uns mit, dass ihre Bewertung ihrer Leistung im Hinblick auf den ICE-Plan in einem vergleichsweise weniger detaillierten Format erfolgte (das grob bewertet, ob sie die einzelnen Anforderungen übertroffen, erfüllt oder nicht erfüllt haben), und SIS teilte uns mit, dass *„die Frage des Leistungsmanagements und der Messung ... ein Prozess ist, der sich noch in der Entwicklung befindet*".[106] Die Behörden sollten ihre Leistung detaillierter messen – wir akzeptieren, dass dies keine exakte Wissenschaft ist, aber sie müssen sich ein umfassendes Bild davon machen, wie erfolgreich ihre Arbeit in Bezug auf Russland ist.

91. Wir haben versucht, uns ein Bild von der Qualität der aktuellen Berichterstattung der Behörden über Russland zu machen. Dies wurde jedoch in gewissem Maße dadurch erschwert, dass die von uns beaufsichtigten Organisationen in mündlichen Aussagen häufig auf die Ausnahmeregelung (im Justiz- und Sicherheitsgesetz von 2013) für Informationen Bezug nahmen, die sich auf laufende Operationen beziehen. Wir erinnern die Regierung daran

---

[104] Mündliche Aussagen – Verteidigungsnachrichtendienst, *** Dezember 2018.
[105] Mündliche Aussage – Verteidigungsnachrichtendienst, *** Januar 2019.
[106] Mündliche Aussage – SIS, *** Dezember 2018.

dass das Justiz- und Sicherheitsgesetz von 2013 nicht verpflichtet, Informationen über laufende Operationen zurückzuhalten, sondern lediglich die Möglichkeit dazu bietet. Die Behörden und Ministerien können freiwillig alle Informationen im Zusammenhang mit laufenden nachrichtendienstlichen oder sicherheitspolitischen Operationen bereitstellen. Obwohl wir in den meisten Fällen nicht erwarten würden, hochsensibles aktuelles operatives Material zu erhalten, ist es enttäuschend, dass diese Option in Bezug auf ein Thema von solch großem öffentlichem Interesse so umfassend genutzt wurde.

EIN SCHWIERIGES ZIEL FÜR DIE „ ”

92. Wie bereits erwähnt, ist die russische Regierung ein versierter Gegner mit gut ausgestatteten und erstklassigen offensiven und defensiven nachrichtendienstlichen Fähigkeiten. Die vielfach publizierten Fehler, die russische Agenten in Salisbury und später bei dem Versuch, die Organisation für das Verbot chemischer Waffen (OPCW) zu infiltrieren, begangen haben, haben zu öffentlichen Spekulationen über die Kompetenz der russischen Nachrichtendienste (RIS) und insbesondere des GRU geführt. Diese Angriffe zeigen zwar, dass die RIS nicht unfehlbar sind, aber es wäre töricht zu glauben, dass sie aufgrund dieser Fehler weniger gefährlich sind. Vielmehr ist es wahrscheinlich, dass die RIS aus ihren Fehlern lernen und dadurch noch schwerer zu entdecken und abzuwehren sein werden.

Eine einzigartige Herausforderung für die „ ”

93. Alle Zeugen waren sich einig, dass Russland eine der größten Herausforderungen im Bereich der Nachrichtendienste darstellt. Dafür gibt es eine Reihe von Gründen. Während es sich bei einigen um allgemeine Probleme handelt, die durch die Fähigkeit Russlands, sie auszunutzen, noch verschärft werden (z. B. ***), sind andere einzigartig für Russland (z. B. ***).

(i) Struktur

94. Der russische Entscheidungsapparat konzentriert sich auf Putin und eine kleine Gruppe vertrauenswürdiger und geheimniskrämerischer Berater (von denen viele Putins Hintergrund in der RIS teilen). Die begrenzte Anzahl von Personen, die „eingeweiht” sind, macht die Entscheidungsfindung schwer nachvollziehbar, verglichen mit Systemen, in denen Macht und Einfluss auf eine große Anzahl politischer Akteure verteilt sind. Darüber hinaus kann der Präsident schnelle Entscheidungen treffen, von denen selbst sein engster Kreis nichts weiß – was es noch schwieriger macht, die Absichten der russischen Regierung zu verstehen oder vorherzusagen.

95. Diese zentralisierte Entscheidungsfindung ermöglicht es der russischen Regierung, Entscheidungen schnell umzusetzen. Putins innerer Kreis scheint bereit und in der Lage zu sein, wichtige Entscheidungen (zum Beispiel über den Einsatz von Truppen) innerhalb weniger Tage zu treffen und umzusetzen, und er behält die strenge Kontrolle über die gesamte Regierungsinfrastruktur – die jederzeit in den Dienst der außenpolitischen Ziele Russlands gestellt werden kann. Für die demokratischen und konsensorientierten Strukturen Großbritanniens ist es schwierig, mit diesem Tempo Schritt zu halten. Putin scheint Überraschungen und Unvorhergesehenes zu schätzen und hat daher diesen „Entscheidungsvorteil” bewusst beibehalten und gepflegt, um seine Gegner auszumanövrieren.

96. Dem Ausschuss ist nicht klar, ob die britische Regierung und unsere Verbündeten bereits einen wirksamen Weg gefunden haben, um auf das Tempo der russischen Entscheidungsfindung zu reagieren. Dies hat die Fähigkeit des Westens, wirksam auf russische Aggressionen in der Vergangenheit zu reagieren, erheblich beeinträchtigt – beispielsweise auf die Annexion der Krim im Jahr 2014. [107]Im Gegensatz dazu war das Tempo der Reaktion auf den Anschlag in Salisbury beeindruckend. Allerdings ***: Es muss ein Weg gefunden werden, diese Dynamik in der gesamten Regierung aufrechtzuerhalten.

[107] Dies ist zum Teil auf die inhärenten Unterschiede zwischen dem politischen System Russlands und dem des Westens zurückzuführen.

(ii) Technologie und Daten

97. Fortschritte in der Technologie und Datenanalyse stellen alle vom Ausschuss beaufsichtigten Organisationen vor eine Reihe von Herausforderungen. Im Zusammenhang mit der Signalaufklärung (SIGINT) stellt der zunehmende Schutz der Privatsphäre – einschließlich der allgegenwärtigen Verschlüsselung – für das GCHQ ein besonderes Problem dar, und im Falle Russlands steht es vor einer echten SIGINT-Herausforderung durch die Verwendung von *** durch die russische Regierung.

98. Im Bereich der Human Intelligence (HUMINT) haben technologische Fortschritte, die Daten über Personen sammeln und analysieren, die Schwierigkeit *** generell erhöht. Die Ausweitung der Smart-City-Technologie (wie CCTV, intelligente Sensoren und die Verfolgung mobiler Geräte) und die damit verbundenen Möglichkeiten haben die Fähigkeiten von *** erhöht. [108] ***.

(iii) Das Risiko einer Eskalation

99. Verdeckte Aktivitäten gegen einen Staat bergen das Potenzial für Konflikte, und Maßnahmen gegen einen nuklear befeindeten Staat umso mehr, da die Gefahr einer Eskalation zu diplomatischen, wirtschaftlichen oder sogar militärischen Konflikten besteht. Die Geheimdienste und der Militärgeheimdienst müssen daher besonders umsichtig vorgehen ***.

100. Im Falle Russlands ist das Eskalationspotenzial besonders groß: Das russische Regime ist paranoid gegenüber westlichen Geheimdienstaktivitäten und *„nicht in der Lage, objektiv* mit“ internationaler Kritik an seinen Handlungen *umzugehen*. [109] Es betrachtet solche Schritte als Bemühungen des Westens, interne Proteste und einen Regimewechsel zu fördern. Das Risiko wird durch die Einschränkungen der Beziehungen des Vereinigten Königreichs zur russischen Regierung auf offizieller und politischer Ebene noch verstärkt, was es noch schwieriger macht, die Absichten der russischen Führung zu entschlüsseln.

Die Herausforderung „ “ meistern

(i) Fokus

101. Aufgrund der Schwierigkeit von *** hat die Geheimdienstgemeinschaft ihre Bemühungen auf *** strategische Hauptziele konzentriert, von denen sie annimmt, dass sie Einblicke in die wichtigsten strategischen Themen liefern werden, während Informationen mit der niedrigsten Priorität nur bei Gelegenheit gesammelt werden. Diese Schlüsselziele sind ***.

102. ***.[110]

103. Der SIS teilte uns mit, dass dies sowohl bei der Anwerbung von Agenten als auch bei der Aufstockung des Personals „*strategische* Geduld” erfordert. [111] Zwar gibt es eine *** Gruppe von Mitarbeitern, die sich mit diesem Thema befassen, doch stellte der SIS klar, dass eine plötzliche Aufstockung des Personals nicht zu schnelleren Ergebnissen führen würde.[112] Es ist schwierig, russische Agenten mit den richtigen Zugängen zu rekrutieren, und es bedarf einer sorgfältigen Planung, Handwerkskunst und operativen Sicherheit im Umgang mit potenziellen Agenten, um deren Sicherheit zu gewährleisten

---

[108] Mündliche Aussage – GCHQ, *** Dezember 2018.
[109] Mündliche Aussage – MI5, *** November 2018.
[110] Schriftliche Aussage – Anforderungen des ICE-Plans 2018 für Russland.
[111] Mündliche Aussage – SIS, *** Dezember 2018.
[112] Mündliche Aussage – SIS, *** Dezember 2018; wir stellen fest, dass SIS *** und über eine *„Reihe von* Schutzmaßnahmen” für die Personen verfügt, die dem Team angehören.

und minimiert politische Risiken für die britische Regierung – was bedeutet, dass es relativ lange dauert, bis die Geheimdienstarbeit Ergebnisse zeigt.

(ii) Nutzung einer Reihe von Fähigkeiten

104. Russland ist für Geheimdienstmitarbeiter anderer Länder ein besonders schwieriges Einsatzgebiet, daher ***. [113] ***. [114] Daher müssen HUMINT-Möglichkeiten anderweitig gesucht werden. Dies kann *** sein. [115]

105. Aufgrund der Schwierigkeiten, HUMINT-Quellen zu Russland zu finden und zu betreiben, stützt sich die Geheimdienstgemeinschaft auf die *„Zusammenführung einer Reihe von* Geheimdienstdisziplinen", um sich ein möglichst genaues Bild von der russischen Bedrohung zu machen.[116] In Bezug auf SIGINT hat sich das GCHQ nicht nur darauf konzentriert, eine breite Palette von Fähigkeiten gegen Russland einzusetzen, sondern sich auch mit anderen zusammengetan, um deren Fähigkeiten gemeinsam zu nutzen, wodurch sie ***.

106. Der Verteidigungsnachrichtendienst verfügt über eine Reihe spezialisierter Fähigkeiten im Bereich der georäumlichen Aufklärung (GEOINT) sowie der Mess- und Signaturerkennung (MASINT), mit denen russische Ziele aus der Ferne beobachtet werden können, wobei der Schwerpunkt auf militärischen Fähigkeiten und Organisationen liegt. Der Verteidigungsnachrichtendienst hat sich bemüht, *** *„zu verstehen, wie sie denken und warum sie so denken*".[117] Der Verteidigungsnachrichtendienst ist auch an der Erweiterung der Open-Source-Nachrichtendienstkapazitäten der britischen Regierung (d. h. der Analyse von Informationen, die im Internet frei zugänglich sind oder über kommerzielle Anbieter gekauft werden können) durch den Defence Intelligence Open Source Hub beteiligt. Die Analyse von Open-Source-Informationen wird von den Behörden und dem Verteidigungsnachrichtendienst zunehmend genutzt, um ihr allgemeines Lagebewusstsein zu verbessern, und kann mit einem geringeren Anteil geheimer Informationen kombiniert werden, um ein umfassenderes Bild zu erhalten.

(iii) Reale Bedrohungen, reale Ergebnisse

107. Der Ausschuss war überrascht über den relativ geringen Anteil der Arbeit, die die Behörden in Bezug auf Russland leisten, verglichen mit der Informationsbeschaffung über Russland. So setzt beispielsweise der SIS in der Regel nur *** seiner gesamten operativen Kapazitäten für Russland zur Unterstützung von *** ein, während der GCHQ etwa *** einsetzt. [118]

108. Uns wurde mitgeteilt, dass, da das übergeordnete Ziel der Russland-Strategie der britischen Regierung in Bezug auf Russland darin besteht, *„ein Russland* zu entwickeln*, das sich für Zusammenarbeit statt für Konfrontation* entscheidet", alle Maßnahmen in einem angemessenen Verhältnis zu diesem Ergebnis stehen müssen – insbesondere setzt die britische Regierung keine Maßnahmen ein, die auf einen Zusammenbruch der Organisation abzielen, wie dies beispielsweise bei internationalen terroristischen Gruppen der Fall sein könnte.[119] Ebenso wichtig scheint jedoch die Notwendigkeit zu sein, vorsichtig vorzugehen, um keine unerwartete Eskalation zu provozieren. Daher konzentrieren sich die Maßnahmen der Behörden in erster Linie auf ***, den Aufbau von Kapazitäten (den Austausch von Wissen und Fähigkeiten mit Partnern) und Spionageabwehrmaßnahmen zur Störung von ***-Operationen.

---

[113] Die Mitarbeiter des GCHQ und des Verteidigungsnachrichtendienstes, die sich mit Russland befassen, sind in Großbritannien stationiert.
[114] Mündliche Aussage – SIS, *** Dezember 2018.
[115] ***
[116] Mündliche Aussage – Verteidigungsnachrichtendienst, *** Dezember 2018.
[117] Mündliche Aussage – Verteidigungsnachrichtendienst, *** Dezember 2018.
[118] Mündliche Aussage – SIS und GCHQ, *** Januar 2019.
[119] Weitere Informationen hierzu finden Sie im Abschnitt „Strategie, Koordination und Aufgabenstellung" dieses Berichts.

109. Wir stellen fest, dass der Fokus auf ***-Arbeit nach den Ereignissen in Salisbury deutlich zugenommen hat, da die britische Regierung *** umfangreiche und konzertierte diplomatische Bemühungen unternommen hat, um eine starke internationale Reaktion auf den Einsatz chemischer Waffen gegen Zivilisten auf britischem Boden zu koordinieren. [120] Dies wirft die Frage auf, ob eine Rückkehr zu einem „normalen", relativ niedrigen Niveau der
*** Bemühungen gegen Russland dies untergraben würde oder ob es nun angemessener wäre, wenn die britische Regierung ihre gestärkten internationalen Beziehungen nutzen und sich stärker darauf konzentrieren würde, die feindseligen Aktivitäten Russlands auf multilateraler Ebene aufzudecken; unserer Ansicht nach muss es Letzteres sein.

[120] Die internationale Reaktion auf Salisbury wird im Abschnitt „Internationale Partnerschaften" dieses Berichts ausführlicher behandelt.

110. Angesichts der Schwierigkeiten, die mit der Bekämpfung feindlicher Aktivitäten Russlands verbunden sind, ist es unerlässlich, dass die Geheimdienste über die erforderlichen gesetzlichen Befugnisse und Instrumente verfügen. Der Innenminister stellte jedoch klar, dass *„wir noch nicht über alle Befugnisse verfügen“*.[121]

Bekämpfung von Spionage durch „Counter- “

111. Die derzeitigen Rechtsvorschriften, die Maßnahmen gegen ausländische Spione ermöglichen, gelten als unzureichend. Insbesondere die Gesetze zum Schutz von Staatsgeheimnissen sind veraltet – entscheidend ist, dass es in diesem Land nicht illegal ist, als ausländischer Agent tätig zu sein.[122]Der Generaldirektor des MI5 erklärte uns:

> *… es gibt Dinge, die wir unbedingt untersuchen müssen, von denen jeder erwartet, dass wir uns damit befassen, bei denen es jedoch aufgrund der sich wandelnden Bedrohungslage keine offensichtliche Straftat gibt, und genau das ist für mich der Punkt, an dem dies keinen Sinn ergibt.* [123]

112. Im Jahr 2017 führte die Law Commission eine Konsultation durch, in der Optionen für eine Aktualisierung der Official Secrets Acts und deren Ersatz durch ein neues „Espionage Act“ geprüft wurden. Das Ergebnis der Konsultation steht noch aus. In der Zwischenzeit forderte der Premierminister im März 2018 den Innenminister auf, *„zu prüfen, ob neue Befugnisse zur Spionageabwehr erforderlich sind, um das gesamte Spektrum feindlicher Aktivitäten ausländischer Agenten in unserem Land zu bekämpfen*”.[124]

113. In seiner Stellungnahme gegenüber uns räumte der Innenminister ein, dass die Gesetze über Staatsgeheimnisse *„völlig veraltet”* seien.[125]Der Generaldirektor des MI5 schloss sich dieser Meinung an und erklärte:

> *Der Zweck* [eines möglichen neuen Spionagegesetzes] *besteht darin, die Befugnisse zu verschärfen, die seit den Tagen des Gesetzes über Staatsgeheimnisse, das zur Hälfte für die Zeit des Ersten Weltkriegs entworfen wurde und sich mit Skizzen von Marinewerften usw. befasste, veraltet und weitgehend unwirksam geworden sind. und dann gab es 1989 eine Ergänzung dazu, aber wir haben nun etwas, das es heutzutage sehr schwierig macht, mit einigen der Situationen umzugehen, über die wir heute im Bereich der Wirtschaft, des Cyberspace und anderer Dinge sprechen, die eher mit Einfluss zu tun haben könnten.* [126]

114. Ein konkretes Problem, das ein neues Spionagegesetz angehen könnte, sind Personen, die im Auftrag einer ausländischen Macht handeln und versuchen, diese Verbindung zu verschleiern. Die USA führten 1938 das US-Gesetz zur Registrierung ausländischer Agenten (FARA) ein, das vorschreibt, dass sich alle Personen außer akkreditierten Diplomaten – sowohl US-Bürger als auch Nicht-US-Bürger –, die die Interessen ausländischer Mächte in *„politischer oder quasi-politischer* Funktion” vertreten, beim Justizministerium registrieren lassen und ihre Beziehung zur ausländischen Regierung sowie Informationen über damit verbundene Aktivitäten und Finanzen offenlegen müssen. Darüber hinaus schreibt die US-Gesetzgebung vor, dass Agenten, die keine Diplomaten sind und unter der Kontrolle ausländischer Regierungen oder ausländischer Beamter nichtpolitische Aktivitäten ausüben, den Generalstaatsanwalt benachrichtigen müssen (die Registrierung gemäß FARA dient als erforderliche

---

[121] Mündliche Aussage – Innenminister, 31. Januar 2019.
[122] Es gibt vier separate Gesetze: 1911, 1920, 1939 und 1989.
[123] Mündliche Aussage – MI5, *** Februar 2019.
[124] Mündliche Aussage – Innenminister, 31. Januar 2019.
[125] Mündliche Aussage – Innenminister, 31. Januar 2019.
[126] Mündliche Aussage – MI5, *** Januar 2019.

Meldung).[127] Jeder, der sich hätte registrieren müssen, dies aber nicht getan hat, kann strafrechtlich verfolgt und, im Falle von Nicht-US-Bürgern, abgeschoben werden.

115. Das Vereinigte Königreich verfügt über keine dem FARA entsprechenden Rechtsvorschriften, die eindeutig wertvoll wären, um dem Einfluss Russlands im Vereinigten Königreich entgegenzuwirken. Der Generaldirektor des MI5 erklärte, dass Rechtsvorschriften nach dem Vorbild des FARA Folgendes bewirken würden:

> *... die Grundlage dafür, jemanden strafrechtlich verfolgen zu können, der sich nicht zu erkennen gibt und somit verdeckt ermittelt. Wenn also jemand ein illegaler russischer Agent oder ähnliches war, ist es heute in keiner Weise strafbar, ein verdeckter Agent des russischen Geheimdienstes in Großbritannien zu sein – einfach nur das zu sein, verdeckte Kontakte zu pflegen, einen Auftrag zu verfolgen –, es sei denn, man beschafft sich schädliche Geheimnisse und gibt sie an seine Vorgesetzten weiter.* [128]

116. Wir stellen fest, dass neue Befugnisse zur Festnahme, Befragung, Durchsuchung oder Inhaftierung von Personen, die in das Vereinigte Königreich einreisen, im Februar 2019 die königliche Zustimmung erhalten haben; es ist nicht erforderlich, dass der Verdacht auf feindliche Aktivitäten besteht, um diese Befugnisse auszuüben. [129]Dies ist ein guter erster Schritt, aber mehr als ein Jahr nach dem Auftrag des Premierministers gibt es noch immer keine Anzeichen dafür, dass eine umfassendere Gesetzgebung auf den Weg gebracht wird. Der Innenminister erklärte:

> *Es handelt sich per Definition um einen komplexen Bereich. Die Law Commission hat ebenfalls in diesem Bereich gearbeitet, zu Recht unabhängig, und sie wird darüber Bericht erstatten. Ich halte es für sinnvoll, auch ihre Erkenntnisse zu berücksichtigen, bevor wir übereilt einen Gesetzesvorschlag vorlegen.* [130]

117. Wir sind uns der Notwendigkeit bewusst, die Gesetzgebung richtig zu gestalten. Dennoch ist es ganz klar, dass das System des Official Secrets Act nicht zweckmäßig ist, und je länger dies unkorrigiert bleibt, desto länger sind der Geheimdienstgemeinschaft die Hände gebunden. Es ist unerlässlich, dass es eine klare Verpflichtung gibt, neue Gesetze vorzulegen, die es ersetzen (und einen Zeitplan, innerhalb dessen es eingeführt wird), die vom MI5 genutzt werden können, um das Vereinigte Königreich gegen Agenten einer feindlichen ausländischen Macht wie Russland zu verteidigen.

Bekämpfung von Straftaten im Bereich der „ “

118. Um gegen kriminelle Aktivitäten russischer Auswanderer und derjenigen, die solche Aktivitäten ermöglichen, vorzugehen, traten im Januar 2018 im Rahmen des Criminal Finances Act 2017 (Gesetz über kriminelle Finanzen) sogenannte Unexplained Wealth Orders (Anordnungen zur Offenlegung unerklärlicher Vermögenswerte) in Kraft.[131] Diese verlangen von Personen mit unerklärlichen Vermögenswerten von über 50.000 £, Informationen über die Rechtmäßigkeit dieser Vermögenswerte vorzulegen. Die Nichtbeantwortung oder Nichtbefolgung der Anordnung kann dazu führen, dass das Vermögen in einem späteren zivilrechtlichen Rückforderungsverfahren vor dem High Court als rückforderbares Vermögen angesehen wird.

---

[127] Titel 18 des United States Code (Straftaten und Strafverfahren), Absatz 951.
[128] Mündliche Aussage – MI5, *** Januar 2019.
[129] Die Bestimmungen des Gesetzes zur Terrorismusbekämpfung und Grenzsicherheit von 2019 orientieren sich stark an den Befugnissen gemäß „Schedule 7 port stop" (Anhang 7 Hafenstopp) des Terrorism Act 2000 (Terrorismusgesetz von 2000).
[130] Mündliche Aussage – Innenminister, 31. Januar 2019.
[131] Enthalten im Gesetz über Erträge aus Straftaten von 2002, geändert durch das Gesetz über kriminelle Finanzen von 2017.

119. Die National Crime Agency (NCA) kann eine Unexplained Wealth Order (Anordnung zur Offenlegung unerklärlicher Vermögenswerte) gegen jede Person erwirken, die entweder eine politisch exponierte Person[132] von außerhalb des Europäischen Wirtschaftsraums (EWR) ist, an schweren Straftaten beteiligt ist oder mit solchen Personen in Verbindung steht. Der Sicherheitsminister erklärte gegenüber dem Ausschuss, dass Unexplained Wealth Orders eine abschreckende Wirkung hätten:

> *Wir wissen sowohl aus Geheimdienstinformationen als auch aus öffentlich zugänglichen Quellen, dass Menschen aufgrund dieser Unexplained Wealth Orders (UWO) Finanzberater konsultieren, um ihr Geld aus Großbritannien herauszuholen, und ich denke, dass diese Orders in Zukunft noch häufiger zum Einsatz kommen werden.* [133]

Der Generaldirektor der NCA warnte jedoch:

> *… unerklärlicher Reichtum muss tatsächlich unerklärlich sein, und leider … investieren Russen schon seit langer Zeit … man kann zurückverfolgen und sehen, wie sie vor Gericht argumentieren werden, dass ihr Reichtum nicht unerklärlich ist, sondern sehr klar erklärt werden kann.* [134]

Daher scheint es, dass Unexplained Wealth Orders in Bezug auf die russische Elite möglicherweise nicht so nützlich sind. Darüber hinaus gibt es praktische Probleme bei ihrer Anwendung, wie die NCA erklärte:

> *Wir sind, offen gesagt, besorgt über die Auswirkungen auf unser Budget, denn es handelt sich um wohlhabende Personen, die Zugang zu den besten Anwälten haben, und der Fall, zu dem wir eine Entscheidung getroffen haben, wurde vor allen Gerichten des Landes verhandelt. Ich habe zwar ein sehr gutes Rechtsteam innerhalb der National Crime Agency, aber für diese Arbeit mussten aus meinem relativ kleinen Budget viele Ressourcen bereitgestellt werden.* [135]

120. Ähnliche Bedenken scheinen in Bezug auf Sanktionen zu bestehen. Die NCA teilte uns mit, dass Sanktionen *„eine starke* Wirkung" auf Mitglieder der russischen Elite und ihre professionellen Unterstützer haben und *„bei ihrer Verhängung eine erhebliche primäre Störung bewirken und durch Verstöße gegen Sanktionen auch eine Reihe wirksamer sekundärer Störungen nach sich ziehen*".[136] Die NCA betonte jedoch auch, dass das Gesetz über Sanktionen und Geldwäschebekämpfung von 2018 in mehrfacher Hinsicht zu restriktiv sei. Die NCA skizzierte Änderungen, die sie sich für die Gesetzgebung wünscht:

- Einbeziehung schwerer und organisierter Kriminalität als Grund für die Verhängung von Sanktionen;[137] und

---

[132] Der Begriff „politisch exponierte Person" (PEP) wird in der Finanzregulierung verwendet, um eine Person zu bezeichnen, die mit einer bedeutenden öffentlichen Funktion betraut ist. Im Vereinigten Königreich umfasst dies alle ausländischen Personen, die im vergangenen Jahr zu irgendeinem Zeitpunkt eine wichtige öffentliche Funktion außerhalb des Vereinigten Königreichs in einem Staat oder einer internationalen Institution ausgeübt haben: Botschafter, hochrangige Militärangehörige, Mitglieder des Parlaments, Mitglieder der Vorstände von Zentralbanken und Mitglieder von Obersten Gerichten. Der PEP-Status erstreckt sich auch auf Verwandte und enge Vertraute.

[133] Mündliche Aussage – Sicherheitsminister, 31. Januar 2019.

[134] Mündliche Aussage – NCA, 24. Januar 2019.

[135] Mündliche Aussage – NCA, 24. Januar 2019.

[136] Schriftliche Aussage – NCA, 6. November 2018.

[137] Das derzeitige Sanktionsregime umfasst zwar keine schweren Straftaten, erlaubt jedoch die Verhängung von Sanktionen gegen Personen oder Organisationen aufgrund schwerwiegender Menschenrechtsverletzungen. Diese Bestimmungen wurden nach dem Anschlag in Salisbury in das Gesetz über Sanktionen und Geldwäschebekämpfung von 2018 aufgenommen. Das Gesetz über Erträge aus Straftaten von 2002 wurde ebenfalls durch das Gesetz über kriminelle Finanzen von 2017 geändert (diese Bestimmung trat im Januar 2018 in Kraft), um die Definition von „rechtswidrigem Verhalten" auf schwere Menschenrechtsverletzungen auszuweiten (sodass Erträge aus Straftaten, einschließlich schwerer Menschenrechtsverletzungen, beschlagnahmt werden können). Diese Bestimmungen werden manchmal als „Magnitsky"-Gesetzgebung des Vereinigten Königreichs bezeichnet: Das sogenannte US-amerikanische „Magnitsky Act" wurde 2012 verabschiedet, um russische Beamte zu bestrafen, die für den Tod des russischen Steuerberaters Sergei Magnitsky in einem Moskauer Gefängnis im Jahr 2009 verantwortlich waren. Dieses Gesetz enthält Bestimmungen, die es der US-Regierung ermöglichen, weltweit tätig zu werden, um die Vermögenswerte einzelner Menschenrechtsverletzer einzufrieren und ihnen die Einreise in die USA zu verbieten. Seitdem haben eine Reihe anderer Länder, darunter Kanada und die baltischen Staaten, ähnliche Gesetze eingeführt.

- Einführung von Verfahren unter Ausschluss der Öffentlichkeit zum Schutz sensibler Informationen bei der Verhängung von Sanktionen und bei Einsprüchen gegen diese (die Verfahren der Special Immigration Appeals Commission bieten hierfür ein nützliches Modell).

Wir nehmen zur Kenntnis, dass der Außenminister erklärt hat, er sei *„sehr begeistert von Sanktionen gegen Einzelpersonen, da wir alle ziemlich skeptisch sind, dass Sanktionen gegen Länder eine große Wirkung haben, und sie oft genau den Menschen schaden, denen man helfen will*".[138] Wir stimmen dem zu und unterstützen nachdrücklich die von der NCA vorgeschlagenen Gesetzesänderungen.

121. Der einzige verbleibende Bereich, in dem Handlungsbedarf besteht, betrifft das Gesetz über Computermissbrauch von 1990. Die NCA erklärte:

> *Der Computer Misuse Act … ist ein sehr veraltetes Gesetz. Es wurde zu einer Zeit entworfen, als wir noch nicht alle sechs Telefone und Computer mit uns herumtrugen, geschweige denn Kriminelle, die das Gleiche tun.* [139]

Der Computer Misuse Act sollte aktualisiert werden, um der modernen Nutzung persönlicher elektronischer Geräte Rechnung zu tragen.

Schutz der Demokratie in „ "

122. Der Sonderausschuss für Digitales, Kultur, Medien und Sport (DCMS) hat die Regierung bereits gefragt, *„ob die aktuellen Gesetze zum Schutz des Wahlprozesses vor böswilligen Eingriffen ausreichend sind. Die Gesetzgebung sollte mit den neuesten technologischen Entwicklungen Schritt halten."* Wir stellen fest, dass physische Eingriffe in die demokratischen Prozesse des Vereinigten Königreichs aufgrund der Verwendung eines papierbasierten Systems weniger wahrscheinlich sind – dennoch unterstützen wir die Forderung des DCMS-Sonderausschusses, der Wahlkommission die Befugnis zu erteilen, *„Personen, die außerhalb des Vereinigten Königreichs leben, daran zu hindern, sich illegal an einer Wahlkampagne zu beteiligen*".[140]

123. Unabhängig davon stellt sich die Frage nach dem Einfluss auf unsere demokratischen Prozesse. Es wurden Zweifel daran geäußert, ob *das* Wahlrecht angesichts *„des Übergangs von physischen Plakatwänden zu onlinebasierten, mikrotargetierten Wahlkampagnen"* noch zeitgemäß ist.[141] Wir stellen fest – und stimmen auch hier mit dem DCMS-Sonderausschuss überein –, dass *„das Vereinigte Königreich eindeutig anfällig für verdeckte digitale Einflusskampagnen ist*".[142] In diesem Zusammenhang haben wir bereits die Frage aufgeworfen, ob die Wahlkommission über ausreichende Befugnisse verfügt, um die Sicherheit demokratischer Prozesse zu gewährleisten, wenn feindliche staatliche Bedrohungen im Spiel sind. Wenn sie gegen ausländische Einmischung vorgehen soll, muss sie mit den erforderlichen Gesetzgebungsbefugnissen ausgestattet werden.

124. Wir betonen auch, dass der Fokus nicht ausschließlich auf nationalen Ereignissen und Institutionen liegen darf. Es ist wichtig, lokale Behörden einzubeziehen ***.[143] Wir sind erfreut, dass dieses Problem offenbar erkannt wurde und Maßnahmen ergriffen werden.

---

[138] Mündliche Aussage – Außenminister, 7. Februar 2019.
[139] Mündliche Aussage – NCA, 24. Januar 2019.
[140] DCMS-Sonderausschuss, *Desinformation und „Fake News"*, HC 1791, 18. Februar 2019.
[141] DCMS-Sonderausschuss, *Desinformation und „Fake News"*, HC 1791, 18. Februar 2019.
[142] DCMS-Sonderausschuss, *Desinformation und „Fake News"*, HC 1791, 18. Februar 2019.
[143] Mündliche Aussage – GCHQ, *** Februar 2019.

INTERNATIONALE PARTNERSCHAFTEN IM BEREICH DER INFORMATIONSSICHERHEIT

Zusammenarbeit mit anderen Geheimdiensten

125. Die Geheimdienste müssen sich für die Bekämpfung der russischen Bedrohung rüsten, aber wir müssen auch über die Grenzen des Vereinigten Königreichs hinausblicken. Der Kreml hat seine Bereitschaft und Fähigkeit unter Beweis gestellt, weltweit zu agieren, um den Westen zu untergraben, indem er Spaltungen sucht und diejenigen einschüchtert, die von der internationalen Gemeinschaft isoliert zu sein scheinen. Der Westen ist am stärksten, wenn er im Verbund handelt, und daher kommt den Geheimdiensten und dem Verteidigungsnachrichtendienst eine wichtige Rolle dabei zu, ihre internationalen Partner zur Zusammenarbeit zu ermutigen.

126. Bei der Reaktion auf die russische Bedrohung ist die langjährige Partnerschaft Großbritanniens mit den USA von Bedeutung. Es ist klar, dass diese Partnerschaft Großbritannien wertvolle Fähigkeiten bietet und durch eine effektive Lastenteilung Doppelarbeit vermeidet. Es bleibt jedoch die Frage, ob ***. Dies ist angesichts der relativen Priorität der Arbeit zu Russland innerhalb der Five-Eyes-Partnerschaft wichtig.

127. Die Geheimdienste und der Militärgeheimdienst arbeiten zunehmend mit *** zusammen, um der russischen Bedrohung zu begegnen. Ihre Sichtweisen sind besonders nützlich: Während die Ressourcen des Vereinigten Königreichs und des Westens Anfang der 2000er Jahre auf die Bedrohung durch den internationalen Terrorismus umgelenkt wurden, ***. Sie liefern nicht nur eine Fülle von *** Informationen über Russland, sondern teilen auch die Haltung des Vereinigten Königreichs gegenüber der russischen Bedrohung und sind bereit, gemeinsam mit dem Vereinigten Königreich eine zunehmend entschlossene Haltung gegenüber den Aktivitäten Russlands einzunehmen.

128. Andere teilen die Besorgnis Großbritanniens gegenüber Russland nicht – oder selbst wenn sie dies tun, sind sie nicht bereit, einen so entschlossenen Ansatz gegenüber den böswilligen Aktivitäten Russlands zu verfolgen. Zwar gibt es zunehmend Anzeichen dafür, dass andere europäische Länder die Bedrohung durch Russland ernster nehmen ***, doch ist es offensichtlich weniger gut gelungen, dies in öffentliche Unterstützung für den diplomatischen Ansatz Großbritanniens zur Zuordnung und Verurteilung der Cyberaktivitäten Russlands umzusetzen. Insbesondere stellen wir fest, dass Frankreich die russischen Cyberaktivitäten offenbar nicht öffentlich verurteilt hat, und es wurde vielfach berichtet, dass andere europäische Regierungen, wie beispielsweise Österreich und Italien, sich in den letzten Jahren öffentlich dem Kreml angenähert zu haben scheinen.[144] Wir nehmen auch Berichte zur Kenntnis, wonach Israel *** russische Oligarchen und deren Investitionen willkommen geheißen hat und bislang nicht bereit war, den Kreml offen herauszufordern.[145]

129. Die NATO steht weiterhin im Mittelpunkt strategischer Überlegungen: Der Kreml ist der Ansicht, dass jede weitere Erweiterung der NATO einen Verstoß gegen die NATO-Russland-Grundakte von 1997 und einen inakzeptablen Eingriff in seinen vermeintlichen „Einflussbereich" darstellen würde. Die Schwächung der NATO ist daher ein wichtiges Ziel des Kremls, ebenso wie die Untergrabung der Glaubwürdigkeit von Artikel V des Nordatlantikvertrags von 1949 [146], weshalb *die „Abschreckung durch die NATO und Nicht-NATO*-Staaten" ein wesentlicher Bestandteil der Russland-Strategie 2019 der britischen Regierung ist.

130. *Wir* sehen es als ermutigend an, dass der Militärgeheimdienst seine Geheimdienstbewertungen mit der NATO teilt, was, wie uns gesagt wurde, darauf abzielt, *„ein möglichst einheitliches Verständnis der*

---

[144] „Der Aufstieg der extremen Rechten in Italien und Österreich verschafft Putin einige Freunde im Westen", *The Guardian*, 7. Juni 2018.

[145] „Russische Oligarchen in Israel: Willkommen im gelobten Land", *The Economist*, 17. September 2015.

[146] Artikel V des Nordatlantikvertrags von 1949 betrifft den Grundsatz der „kollektiven Selbstverteidigung" und besagt, dass ein bewaffneter Angriff gegen einen oder mehrere NATO-Mitglieder als Angriff gegen alle angesehen wird und dass alle NATO-Mitglieder Maßnahmen ergreifen werden, um den Angriff gegen den/die betroffenen Mitgliedstaat(en) abzuwehren.

Art der russischen Bedrohung und die Situation, mit der wir konfrontiert sind". Der Verteidigungsnachrichtendienst hob mehrere *„wirklich wichtige* Aspekte *unserer Arbeit für das* NATO-System" hervor, darunter *„die sehr enge Zusammenarbeit mit NATO-Kollegen, die Weitergabe von Einschätzungen an die NATO* [und] *die sehr enge Zusammenarbeit mit der NATO Intelligence Fusion Cell in RAF Molesworth*".[147]

Anderen helfen, uns zu helfen

131. Einige Partner, mit denen das Vereinigte Königreich eng zusammenarbeiten möchte, verfügen jedoch nicht über die erforderlichen nachrichtendienstlichen Kapazitäten. ***.

132. Was sein „nahes Ausland" betrifft, so beabsichtigt Russland eindeutig, diese Länder in seinem „Einflussbereich" zu halten, und führt zu diesem Zweck Cyberaktivitäten durch und verfolgt eine entsprechende Wirtschaftspolitik in ***. Initiativen der britischen Regierung *** sind daher unerlässlich. Wir stellen jedoch fest, dass es sich hierbei nicht um ein kurzfristiges Projekt handelt: Gegen den russischen Einfluss sind kontinuierliche Investitionen und eine langfristige Strategie erforderlich ***.

Die internationale Reaktion auf den „ " in Salisbury

133. Nach dem Angriff der GRU in Salisbury war es das Ziel des Vereinigten Königreichs, schnell zu reagieren und – in dem Bewusstsein, dass Russland sich nicht sonderlich um individuelle Vergeltungsmaßnahmen sorgt – alle Maßnahmen gegen Russland zu „internationalisieren", indem eine möglichst breite Koalition gebildet wurde.[148] Die britische Regierung (***) unternahm diplomatische Bemühungen, um den Verbündeten die Beweise für den Angriff vorzulegen und sie davon zu überzeugen, sich dem Vereinigten Königreich anzuschließen und Maßnahmen in Form von Ausweisungen und verschärften Sanktionen zu ergreifen.

134. Wie bereits erwähnt, war die daraus resultierende Ausweisung von 153 russischen Geheimdienstmitarbeitern und Diplomaten aus 29 Ländern und der NATO eine beispiellose internationale Reaktion. [149] Zwar war die Tatsache, dass chemische Waffen eingesetzt wurden – was einen klaren Verstoß gegen das Völkerrecht darstellt und die Verurteilung der internationalen Gemeinschaft nach sich zog – zweifellos ein Faktor, der die Länder davon überzeugte, sich mit dem Vereinigten Königreich zusammenzuschließen, doch erleichterte die schnelle und koordinierte Reaktion der
*** HMG, die den Partnern Beweise und Sicherheit lieferte, machte es ihnen leichter, sich der öffentlichen Verurteilung anzuschließen.

135. Diese diplomatische Reaktion und die anschließende Entlarvung der verantwortlichen GRU-Agenten sendeten eine deutliche Botschaft an Russland, dass solche Handlungen nicht toleriert werden, und bieten eine Plattform für die Zukunft. Uns wurde gesagt, dass

> [Salisbury] *die Dynamik verändert hat ...* [und] *unter den Ländern, die sich von Russland bedroht fühlen, wächst das Bewusstsein, dass es sowohl durch Zusammenarbeit im Bereich der Nachrichtendienste und Sicherheit als auch auf diplomatischer Ebene Möglichkeiten gibt, reale Auswirkungen gegen Russland zu erzielen, und das fühlt sich ganz anders an. Das scheint ein sehr positives Ergebnis einer Krise zu sein.* [150]

---

[147] Mündliche Aussage – Verteidigungsnachrichtendienst, *** Januar 2019.

[148] ***

[149] Dies steht in krassem Gegensatz zu der langsamen und isolierten Reaktion der britischen Regierung auf die russische Aggression nach der Ermordung von Alexander Litvinenko im Jahr 2006 (obwohl in diesem Fall eine radioaktive Substanz verwendet wurde).

[150] Mündliche Aussage – SIS, *** Dezember 2018. Der Verteidigungsnachrichtendienst stellte außerdem fest, dass die Auswirkungen des Anschlags von Salisbury auf die NATO-Nachrichtendienste *„im Hinblick auf die Stärkung des Einzelnen erheblich* waren", und merkte an, dass *** (mündliche Aussage – Verteidigungsnachrichtendienst, *** Februar 2019).

Wir sind uns bewusst, wie viel Aufwand dafür erforderlich war, und sprechen allen Beteiligten unsere Anerkennung für ihre harte Arbeit aus.

e Dynamik aufrechterhalten

136. Salisbury darf nicht zum Höhepunkt der internationalen Einigkeit über die Bedrohung durch Russland werden: Es bedarf einer kohärenten und nachhaltigen Strategie, um auf diesem Erfolg aufzubauen und sicherzustellen, dass diese Lehren für ähnliche Ereignisse, sei es gegen das Vereinigte Königreich oder seine Verbündeten, verinnerlicht werden. Es ist klar, dass die Eindämmung russischer Aktivitäten in Zukunft davon abhängen wird, dass der Preis, den die Russen für solche Einmischungen zahlen, hoch genug ist. Die Geheimdienste müssen sicherstellen, dass die private Zusammenarbeit die fortgesetzte öffentliche Aufdeckung russischer Aktivitäten unterstützt und ergänzt und dass eine breite internationale Koalition aufgebaut wird, die bereit ist, schnell und entschlossen gegen russische Aggressionen vorzugehen.

Strebt Russland Allianzen auf der Grundlage von „ “ an?

137. Im Gegensatz zum Westen steht Russland dem Aufbau bedeutender internationaler Partnerschaften traditionell skeptisch gegenüber. Wir stellen jedoch fest, dass es in den letzten Jahren weltweit proaktiv nach „Allianzen der Zweckmäßigkeit" gesucht hat. Dazu gehören eine vertiefte Zusammenarbeit mit China im Bereich Verteidigung und Sicherheit als nützlicher Partner gegen die USA (die sogar gemeinsame Militärübungen umfasst), ein verstärkter Einfluss in Südamerika und ein substanzielles Engagement in mehreren afrikanischen Ländern, einschließlich weitreichender Handelskampagnen. [151]

138. Russland hat auch versucht, seinen Einfluss im Nahen Osten auszuweiten. Obwohl Einigkeit darüber besteht, dass Russlands Ausnutzung des Machtvakuums in Syrien *„einer der größten* Rückschläge" [152]für die britische Außenpolitik im Jahr 2018 war, sind wir nach wie vor der Ansicht, dass Großbritannien keine klare Strategie in dieser Frage verfolgt. Russland betrachtet seine Intervention zur Unterstützung des Assad-Regimes als Erfolg, und es ist offensichtlich, dass seine Präsenz in Syrien es dem Westen erschwert, den Frieden in der Region zu unterstützen. Die verstärkten Beziehungen Russlands zum Iran und seine Handelsinitiativen mit einer Reihe von Ländern in der Golfregion verkomplizieren die Situation zusätzlich. Wenn die britische Regierung zu Frieden und Sicherheit im Nahen Osten beitragen will, muss die Geheimdienstgemeinschaft ***, und Großbritannien muss eine klare Strategie haben, wie dies angegangen werden soll.

[151] Im September 2018 führte Russland gemeinsam mit chinesischen und mongolischen Streitkräften die Militärübung „VOSTOK 2018" durch.
[152] Mündliche Aussage – Außenminister, 7. Februar 2019.

Russlands Rückzug aus der internationalen Gemeinschaft

139. Wie bereits erwähnt, gab es nach dem Ende des Kalten Krieges und der Auflösung der UdSSR konzertierte Bemühungen des Westens, Russland als potenziellen zukünftigen Partner in die regelbasierte internationale Ordnung einzubinden. Nach der Wahl Putins zum Präsidenten im Jahr 2000 zeigte sich die russische Regierung jedoch zunehmend aktiv feindselig gegenüber Großbritannien und dem Westen und grundsätzlich nicht bereit, sich an internationale Gesetze und Normen zu halten.

140. Die russische Regierung strebt eine Zusammenarbeit nur zu ihren Bedingungen an: Sie gibt Lippenbekenntnisse zu besseren Beziehungen mit Großbritannien ab und strebt mehr wirtschaftliche Zusammenarbeit an, missachtet dabei jedoch die Souveränität Großbritanniens und – im Fall des Skripal-Anschlags – die grundlegendsten internationalen Prinzipien zum Verbot chemischer Waffen.

Der Zweck der Kommunikation „ “

141. Die Frage ist, wie Großbritannien darauf reagiert, und dabei ist es wichtig, zwischen öffentlichen „Botschaften“ und „Hintertürchen“ der Kommunikation zu unterscheiden, die für eine Deeskalation in Krisenzeiten unerlässlich sind.

142. Nach einer Unterbrechung der Beziehungen im Jahr 2007 nach der Ermordung von Alexander Litvinenko wurden die Kommunikationskanäle mit Russland 2013 wieder geöffnet, um den Austausch von Informationen über die terroristische Bedrohung der Olympischen Spiele in Sotschi zu ermöglichen.[153]Diese wurden nach den Spielen 2014 wieder geschlossen, aber 2016 vor der Fußball-Europameisterschaft wieder geöffnet und im Vorfeld der Fußball-Weltmeisterschaft 2018 offen gehalten, um die Sicherheit russischer Staatsbürger, die das Vereinigte Königreich besuchen, bzw. britischer Staatsbürger, die Russland besuchen, zu gewährleisten. *** Eine proaktivere Zusammenarbeit oder der Aufbau von Beziehungen wurden kürzlich ebenso wie geplante ministerielle Kontakte eingefroren.

143. Begrenzte Kommunikationskanäle mit der russischen Regierung können von Vorteil sein. Die Möglichkeit direkter Gespräche ermöglicht es, in Krisenzeiten die Absichten beider Seiten zu verstehen – ***. Durch solche Kanäle kann daher das Risiko von Missverständnissen und einer Eskalation der Feindseligkeiten verringert werden. Außerdem bieten sie die Möglichkeit, militärische Aktivitäten in Gebieten, in denen sowohl Großbritannien als auch Russland militärisch präsent sind, zu entschärfen.

Die richtige Botschaft „ “ senden

144. Es ist dennoch auffällig, dass zwei der fünf „Säulen“ [154]der Russland-Strategie der britischen Regierung nach wie vor auf eine proaktive Zusammenarbeit und den Aufbau von Beziehungen zu Russland ausgerichtet sind, die über die notwendige Kommunikation hinausgehen [155].Zwar ist es möglich, dass eine Verbesserung der Beziehungen zwischen Russland und Großbritannien eines Tages die Bedrohung für Großbritannien verringern könnte, doch ist es unrealistisch zu glauben, dass dies unter der derzeitigen russischen Führung geschehen könnte. Dies würde davon abhängen, dass Russland seine Aggressionen gegenüber Großbritannien, wie beispielsweise den Einsatz chemischer Waffen, einstellt.

---

153 ***

154 Wir stellen jedoch fest, dass diese beiden Säulen nur einen sehr kleinen Teil der Gesamtmaßnahmen ausmachen.

155 Die ressortübergreifende Russland-Strategie zielt auf eine Zusammenarbeit sowohl mit der russischen Zivilgesellschaft als auch mit der russischen Regierung ab.

auf britischem Boden. Als westliche Demokratie kann Großbritannien nicht zulassen, dass Russland die regelbasierte internationale Ordnung missachtet, ohne dass dies entsprechende Konsequenzen nach sich zieht. Jeder öffentliche Schritt in Richtung einer engeren Allianz mit Russland würde derzeit die Stärke der internationalen Reaktion auf Salisbury sowie die Führungsrolle und Glaubwürdigkeit Großbritanniens innerhalb dieser Bewegung erheblich untergraben.

ZEUGEN

Minister

Jeremy Hunt, MP – damaliger Außenminister Sajid Javid, MP

– damaliger Innenminister Ben Wallace, MP – damaliger

Sicherheitsminister

Beamte

KABINETTSAMT

Madeleine Alessandri CMG – damals stellvertretende nationale Sicherheitsberaterin

Sir Charles Farr CMG OBE – ehemaliger Vorsitzender des Gemeinsamen

Geheimdienstausschusses Weitere Beamte

VERTEIDIGUNGSNAHME

Lt Gen. Jim Hockenhull OBE – Chef des Verteidigungsnachrichtendienstes

Weitere Beamte

AUSSEN- UND GEMEINSCHAFTSMINISTERIUM

Sir Philip Barton KCMG OBE – damals Generaldirektor für Konsular- und Sicherheitsangelegenheiten im Außenministerium und regierungsübergreifender Senior Responsible Owner für Russland

Weitere Beamte

REGIERUNGSKOMMUNIKATIONSZENTRALE

Jeremy Fleming – Direktor, GCHQ Weitere

Beamte

NATIONALE KRIMINALPOLIZEI

Frau Lynne Owens CBE QPM – Generaldirektorin, NCA

Weitere Beamte

AMT FÜR SICHERHEIT UND TERRORISMUSBEKÄMPFUNG

Tom Hurd OBE – Generaldirektor, OSCT Weitere Beamte

GEHEIMDIENST (MI6)

Sir Alex Younger KCMG – Chef, SIS Weitere

Beamte

SICHERHEITSDIENST (MI5)

Sir Andrew Parker KCB – damaliger Generaldirektor, Sicherheitsdienst Weitere

Beamte

Externe Sachverständige

Professor Anne Applebaum – Institut für globale Angelegenheiten

William Browder – Leiter der Global Magnitsky Justice Movement Christopher

Donnelly CMG TD – Leiter des Institute for Statecraft

Edward Lucas – Autor und Berater mit Schwerpunkt auf europäischer und transatlantischer Sicherheit

Christopher Steele – Direktor, Orbis Business Intelligence Ltd

ANHANG

***

VERTRAULICHE MÜNDLICHE UND SCHRIFTLICHE BEWEISE VON

“
”

***

CCS0221966010
978-1-5286-1686-7