Bundesamt für
Verfassungsschutz

Gefährdungen durch russische Spionage, Sabotage und Desinformation

Momentaufnahme und Einordnung

Gefährdungen durch russische Spionage, Sabotage und Desinformation

Momentaufnahme und Einordnung

Inhalt

Kapitel 1

Einleitung

Die Gefahren durch Spionage[1], Sabotage[2] und Desinformation[3] sind mit dem russischen Angriffskrieg auf die Ukraine seit 2022 stark gestiegen. Während die Hemmschwelle für Aktionen gegen Deutschland auf russischer Seite gesunken ist, zeigt der in Europa verzeichnete Anstieg von Vorfällen, die auch in der Öffentlichkeit Aufmerksamkeit

1 Spionage ist das Erkunden von politischen Faktoren sowie der wirtschaftlichen, wissenschaftlichen und militärischen Potenziale eines anderen Staates mit verdeckten Mitteln. Sie ist bei der Nutzung von Staatsbürgern und Geheimnisträgern eines anderen Staates nach dessen Gesetzen strafbar. Bei Spionage gegen Deutschland kommt eine Strafbarkeit gemäß §§ 93 ff. Strafgesetzbuch (StGB) in Betracht.

2 Sabotage ist die bewusste Beeinträchtigung wirtschaftlicher, militärischer oder politischer Prozesse. Dies kann durch die Beschädigung oder Zerstörung wichtiger Anlagen und Einrichtungen erfolgen, insbesondere im Bereich Kritischer Infrastrukturen (KRITS, zum Beispiel Kraftwerke, Verkehrsverbindungen oder Kommunikationsanlagen).

3 Desinformation ist die Verbreitung falscher oder irreführender Informationen, um Einzelpersonen, Gruppen oder die öffentliche Meinung als Ganzes zu beeinflussen. Eine Desinformation liegt vor, wenn sie nach objektiven Maßstäben inhaltlich unzutreffend ist, der Urheber dies weiß und sie dennoch mit dem Ziel der Beeinflussung verwendet. Gleiches gilt für das Verschweigen wesentlicher Teile einer Information. Desinformationsaktivitäten sollen Emotionen, Wahrnehmungen und Einstellungen verändern. Sie sind ein klassisches Instrument fremder Nachrichtendienste. Diese unterstützen damit ihre Regierungen beim Ausbau der politischen, wirtschaftlichen oder strategischen Positionen sowie der internationalen Reputation.

erzeugen, dass Russland den Einsatz von Gewalt als legitimes Mittel betrachtet. Dabei wird gezielt der öffentliche Raum als Resonanzkörper genutzt. Diese Gefährdung für die innere Sicherheit umfasst auch klandestine Aktivitäten der russischen Nachrichtendienste. Es wird jedoch deutlich, dass Aktionen mit einer für die Öffentlichkeit wahrnehmbaren Komponente – etwa die in der Presse wiederholt thematisierten und zum Teil möglicherweise von Russland gesteuerten Drohnenüberflüge über militärische Liegenschaften und weitere sensible Bereiche, Cyberangriffe gegen öffentliche Stellen und Unternehmen, unzulässige Einflussnahme[4] sowie Sabotagehandlungen und die Flankierung entsprechender Aktivitäten durch Propaganda[5] – für Russland ebenfalls Mittel der Machtdemonstration und der Einschüchterung darstellen.

Das BfV klärt solche Aktivitäten auf und wirkt daran mit, Aufmerksamkeit für die vielfältigen und sich wandelnden Aktivitäten der russischen Dienste in Deutschland zu schaffen. Denn diese gehen seit 2022 zunehmend offensiv gegen die europäischen Demokratien und damit auch Deutschland vor.

4 Staaten verfolgen ihre Interessen über eine Vielzahl zulässiger, meist diplomatischer Aktivitäten. Darüber hinaus gibt es aber auch unzulässige Einflussnahmeaktivitäten. Diese erfolgen eher im Verborgenen, unter Vortäuschung falscher Tatsachen und teilweise unter Einsatz von Nachrichtendiensten. Sie sollen auf Meinungs- und Willensbildungsprozesse sowie Entscheidungs- und Funktionsträger anderer Staaten einwirken, das Vertrauen der Bevölkerung in die Institutionen und die Mechanismen der Demokratie schwächen oder Bündnisse untergraben.

5 Mit Propaganda wollen Staaten die öffentliche Meinung anderer Staaten beeinflussen, um eine gewünschte Reaktion oder Haltung zu erzeugen. Maßgeblich ist nicht der Wahrheitsgehalt einer Nachricht, sondern die geschickte Auswahl beziehungsweise die Manipulation einer Nachricht.

Kapitel 2

Vielzahl von Akteuren und Mix an Methoden

Eine Gemengelage von staatlichen, staatlich gesteuerten sowie privaten Akteuren prägt 2025 die nachrichtendienstliche Bedrohungslage durch Russland. Diese Vermengung ist zugleich auch ein Grund, warum Aufklärung, Abwehr und Resilienz eine kontinuierliche Herausforderung darstellen.

Auf die aktuelle Gefährdungslage in Europa wirken neben den russischen Nachrichtendiensten auch andere Stellen im russischen Staatsapparat, insbesondere die staatlichen Medien, mit ein. Daneben werden durch Russland halbstaatliche Stellen wie Staatsunternehmen oder staatlich gesteuerte Einrichtungen wie Thinktanks oder Wissenschaftseinrichtungen für illegitime Aktivitäten eingesetzt. Hinzu kommen private Akteure wie prorussische Hacktivisten, die immer wieder versuchen, auch deutsche Stellen mit Cyberangriffen, unter anderem DDoS-Attacken, zu beeinträchtigen. Auch bei Desinformationsaktivitäten kommen externe Akteure zum Einsatz, wie zum Beispiel das russische IT- und Kommunikationsunternehmen Social Design Agency (SDA), das seit Jahren im Bereich Desinformation tätig ist und deshalb bereits 2023 von der EU sanktioniert wurde.

Hinzu kommt, dass Russland seine Angriffsmethoden als langjähriger nachrichtendienstlicher Akteur fortlaufend weiterentwickelt und an die aktuellen Gegebenheiten anpasst. Dabei profitieren die russischen Nachrichtendienste von erheb-

lichen Ressourcen, dem Zugriff auf den ganzen Staatsapparat und ihren methodischen Erfahrungen aus den Zeiten der Sowjetunion. Einzelne Vorgehensweisen werden zu komplexeren Operationen kombiniert beziehungsweise verknüpft. Insgesamt können sich die russischen Nachrichtendienste aus einem großen Werkzeugkasten bedienen und verschiedene Werkzeuge lageangepasst, entweder einzeln oder auch gleichzeitig, einsetzen. Dieser Mix von Methoden findet gegen eine Vielzahl von Angriffszielen Anwendung.

Das Schaubild dieses russischen Werkzeugkastens – die „Toolbox Russland" – bildet skizzenhaft die zur Verfügung stehenden Mittel Russlands ab.[6] Diese umfassen Methoden, die in Deutschland eingesetzt werden beziehungsweise nach Deutschland reichen bis hin zu Aktivitäten in Russland, die neben der einheimischen Bevölkerung auch gegen deutsche Staatsangehörige und Stellen in Russland wirken.

Gegenwärtig verdienen dabei drei Positionen besondere Aufmerksamkeit:

- Spionage, die als Reaktion auf das gestiegene Informationsbedürfnis Russlands seit Kriegsbeginn als Handlungsoption auch im Cyberraum wichtiger geworden ist,
- die Bereitschaft Russlands für Sabotage, die neben Schäden auch Unsicherheit und Angst erzeugen soll,
- wie auch Einflussnahmeaktivitäten, die im Zusammenhang mit der Bundestagswahl 2025 durch Desinformation und Propaganda signifikant zu verzeichnen waren.

6 Die 2023 veröffentlichte „Toolbox Russland" wurde im Januar 2025 auf dem X-Kanal des BfV in einer aktualisierten Form verbreitet, vgl. auch www.verfassungsschutz.de.

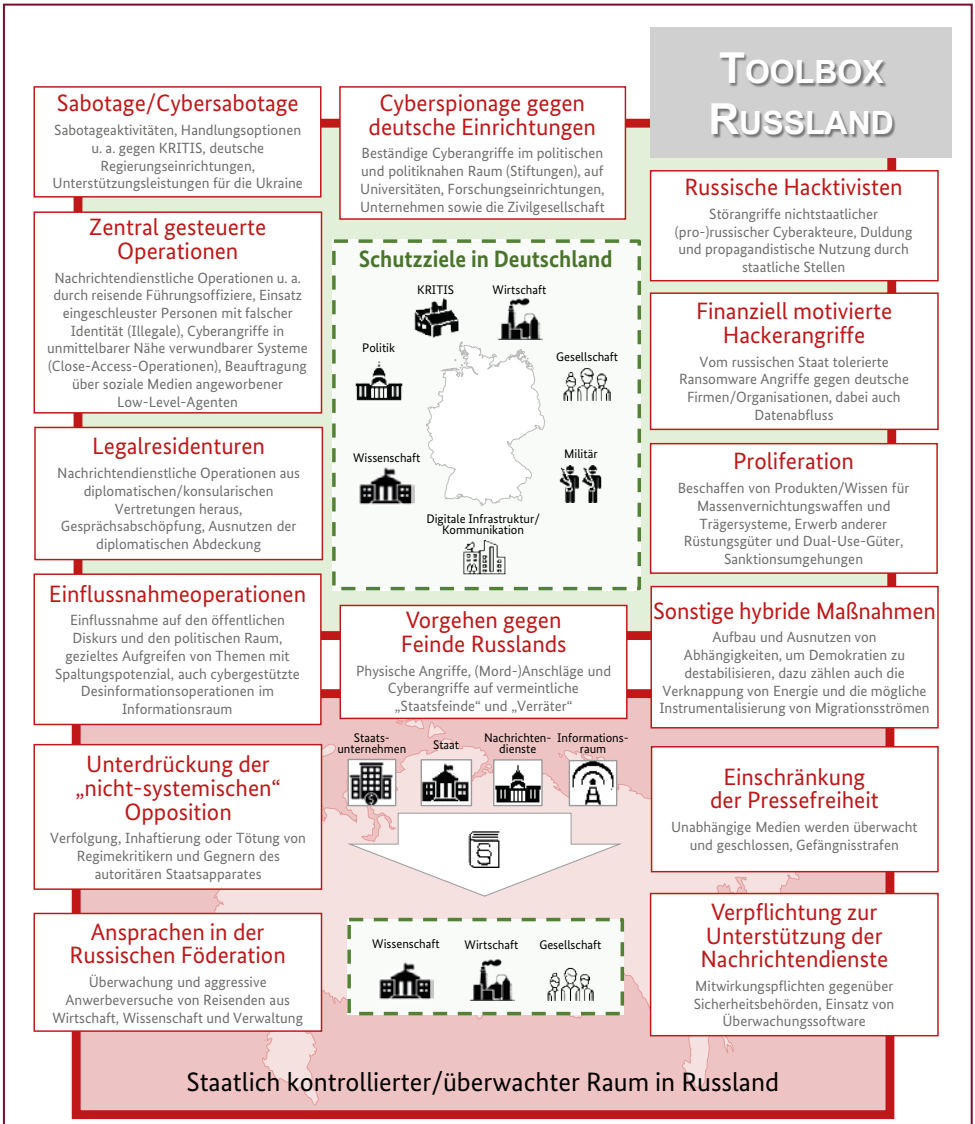


Schaubild des russischen „Werkzeugkastens“

Kapitel 3

Spionage

Mit Spionage beschaffen Nachrichtendienste – durch den Einsatz menschlicher Quellen wie auch durch Cyberangriffe – sensible Informationen anderer Staaten aus Bereichen wie Politik, Militär, Wirtschaft oder Wissenschaft. Das können zum Beispiel Pläne und Konzepte von Regierungen oder Parteien, Funktionsweisen von Waffensystemen, Strategien von Unternehmen oder Erkenntnisse von Forschungsinstituten sein.

Der Angriffskrieg gegen die Ukraine hat wie ein Katalysator auf die Tätigkeiten der russischen Nachrichtendienste gewirkt. Die wahrnehmbare Verschiebung ihrer Aufklärungsschwerpunkte erklärt sich mit der politischen Unterstützung der Ukraine sowie der Bedeutung Deutschlands als wichtiges Drehkreuz für zivile und militärische Hilfsleistungen. Für Deutschland sind damit einhergehend die Risiken im politischen Raum, in Wirtschaft, Wissenschaft und Gesellschaft wie auch im Cyber- und Informationsraum deutlich gestiegen. Im Aufklärungsfokus Russlands stehen neben Politik und Verwaltung gegenwärtig insbesondere militärische Liegenschaften sowie Sektoren der Kritischen Infrastrukturen (KRITIS[7]) wie die Logistik.

Auch der maritime Raum ist Teil der umfassenden Bemühungen Russlands, Dominanz in Europa zurück-

7 KRITIS ist die Abkürzung für Kritische Infrastrukturen. Damit sind Anlagen, Systeme und Organisationen gemeint, die eine wichtige Bedeutung für die Aufrechterhaltung gesellschaftlicher Funktionen haben. Deren Ausfall hätte erhebliche Auswirkungen auf das Gemeinwesen, zum Beispiel in Form von Versorgungsengpässen und Gefährdungen der öffentlichen Sicherheit. In Deutschland zählen mehrere Sektoren zu KRITIS, wie Einrichtungen aus den Bereichen Energieversorgung, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Siedlungsabfallentsorgung, Finanz- und Versicherungswesen, Staat und Verwaltung, Medien und Kultur.

zugewinnen und seinen Handlungsspielraum zu demonstrieren. So besteht insbesondere in der Ostsee eine anhaltende Gefährdung durch hybride Maßnahmen Russlands. In den letzten Jahren wurde deutlich, dass die maritime KRITIS in den Bereichen Energie und Telekommunikation immer wichtiger geworden ist, aber gleichzeitig – wie verschiedene Vorfälle in der Ostsee aufzeigen – auch verletzlich ist. Das BfV leistet mit seiner Zuständigkeit für die Cyber- und Spionageabwehr im Zusammenspiel mit anderen Bundes- und Landesbehörden deshalb auch einen Beitrag, Spionage und Sabotage gegen deutsche Interessen auf und in Nord- und Ostsee aufzuklären und abzuwehren.

Die russischen Dienste sind durch die europaweite Ausweisung mehrerer hundert Nachrichtendienstangehöriger seit 2022 gezwungen, ihr übliches Vorgehen der Informationsbeschaffung aus Legalresidenturen[8] mit weiteren nachrichtendienstlichen Methoden zu ergänzen. Vor diesem Hintergrund beobachtet das BfV das Agieren der russischen Nachrichtendienste besonders aufmerksam und passt seine analytisch-methodische Arbeit fortlaufend an.

Verschiedene zum Einsatz kommende Formen der Informationsbeschaffung können unter Spionage gefasst werden: So können mit Satelliten oder Drohnen Kasernen und Fabriken ausgekundschaftet oder mit Abhöreinrichtungen Funk und andere elektronische Kommunikation abgehört und/oder aufgezeichnet werden. Aber auch die intensiven Cyberangriffe dienen der Informationsbeschaffung. Beispielhaft dafür stehen die Angriffe des russischen Cyberakteurs APT 28. Zuletzt fanden unter anderem Cyberangriffe auf den Transport- und Logistiksektor sowie politiknahe Einrichtungen statt. Dabei konnten die Angreifer sehr wahrscheinlich auch sensible Daten aus IT-Netzwerken der Opfer ausleiten. Darüber hinaus kann Spionage mit menschlichen Quellen wie mit Cyberangriffen auch ein Teil von Vorbereitungshandlungen für Sabotage sein – beispielsweise wenn Schwachstellen, potenzielle Ziele, Schutzmaßnahmen oder auch mögliche Reaktionen ausgekundschaftet werden.

8 Eine Residentur ist ein getarnter Stützpunkt eines ausländischen Nachrichtendienstes im Operationsgebiet. Befindet sich der Stützpunkt in einer offiziellen oder halboffiziellen Vertretung, wie einer Botschaft oder Handelsvertretung, spricht man von einer Legalresidentur.

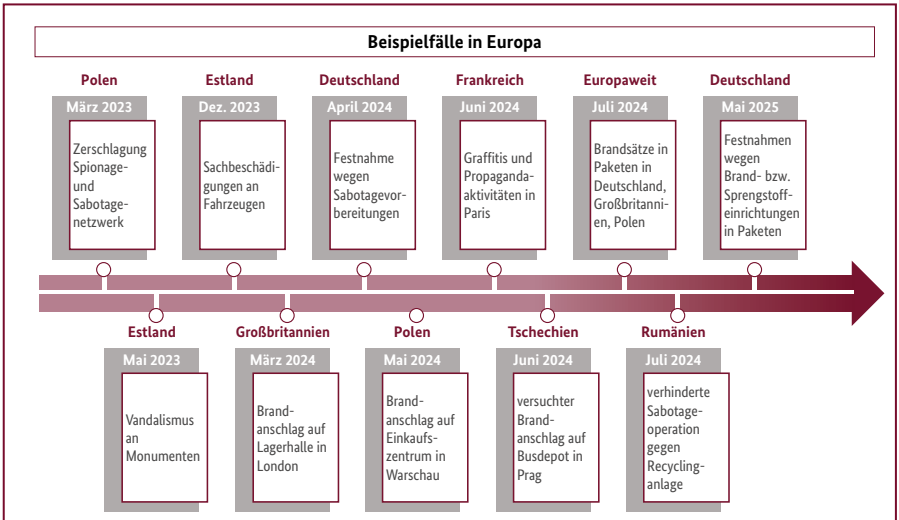
Kapitel 4

Sabotage

Jahrelang wurden Sabotageaktivitäten vorrangig von extremistischen und terroristischen Akteuren durchgeführt. Doch spätestens seit 2023 sieht sich Deutschland mit einer in dieser Form neuen Bedrohung konfrontiert: Sabotage durch fremde Nachrichtendienste. Insbesondere seit dem Jahr 2024 geht die Spionageabwehr einer Reihe von ungeklärten Vorfällen nach, die möglicherweise im Zusammenhang mit Sabotagehandlungen im russischen Auftrag stehen.

Cyberattacken, Sachbeschädigungen und Brandsätze sind nur einige Beispiele für mögliche Aktivitäten, die nicht nur einen Sachschaden oder die Störung von Prozessen zum Ziel haben, sondern Unsicherheiten schüren, Angst verbreiten sowie Sicherheitsbehörden und Politik überlasten sollen.

2024 kam es in mehreren europäischen Ländern zu Vorfällen wie Bränden, Ausspähungen von Menschen und Einrichtungen, Drohnensichtungen über sensiblen Bereichen von Verteidigung und KRITIS sowie Cyberangriffen. Auch nach sorgfältiger Prüfung können Verantwortliche nicht immer zweifelsfrei identifiziert werden. Während bei manchen Fällen ein Sabotagehintergrund wahrscheinlich ist, sind bei einer Reihe von Vorfällen keine Hinweise auf eine staatliche Steuerung auszumachen. Dennoch besteht aufgrund der sich zuspitzenden Konfrontation Russlands mit den europäischen Demokratien sowie der Bereitschaft Russlands zu Sabotageaktionen eine erhöhte Gefährdung der inneren Sicherheit und infolgedessen eine ausgeprägte Wachsamkeit der Sicherheitsbehörden.



Ereignisse mit mutmaßlich russischem Hintergrund

Sabotage umfasst die bewusste Beeinträchtigung militärischer, politischer oder produktionsbezogener Prozesse, einschließlich der Supply-Chain-Ketten[9]. Dies kann auch zur Beschädigung oder Zerstörung wichtiger Anlagen und Einrichtungen von KRITIS führen, die für das Gemeinwesen unverzichtbar sind. Möglich sind zudem verschiedene Gewalttaten wie Brandstiftungen, gefährliche Eingriffe in den Bahn-, Luft-, Schiffs- und Straßenverkehr oder Straftaten wie Sachbeschädigungen oder andere Formen der Störung von Abläufen.

Neuartig bei der russischen Vorgehensweise ist der Einsatz von niederschwellig rekrutierten Low-Level-Agenten[10], die als Handlanger fungieren und im Auftrag russischer Stellen Aktionen wie Ausspähung, Propaganda oder Sabotage ausführen. Dabei handelt es sich um Personen, die für russische Nachrich-

9 Bei einem Supply-Chain-Angriff wird zunächst nicht direkt das eigentliche Ziel mit einem Cyberangriff attackiert, sondern ein schwächer geschütztes Element in der Liefer- oder Versorgungskette. Die Kompromittierung des schwächer geschützten Elements ermöglicht dann den Angriff auf das eigentliche Ziel.

10 Der Begriff „Low-Level-Agent“ beschreibt Personen, die im Interesse eines gegnerischen fremden Nachrichtendienstes oder sonstiger Staatsorgane tätig werden, ohne diesem selbst anzugehören. Neben dem Begriff „Low-Level-Agent“ tauchen in der Presse auch Synonyme wie „Proxy“, „Wegwerf-Agenten“ oder „Taschengeld-Agenten“ auf.

tendienste oder sonstige staatliche Organe tätig werden, ohne diesen selbst anzugehören. Die oftmals (klein-)kriminellen Akteure werden häufig über soziale Medien oder Messengerdienste angeworben und gesteuert. Sie agieren zumeist aus finanziellen Beweggründen, jedoch kann zugleich auch eine ideologische Motivation vorliegen. Der nachrichtendienstliche Hintergrund des Auftraggebers bleibt ihnen dabei mutmaßlich oft verborgen – auch aufgrund von undurchsichtigen Auftragsketten mit zwischengeschalteten Mittelsmännern.

Sabotage stellt für verschiedene Sektoren eine ernst zu nehmende Gefahr dar. Die im Sommer 2024 auch per Luftfracht versandten Brandsätze in Paketen stehen dafür beispielhaft. Aber auch weitere Lebensbereiche und die Bevölkerung können mittel- und unmittelbar betroffen sein, beispielsweise durch mögliche Energieversorgungsengpässe in Folge eines Sabotageaktes. Zudem können umgesetzte Sabotagehandlungen zu erheblichen gesellschaftlichen Konsequenzen führen, wie beispielsweise zu einem Vertrauensverlust in staatliche Institutionen oder zu Protesten. Um diese zu verstärken und Angst und Unsicherheit in der Öffentlichkeit zu schüren, wird versucht, aus den Begleiterscheinungen eines Sabotageaktes – auch eines gescheiterten – propagandistisch Nutzen zu ziehen. So ist etwa eine entsprechende Begleitung mutmaßlich prorussischer Sabotagehandlungen durch unterschiedliche Stellen wie Staatsmedien oder Hacktivisten denkbar.

Das BfV und weitere Sicherheitsbehörden stehen zu möglichen Sabotagevorfällen im engen Austausch und richten Präventionsangebote an gefährdete Stellen. Auch der Präventionsbereich des Verfassungsschutzes steht als vertraulicher Ansprechpartner für betroffene Bereiche jederzeit zur Verfügung.[11] Darüber hinaus haben Bürgerinnen und Bürger die Möglichkeit, über das BfV-Hinweistelefon verdächtige Sabotagehandlungen zu melden.[12] Solche Hinweise werden vertraulich behandelt.

11 Der Bereich Prävention (Wirtschafts- und Wissenschaftsschutz) ist erreichbar unter wirtschaftsschutz@bfv.bund.de.

12 Hinweise auf Sabotage können dem BfV auch über hinweise@bfv.bund.de gegeben werden.

Kapitel 5

Desinformation

Einhergehend mit seinem Angriffskrieg hat Russland die Verbreitung (pro-)russischer und antiwestlicher Narrative offensiv ausgebaut und spricht selbst davon, in einem „Informationskrieg“ zu stehen. In diesem Zuge werden Desinformation und Propaganda bewusst eingesetzt, um Einfluss auf den öffentlichen Diskurs wie die politische Willensbildung in Deutschland und Europa zu nehmen und Öffentlichkeit wie Politik vorsätzlich zu täuschen oder zu beeinflussen.

Ziel dieser Aktivitäten ist es, Unsicherheiten und Spaltungslinien in der deutschen Gesellschaft zu erzeugen beziehungsweise zu vertiefen, die Bereitschaft für die Unterstützung der völkerrechtswidrig von Russland angegriffenen Ukraine zu mindern und in diesem Sinne Einfluss auf politische Entscheidungen zu nehmen. Immer wieder bespielte Themen sind die (atomare) Eskalationsdominanz Russlands, Falschbehauptungen zur Ukraine, vermeintliche „Russophobie“ in Deutschland, Fragen von Energie, Inflation und Wirtschaft sowie diffamierende Attacken auf Personen im politischen Raum, darunter in Bundesregierung und Bundestag.

Dabei reagieren russische Stellen schnell und flexibel auf aktuelle Ereignisse in Deutschland mit jeweils angepasster Desinformation, die sie oft gezielt über soziale Medien verbreiten. So konnte das BfV feststellen, wie die seit 2022 aktive russische Desinformationskampagne „Doppelgänger“ zur Verbreitung von Desinformation gefälschte Websites beispielsweise von Spiegel, Stern oder FAZ wie auch nachgebaute Behördenseiten nutzt. Dabei greift „Doppelgänger“, zuletzt auch im Vorfeld der Bundestagswahl

im Februar 2025 und zuvor bei der Europawahl 2024, immer wieder Themen auf, die bereits emotional aufgeladen sind beziehungsweise besonders kontrovers diskutiert werden, wie etwa die Themenfelder Migration oder Klimaschutz.

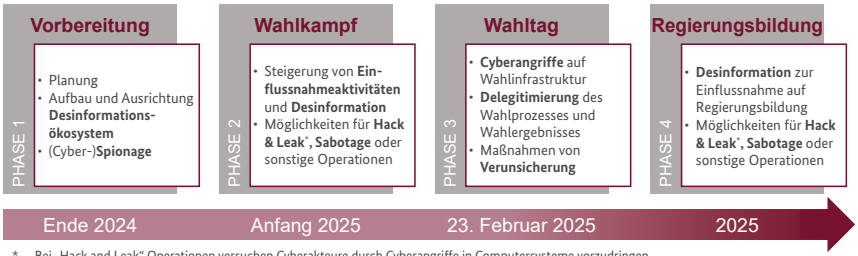
Im Umfeld der Bundestagswahl 2025 konnte das BfV anhaltende und auf die Wahl gerichtete Einflussnahmeversuche detektieren. Mit näher rückendem Wahltermin war dabei eine Zunahme der Desinformationsaktivitäten festzustellen. So wurde ein weiterer mutmaßlich russischer Desinformationsakteur gegen Deutschland aktiv, die Kampagne „Storm-1516". Diese verbreitet Artikel und Videos mithilfe eines Netzwerks von Websites, die den Anschein von Nachrichtenseiten erwecken, und durch die Einbeziehung insbesondere von (pro-)russischen Influencern. Inhalte werden dabei entweder mit KI-Unterstützung generiert oder durch Schauspieler gespielt und aufgezeichnet.

Die Wirkung solcher Kampagnen in den sozialen Medien – die Herbeiführung einer Verhaltensänderung beziehungsweise ein Bestärken vorhandener erwünschter Ansichten bei Angehörigen adressierter Zielgruppen – ist zwar nicht eindeutig zu bewerten. Allerdings macht sich Russland auch hier einen Wirkmechanismus einer freiheitlichen Demokratie zu Nutze: Denn das „desinformierende Narrative nur nennenswerte Reichweite erlangen, wenn sie von der massenmedialen Berichterstattung aufgegriffen werden", hat die Politik- und Medienwissenschaft bereits vor einiger Zeit herausgearbeitet.[13]

Russlands Einflussnahmevorgehen bei Wahlen in europäischen Demokratien kann strukturiert in einem Vierphasenmodell dargestellt werden. Die erste Phase dient dabei der Vorbereitung der beabsichtigten Einflussnahme durch strategische Planung sowie den Aufbau und die Ausrichtung geplanter Maßnahmen. Hier werden auch Strukturen und Netzwerke geschaffen, die in den späteren Phasen die Verbreitung von Desinformation fördern. In den weiteren Phasen erfolgen dann verschiedene Formen der Einflussnahme zu unterschiedlichen

13 Vgl. Jeannette Hoffmann: „Desinformation als Symptom: ein Überblick", in: BfV (Hrsg.): „Tagungsband Wissenschaftskonferenz 2023. Meinungsbildung 2.0 – Strategien im Ringen um Deutungshoheit im digitalen Zeitalter", S. 20–31, hier S. 28, in: www.verfassungsschutz.de.

Zeitfenstern – etwa im Wahlkampf, in zeitlicher Nähe zum Wahltag und schließlich im Nachgang zur Wahl bei einer Regierungsbildung.



Vierphasenmodell der illegitimen Einflussnahme auf die Bundestagswahl

Die identifizierten Narrative zur Bundestagswahl 2025 richteten sich vornehmlich gegen einzelne Parteien beziehungsweise Personen. Dabei wurden die für Russland eher vorteilhaften politischen Positionen, Personen und Parteien durch positive Darstellungen im Informationsraum unterstützt. Nachteilige Positionen, Personen sowie Parteien wurden diskreditiert. Auch wurden Narrative verwendet, die eine besondere Polarisierung versprachen. So wurde beispielsweise das Narrativ verbreitet, dass der Bundesregierung die Unterstützung der Ukraine vermeintlich wichtiger sei als die Belange und Sorgen der Bevölkerung in Deutschland. Zusätzlich verbreiteten russische Einflussakteure zum Wahltag hin Desinformationen, die auf die Sicherheit und Integrität der Bundestagswahl an sich abzielten. Auch nach der Bundestagswahl – vor allem im Zeitraum bis zur Regierungsbildung, aber auch darüber hinaus – ist mit Einflussnahmeversuchen durch Desinformation, Cyberangriffe sowie Spionage und Sabotage zu rechnen.

Generell versucht Russland auf verschiedenen Wegen im digitalisierten Informationsraum, Einfluss auf die freie Meinungs- und Willensbildung zu nehmen. Dazu zählen die russischen Staatsmedien wie beispielsweise RT sowie gekaufte prorussische Influencer. Ein weiteres Beispiel bildet das 2024 aufgedeckte

Einflussnahmenetzwerk in europäischer Politik und europäischen Medien „Voice of Europe“, das unter anderem auch Europaabgeordnete instrumentalisierte sowie Botnetze und unauthentische Accounts auf sozialen Medien nutzte.

Im Herbst 2024 wurde bei den Wahlen in Moldau und später in Rumänien derart intensiv mit Cyberangriffen auf Wahlinfrastruktur und rumänische Behörden, Geld, Influencern und Desinformation Einfluss genommen, dass in Rumänien das Verfassungsgericht die erste Runde der Präsidentschaftswahl annullierte. Zuvor kamen gegen die Wahl in Moldau neben Geldzahlungen und Propaganda auch Bombendrohungen zum Einsatz. Auch Meldungen aus Polen im Januar 2025 illustrieren das heute offensivere Vorgehen Russlands gegen Wahlen in europäischen Demokratien: Zu der im Mai 2025 anstehenden Präsidentschaftswahl wurden bereits Rekrutierungs- und Desinformationskampagnen Russlands aufgedeckt, mit denen die Wahl im Sinne des Kremls beeinflusst werden sollte.

Kapitel 6

Bewertung

Die allgemeine Gefährdungslage hat sich durch die Aggression Russlands gegen die Ukraine wie auch durch das offensive Vorgehen gegen Demokratien in Europa deutlich verschärft. Intensität und Ausmaß der zu antizipierenden Aktivitäten sind wahrscheinlich eng mit dem Kriegsverlauf in der Ukraine verknüpft. Auch insofern ist die innere Sicherheit Deutschlands stark von äußeren Konflikten abhängig. Doch auch nach einem Waffenstillstand oder einer Beendigung des Krieges in der Ukraine wird Russland seine verschleierten oder offen ausgetragenen konfrontativen Aktivitäten gegen Deutschland wie gegen EU und NATO nahezu sicher fortführen, um seine Ziele durchzusetzen.

Auch wenn nicht jeder vermutete Sabotagevorfall eine Maßnahme russischer Nachrichtendienste ist, profitiert Russland von der dadurch entstehenden Unsicherheit. Die heute zu verzeichnende Vermischung von Aktivitäten staatlicher

und nicht staatlicher Akteure erschwert zudem eine Zuordnung und ermöglicht es Russland, Verantwortung abzustreiten.

Wichtig sind daher Klarheit und Sicherheit. Dafür arbeiten das BfV und die Verfassungsschutzbehörden der Länder gewissenhaft im Rahmen ihrer rechtlichen Befugnisse und Zuständigkeiten: bei der Abwehr aller nachrichtendienstlichen Aktivitäten gegen Deutschland bei Spionage und Cyberspionage, Sabotage wie Cybersabotage, Einflussnahme und Desinformation. Der Auftrag des Verfassungsschutzes als Abwehrdienst ist es, die hier skizzierten illegitimen und illegalen Aktivitäten in und gegen Deutschland zu identifizieren, aufzuklären und abzuwenden. Dafür versetzen sich die Verfassungsschutzbehörden in das nachrichtendienstliche Gegenüber und analysieren dessen Handlungsweisen, um die nächsten Schritte antizipieren und unterbinden zu können. Damit das gelingt, werden Schwachstellen in Politik, Wirtschaft und Gesellschaft identifiziert, die von fremden Nachrichtendiensten ausgenutzt werden könnten.

Das können beispielsweise Personen im politischen Raum sein, die sich für eine fremde Macht einspannen lassen und in deren Interesse handeln. Das können Innentäter sein: Personen mit besonderen Zugängen, die als Zuträger für sensible Informationen fungieren, oder die ihre Befugnisse für Störaktionen missbrauchen könnten. Das können eher am Rande der Gesellschaft Stehende sein, die sich als Helfer eines fremden Nachrichtendienstes für Sabotage, Desinformation oder Propaganda kaufen lassen. Die Motivation kann dabei von dem Wunsch nach finanziellen oder anderweitigen Zuwendungen bis hin zu persönlichen politischen Überzeugungen reichen.

Russland wird weiter auf politische und gesellschaftliche Konfliktlinien in Deutschland zielen, um diese als Ansatzpunkte für manipulative Einflussnahme zu nutzen. So soll der politische Diskurs erschwert und das gesellschaftliche Miteinander geschwächt werden. Das langfristige Ziel Russlands ist es, auf diese Weise freiheitliche Demokratien zu schwächen und zu diskreditieren.

Um demgegenüber Resilienz aufzubauen, informiert das BfV Regierung und Parlament über seine Beobachtungen und trägt mit öffentlichen Stellungnahmen und gezielten Prä-

ventionsangeboten zur Awareness bei. Das BfV berät Politik, Verwaltung, Wirtschaft und Wissenschaft mit seinem Wissen über das Vorgehen fremder Nachrichtendienste und trägt durch das Teilen seiner Expertise dazu bei, dass sich Betroffene auch selber besser schützen können.

Die geopolitischen Umbrüche in Europa, Amerika und Asien bleiben Treiber für das nachrichtendienstliche Handeln gegen Deutschland. Das BfV als der für Cyber- und Spionageabwehr zuständige Nachrichtendienst des Bundes stellt sich für die Zukunft auf weitere Gefährdungen durch russische Spionage, Sabotage und Desinformation ein.

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Öffentlichkeitsarbeit
Merianstraße 100
50765 Köln
oeffentlichkeitsarbeit@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0)228 99 792-0
Fax: +49 (0)228 99 10 792-2915

Layout & Produktion
Bundesamt für Verfassungsschutz
Mediengestaltung und Druck
im ServiceCenter I

Stand
Mai 2025 (B-0044)

Bildnachweis

Seite 6: KI generiert | Seite 10: Grafik - BfV | Seite 14: Grafik - BfV | Seite 18: Grafik - BfV | Seite 20: Foto - BfV

Bundesamt für Verfassungsschutz
75 Jahre
IM AUFTRAG DER DEMOKRATIE

www.verfassungsschutz.de