Deutscher Bundestag **Drucksache 21/769**

21. Wahlperiode 07.07.2025

Kleine Anfrage

der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Agnieszka Brugger, Marcel Emmerich, Rebecca Lenhard, Jeanne Dillschneider, Lukas Benner, Schahina Gambir, Lamya Kaddor, Marlene Schönberger, Dr. Anna Lührmann, Dr. Lena Gumnior, Helge Limburg, Dr. Till Steffen, Deborah Düring, Sara Nanni, Robin Wagener und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Fragen zur Notwendigkeit eines umfassenden Lagebilds zu Sabotage, Spionage und Desinformation

Die Bundesrepublik Deutschland, ihre demokratischen Institutionen, aber auch ihre Lebensadern, die kritischen Infrastrukturen (KRITIS), sind seit Jahren sehr ernsten Angriffen, auch und vor allem ausländischer Nachrichtendienste und ihr nahestehender Gruppierungen ausgesetzt. Der russische Angriffskrieg gegen die Ukraine wirkte dabei als Katalysator für die feindlichen nachrichtendienstlichen Tätigkeiten des russischen Regimes unter Wladimir Putin. Es ist ein deutlicher Anstieg sicherheitsrelevanter russischer Aktivitäten in Europa und besonders auch in Deutschland zu verzeichnen. Spionage, Sabotage und Desinformationskampagnen bilden dabei zentrale Elemente zahlreicher fast täglich stattfindender hybrider Angriffe, die sich gezielt gegen politische Institutionen, kritische Infrastrukturen und den öffentlichen Diskurs richten und dadurch zunehmend die gesellschaftliche Stabilität gefährden. Auf diese eklatant gestiegenen Angriffe und die Notwendigkeit, rechtsstaatlich entschlossen auf sie zu reagieren, machen auch Vertreter deutscher Sicherheitsbehörden und der Nachrichtendienste seit Langem vehement aufmerksam. Das Bundesamt für Verfassungsschutz (BfV) stellt in seinem kürzlich veröffentlichten Jahresbericht eine zunehmende Offenheit, Aggressivität und strategische Vielfalt russischer Operationen gegen die Grundpfeiler unserer freiheitlich-demokratischen Gesellschaft fest (www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefaehrdung-russische-spionage-sabotage-desinformation.html).

Diese Entwicklungen sind jedoch nicht isoliert zu betrachten, sondern stehen im Kontext einer umfassenderen Bedrohung durch das zunehmend aggressive Verhalten von Putins Russland und insbesondere seiner verdeckt operierenden Geheimdienste und ihnen nahestehender Gruppierungen. Deren Agieren wird immer aggressiver. Sie schrecken selbst vor schweren Straftaten nicht zurück. Davon zeugen verschiedene Verfahren, die der Generalbundesanwalt (GBA) derzeit führt. Auch bei der letzten öffentlichen Anhörung der Nachrichtendienste durch das Parlamentarische Kontrollgremium (PKGr) am 14. Oktober 2024 warnten deren Spitzen ausdrücklich vor Russlands imperialistischer Expansionspolitik (www.bundestag.de/dokumente/textarchiv/2024/kw42-pa-pkgr-1020558). Insbesondere der Bundesnachrichtendienst und sein (noch) amtierender Präsident Bruno Kahl warnten zuletzt öffentlich davor, dass Russland sogar die Reaktionsmechanismen des NATO-Bündnisses – namentlich den Artikel 5 des

NATO-Vertrages – auf die Probe stellen wird (www.tagesspiegel.de/internationales/haben-nachrichtendienstliche-belege-bnd-chef-kahl-warnt-vor-russischem-angriff-auf-nato-staaten-13834069.html).

Dabei ist ein Schlüsselelement im Baukasten der hybriden russischen Angriffe gegen den Westen – aber auch sonstiger, insbesondere chinesischer Akteure – die Spionage. Ziel dieser Aktivitäten ist es, Informationen aus sensiblen Bereichen wie Politik, Militär, Wirtschaft, Forschung und kritischer Infrastruktur zu gewinnen. Neben der klassischen Spionage – durch Nutzung menschlicher Quellen – kommt dabei auch Cyberangriffen eine herausragende Bedeutung zu. Letztere verursachen nach Erhebungen des Branchenverbandes BITKOM – die nach Auffassung des BfV-Vizepräsidenten Sinan Selen noch immer nicht einmal die Realität widerspiegeln – wirtschaftliche Schäden in dreistelliger Milliardenhöhe (www.rnd.de/wirtschaft/bitkom-wirtschaftsschutzbericht-ueber-cyberangriffe-und-spionage-schaeden-bei-unternehmen-auf-WLMC7BDRXRBLTDP54CQJSJVTW4.html), haben aber auch immer wieder das Ziel, sicherheitsrelevante Information zu extrahieren, und gefährden damit aktiv und mit wachsender Bedrohlichkeit auch die nationale Sicherheit. Auch durch journalistische („Vulcan-Files“) Recherchen wissen die Fragesteller, dass alle EU-Mitgliedstaaten im Fokus der Angreifer stehen, Deutschland als Land im Herzen Europas und einer der wichtigsten Unterstützer der Ukraine jedoch ganz besonders. Ebenso besorgniserregend sind regelmäßig auftretende Drohnenüberflüge über Kasernen, militärische Einrichtungen, Marineanlagen sowie über Anlagen der kritischen Infrastruktur (www.tagesschau.de/investigativ/ndr-wdr/zunahme-drohnensichtungen-100.html oder zur KRITIS www.ndr.de/fernsehen/sendungen/panorama3/meldungen/Drohnen-ueber-Norddeutschland-Kritische-Infrastruktur-im-Visier,drohnen442.html). Bislang nicht ausreichend erfasst scheint nach Ansicht der Fragesteller zudem das Ausmaß rechtswidriger Zutritte und Einbrüche in KRITIS-Anlagen und sensible Rüstungsunternehmen. Betreiber berichten, auch gegenüber den Fragestellern, von einem besorgniserregenden und nicht allein durch Private abwehrbaren Ausmaß, in dem sie aufgebrochene Türen und Fenster, Löcher in Zäunen, maskierte Personen im Umfeld der Anlagen und Ähnliches registrieren. Diese Vorfälle deuten darauf hin, dass systematisch nach Schwachstellen in der deutschen Verteidigungs- und Sicherheitsarchitektur gesucht wird, um diese zu identifizieren und für eigene Zwecke nutzbar zu machen.

Zudem ist eine ähnliche Entwicklung auch im Hinblick auf Sabotageaktivitäten zu beobachten. Diese zeichnet sich sowohl im Hinblick auf die Vielfalt der eingesetzten geheimdienstlichen Methoden als auch der Bandbreite potenzieller Zielobjekte aus. So sind gezielte Tötungen im öffentlichen Raum – wie etwa der Tiergarten-Mord – sowie strategisch vorbereitete Anschlagspläne gegen Führungspersonal der deutschen Rüstungsindustrie dokumentiert. Besonders alarmierend ist der verstärkte Einsatz niedrigschwellig rekrutierter Handlanger – sogenannter Low-Level-Agenten (oder auch Wegwerfagenten) –, die gezielt zur Ausführung von Störaktionen für kleines Geld angeheuert und eingesetzt werden. Darüber hinaus sind auch Sabotageakte, etwa mittels Brandsätze, gegen Energie-, Verkehrs- und Militäreinrichtungen mit mutmaßlich nachweislich russischer Handschrift zu verzeichnen (www.tagesspiegel.de/politik/dhl-paketbrand-in-leipzig-sabotage-akt-vom-juli-hatte-offenbar-fast-zu-flugzeugabsturz-gefuhrt-12528386.html; www.morgenpost.de/vermischtes/article242247132/Grossbrand-in-Berlin-Firma-stellt-Waffen-fuer-Ukraine-her.html).

Eng verknüpft mit diesen physischen Angriffen auf gesellschaftliche Stabilität ist eine weitere digitale Dimension hybrider Kriegsführung: die gezielte Verbreitung von Desinformation. Während Sabotageakte unmittelbar sichtbare Schäden anrichten, entfalten Desinformationskampagnen ihre Wirkung oft schleichend – und sind dabei nicht minder gefährlich für den gesellschaftlichen

Zusammenhalt und die demokratische Ordnung. Russland und seine Proxies verbreiten dazu bewusst und zielgerichtet falsche oder irreführende Informationen bzw. verschweigen und verschleiern wesentliche Teile einer Information. Sie nutzen für die Verbreitung von Desinformation den gesamten Informationsraum, also alle digitalen und analogen Kanäle, Medien und Formate. Damit will man gezielt und vorsätzlich Menschen und die Öffentlichkeit täuschen, beeinflussen und verunsichern, die öffentliche Meinungsbildung manipulieren, kontroverse Debatten zusätzlich emotionalisieren, gesellschaftliche Spannungen verstärken und Misstrauen in staatliche Institutionen und Regierungshandeln schüren. Die Kampagnen greifen dabei häufig emotional aufgeladene oder polarisierende Themen auf und verbreiten gezielt Falschinformationen – etwa über prominente politische Akteure, wie im Fall der Falschbehauptung über einen angeblichen Kokainkonsum von Emmanuel Macron (www.spiegel.de/ausland/emmanuel-macron-versteckt-taschentuch-russland-spinnt-daraus-koks-vorwurf-a-0162d96e-c9f4-47ce-871b-a73e235d2032). Besonders besorgniserregend ist, dass solche Narrative nicht nur über russische Kanäle verbreitet werden, sondern zunehmend auch von inländischen Akteuren oder sogenannten Trollbots aufgegriffen und weiterverbreitet werden, wodurch eine gefährliche Wechselwirkung zwischen ausländischer Einflussnahme und innergesellschaftlicher Radikalisierung entsteht, die den öffentlichen Diskurs massiv beeinflusst und das demokratische Gemeinwesen nachhaltig destabilisiert.

Zugleich sticht neben den russischen feindlichen Attacken gegen die Bundesrepublik Deutschland wie in anderen westlichen und demokratischen Gesellschaften die Volksrepublik China aufgrund ihrer Operationen im Bereich der Spionage und Einflussnahme in Deutschland hervor. Diese stellen sowohl quantitativ und qualitativ sowohl mit ihrem, wie es das Bundesamt für Verfassungsschutz (BfV) betont, „All-Tools-and-All-Sectors-Approach“ (www.verfassungsschutz.de/SharedDocs/hintergruende/DE/wirtschafts-wissenschaftsschutz/chinas-neue-wege-der-spionage.html) als auch mit Blick auf die langfristige Strategie, die Quantität und Qualität der Attacken ebenfalls eine besondere Gefahr dar, die auch nach Ansicht der Fragesteller deutlich mehr an Aufmerksamkeit und ein erhöhtes Maß an Schutzmaßnahmen, unter anderem auch im Wissenschaftsbereich, dringend erforderlich macht.

All diese Entwicklungen verdeutlichen das Ausmaß, in dem Deutschland im Zentrum hybrider Angriffe, insbesondere aus Russland, aber auch aus mehreren anderen autoritären Staaten, steht. Eine echte Zeitenwende auch in der inneren Sicherheit und die schnellstmögliche Erhöhung gesellschaftlicher Resilienz gegenüber der stark gestiegenen Bedrohung bleiben das Gebot der Stunde. Die Erweiterung des Sicherheitsbegriffs im Rahmen der Änderungen der Finanzverfassung waren auch nach Meinung der Fragesteller ein entscheidender Schritt. Weitere müssen dringend folgen. Die neuen finanziellen Möglichkeiten müssen schnell und effektiv genutzt werden. Denn: Es braucht dringend eine moderne, vorausschauende und auf Resilienz ausgerichtete Innen-, Sicherheits- und Verteidigungspolitik. Der Umgang und das Zusammenführen wichtiger Informationen innerhalb der Bundesregierung ist dafür ein herausragend wichtiger Baustein; eine zentrale, ressort- und Bund-Länder-übergreifende Koordinierung und Bündelung sicherheitsrelevanter Erkenntnisse ist nach Einschätzung der Fragesteller bislang jedoch nicht erkennbar. Um hybride Angriffe und Desinformation effektiv erkennen und abwehren zu können, ist dies aber zwingend erforderlich, insbesondere um das Ausmaß der Angriffe überhaupt absehen zu können, um Muster zu erkennen und mögliche politische und gesetzgeberische Handlungsnotwendigkeiten identifizieren zu können. Eine resiliente Gesellschaft ist zudem zwingend auf gut informierte und wachsame Bürgerinnen und Bürger angewiesen. Dies kann nur durch eine gänzlich andere Ansprache durch die Spitzen der Bundesregierung erreicht werden. Auch dafür könnte ein Gesamtlagebild „Nationale Sicherheit“ ein wichtiger Baustein sein.

Wir fragen die Bundesregierung:

1. Wie viele Fälle des unerlaubten Betretens, Ausspähens oder physischen Manipulierens, Beschädigens und Einbrechens von und in Kasernen, militärische Einrichtungen und Marineanlagen auf deutschem Bundesgebiet sind der Bundesregierung seit dem Jahr 2022 bekannt geworden (bitte nach Jahren aufschlüsseln)?
2. Wie viele Fälle des unerlaubten Betretens, Ausspähens oder physischen Manipulierens, Beschädigens und Einbrechens von und in KRITIS-Anlagen sind der Bundesregierung seit dem Jahr 2022 bekannt geworden (bitte nach Jahren aufschlüsseln)?
3. Wie viele Fälle von Drohnen(über-)flügen über Kasernen, militärischen Einrichtungen und Marineanlagen auf deutschem Bundesgebiet sind der Bundesregierung seit dem Jahr 2022 bekannt und dokumentiert worden (bitte nach Einrichtungen und Jahren aufschlüsseln)?
4. Wie viele Fälle von Drohnen(über-)flügen über KRITIS-Einrichtung und Anlagen sind der Bundesregierung seit dem Jahr 2022 bekannt und dokumentiert worden (bitte nach Einrichtungen und Jahren aufschlüsseln)?
5. Bitte jeweils differenziert mit Bezug auf die Fragen 1 bis 4:
   a) In wie vielen Fällen wurden strafrechtliche Ermittlungen eingeleitet?
   b) In wie vielen Fällen konnten tatverdächtige Personen ermittelt werden?
   c) In wie vielen Fällen kam es zur Anklage?
   d) In wie vielen Fällen konnten Bezüge zu ausländischen Nachrichtendiensten und bzw. oder Auftraggebern bzw. Hintermännern festgestellt werden (bitte nach Ländern aufschlüsseln)?
   e) Bestehen aus Sicht der Bundesregierung rechtliche oder faktische Defizite, die die Aufklärung von in den Fragen 1 bis 4 erfragten Fällen besonders erschweren, und wenn ja, welche?
6. Bei welchen landes- und bundesbehördlichen Stellen liegen nach Kenntnis der Bundesregierung Informationen über die in den Fragen 1 bis 4 erfragten Fälle vor, und bei welchen Stellen oder Zentren laufen diese zusammen?
7. Gibt es eine einheitliche Stelle bei der Bundesregierung, bei der sämtliche Informationen über die in den Fragen 1 bis 4 erfragten Fälle zusammengetragen und im Sinne eines Lagebildes gebündelt werden, und wer hat darauf Zugriff oder wird wie darüber informiert?
   a) Wenn nein, wie bewertet die Bundesregierung das Fehlen eines entsprechenden Lagebildes?
   b) Plant die Bundesregierung künftig die Erstellung und Einrichtung eines entsprechenden Lagebildes?
   c) Wenn ja, bei welcher Stelle soll ein solches Lagebild vorliegen, und in welchem zeitlichen Intervall (täglich bzw. wöchentlich bzw. monatlich) sollen dort relevante Informationen für wen zusammengetragen werden?

8. Liegen der Bundesregierung Informationen darüber vor, in wie viel Prozent der in den Fragen 2 und 4 erfragten Fälle Betreiber von KRITIS überhaupt die Behörden informieren?

   a) Falls dies nicht immer der Fall ist, welche Maßnahmen plant die Bundesregierung, um ein zuverlässiges und verbindliches Meldesystem von KRITIS-Betreibern zu den Sicherheitsbehörden zu gewährleisten?

   b) An welche Stellen können sich Betreiber von KRITIS wenden, wenn sie die in den Fragen 2 und 4 erfragten Fälle beobachten?

   c) Falls es sich dabei um mehrere Stellen handelt, in welchem Maß und welchem zeitlichen Intervall und in welchem Format tauschen die beteiligten Behörden Informationen, die sie von Betreibern von KRITIS erhalten haben, aus?

   d) Plant die Bundesregierung die Einrichtung einer einheitlichen Meldestelle für Betreiber von KRITIS zur Meldung von in den Fragen 2 und 4 erfragten Fällen, und wenn ja, in welcher Bundesbehörde oder Stelle soll diese künftig angesiedelt werden?

9. Wie viele Fälle von Cyberangriffen, die nicht ausschließlich wirtschaftlich motiviert, sondern potenziell sicherheitsgefährdend sind, sind der Bundesregierung seit dem Jahr 2022 bekannt (bitte nach Jahren und Sektoren aufschlüsseln)?

10. Wie viele der in Frage 9 erfragten Fälle waren dergestalt erfolgreich, dass eine Beeinträchtigung deutscher oder europäischer Sicherheitsinteressen jedenfalls nicht ausgeschlossen werden kann (bitte nach Jahren aufschlüsseln)?

11. Wie viele der in Frage 9 erfragten Fälle können eindeutig oder wahrscheinlich staatlich oder staatlich gelenkten Akteuren zugeordnet werden (bitte nach Jahren aufschlüsseln und nach konkreten Staaten und eindeutiger bzw. wahrscheinlicher Attribution differenzieren)?

12. Welche Erkenntnisse liegen der Bundesregierung dazu vor, wie hoch die Dunkelziffer der in Frage 9 erfragten Fälle ist, also wie viele Fälle gar nicht bekannt werden?

13. In wie vielen der in Frage 9 erfragten Fälle wurde ein Ermittlungsverfahren eingeleitet?

   a) In vielen dieser Fälle konnten tatverdächtige Personen ermittelt werden?

   b) In wie vielen dieser Fälle kam es zu einer Verurteilung?

   c) In wie vielen der in den Fragen 13, 13a und 13b erfragten Fälle (bitte differenzieren) konnten Bezüge zu ausländischen Nachrichtendiensten und bzw. oder Auftraggebern bzw. Hintermännern festgestellt werden (bitte nach Ländern aufschlüsseln)?

14. Gibt es eine einheitliche Stelle bei der Bundesregierung, bei der sämtliche Informationen über die in den Fragen 9 bis 13 erfragten Fälle zusammengetragen und im Sinne eines Lagebildes gebündelt werden?

   a) Wenn nein, wie bewertet die Bundesregierung das Fehlen eines entsprechenden Lagebildes, und inwieweit würde ein solches Lagebild nach Auffassung der Bundesregierung dazu beitragen, die in den Fragen 9 bis 13 erfragten Fälle besser aufzuklären und zukünftig verhindern zu können?

   b) Plant die Bundesregierung die Einrichtung eines entsprechenden Lagebildes?

c) Wenn ja, bei welcher Stelle soll ein solches Lagebild vorliegen, und in welchem zeitlichen Intervall (täglich bzw. wöchentlich bzw. monatlich) sollen dort relevante Informationen zusammengetragen werden?

d) Bei welchen Stellen bei der Bundesregierung oder den Landesregierungen liegen Informationen oder gar partielle Lagebilder über die in den Fragen 9 bis 13 erfragten Fälle vor?

15. Welche Vorkehrungen trifft die Bundesregierung im Rahmen der Umsetzung der NIS-2-Richtlinie (zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit), um sicherzustellen, dass sämtliche, bei Betreibern von KRITIS vorliegenden, relevanten Informationen über die in den Fragen 9 bis 13 erfragten Fälle beim Bundesamt für Sicherheit in der Informationstechnik (BSI), aber auch allen anderen betroffenen Behörden vorliegen und Teil eines einheitlichen Lagebildes werden?

16. Wie viele Fälle von Desinformation und Einflussnahme auf demokratische Willensbildungsbildungsprozesse in Deutschland seit dem Jahr 2022 sind der Bundesregierung bekannt, die von eindeutig oder wahrscheinlich staatlichen oder staatlich gelenkten Akteuren ausgegangen sind (bitte nach Jahren aufschlüsseln und nach konkreten Staaten und eindeutiger bzw. wahrscheinlicher Attribution differenzieren)?

a) Wie viele dieser Fälle sind nach Kenntnisstand und Auffassung der Bundesregierung nach deutschem Recht strafbar?

b) In wie vielen dieser strafbaren Fälle wurde ein Ermittlungsverfahren eingeleitet und konnten Tatverdächtige ermittelt werden?

c) In wie vielen dieser Fälle kam es zu einer Verurteilung?

d) In wie vielen Fällen konnten Bezüge zu ausländischen Nachrichtendiensten und bzw. oder Auftraggebern bzw. Hintermännern festgestellt werden (bitte nach Ländern aufschlüsseln)

e) Wie viele Fälle standen im Zusammenhang mit den Bundestagswahlen 2025?

17. Gibt es eine einheitliche Stelle bei der Bundesregierung, bei der sämtliche Informationen über die in Frage 16 erfragten Fälle im Sinne eines Lagebildes gebündelt vorliegen?

a) Wenn nein, wie bewertet die Bundesregierung das Fehlen eines entsprechenden Lagebildes, und inwieweit würde ein solches Lagebild nach Auffassung der Bundesregierung dazu beitragen, die in Frage 16 erfragten Fälle besser aufzuklären und gezielte Gegenmaßnahmen einleiten zu können?

b) Plant die Bundesregierung die Einrichtung eines entsprechenden Lagebildes?

c) Wenn ja, bei welcher Stelle soll ein solches Lagebild vorliegen, welche – auch nichtstaatlichen – Stellen sollen zur Informationsübermittlung verpflichtet oder ermutigt werden, und in welchem zeitlichen Intervall (täglich bzw. wöchentlich bzw. monatlich) sollen dort relevante Informationen zusammengetragen werden?

d) Welche Maßnahmen hat die Bundesregierung ergriffen, um den Schaden durch Desinformation einzugrenzen, und was gedenkt sie darüber hinaus an Maßnahmen zu ergreifen, und inwiefern prüft sie dabei den Einsatz auch digitaler Technologien (ggf. welcher konkret)?

e) In welchem formellen und informellen Rahmen tauscht sich die Bundesregierung mit anderen betroffenen Staaten, insbesondere im europäischen, transatlantischen und indopazifischen Raum, dazu aus?

18. Welche Maßnahmen trifft die Bundesregierung, um die Bevölkerung über das Ausmaß und die Gefahren ausländischer, insbesondere russischer und chinesischer, nachrichtendienstlicher Tätigkeiten auf dem Gebiet des Bundesrepublik Deutschland zu unterrichten und ihre Kompetenzen zum Umgang damit zu stärken?

a) Plant die Bundesregierung, etwa im Zuge der Einrichtung eines nationalen Sicherheitsrats, eine grundlegende Neuordnung des Informationsflusses zwischen den Landes- und Bundesbehörden mit Blick auf Sabotage, Spionage und Desinformation?

b) Wenn ja, welche?

c) Wenn ja, ist der Bundesregierung bekannt, welche Auffassung die Innenministerkonferenz (IMK) zu dieser Frage vertritt, und welche Rolle sollte die IMK nach Auffassung der Bundesregierung dabei spielen?

19. Sieht die Bundesregierung den Bedarf, eigene Bemühungen im weiten Feld der „Strategischen Kommunikation“ auszubauen und zu verbessern, und wenn ja, wo genau, und mit welchem Ziel und welchen Maßnahmen (bitte konkret aufschlüsseln)?

Berlin, den 25. Juni 2025

Katharina Dröge, Britta Haßelmann und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333