Deutscher Bundestag **Drucksache 20/14166**

20. Wahlperiode 11.12.2024

Kleine Anfrage

der Abgeordneten Konstantin Kuhle, Renata Alt, Christine Aschenberg-Dugnus, Christian Bartelt, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Sandra Bubendorfer-Licht, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Maximilian Funke-Kaiser, Martin Gassner-Herz, Anikó Glogowski-Merten, Nils Gründer, Julian Grünke, Thomas Hacker, Philipp Hartewig, Ulrike Harzer, Peter Heidt, Katrin Helling-Plahr, Katja Hessel, Manuel Höferlin, Reinhard Houben, Olaf in der Beek, Gyde Jensen, Dr. Ann-Veruschka Jurisch, Dr. Lukas Köhler, Dr. Thorsten Lieb, Michael Georg Link (Heilbronn), Kristine Lütke, Ria Schröder, Anja Schulz, Dr. Stephan Seiter, Judith Skudelny, Bettina Stark-Watzinger, Benjamin Strasser, Jens Teutrine, Stephan Thomae, Sandra Weeser, Katharina Willkomm und der Fraktion der FDP

Hybride Angriffe und Desinformation im Vorfeld der Bundestagswahl

In Zeiten zunehmender internationaler Spannungen sind hybride Angriffe und Desinformation für autoritäre Staaten ein Mittel, um Druck auf demokratische Staaten auszuüben und gezielt auf die öffentlichen Debatten in liberalen Demokratien Einfluss zu nehmen. Die verwendeten Mittel reichen hierbei von Desinformation auf Social Media (vgl. www.bertelsmann-stiftung.de/de/themen/aktuelle-meldungen/2024/februar/grosse-mehrheit-erkennt-in-desinformation-eine-gefahr-fuer-demokratie-und-zusammenhalt, letzter Abruf: 25. November 2024) über Sabotage an kritischer Infrastruktur (vgl. www.zdf.de/nachrichten/politik/ausland/ostsee-finnland-schweden-litauen-unterseekabel-100.html, letzter Abruf 25. November 2024) bis zu Spionage (vgl. www.tagesschau.de/investigativ/ndr-wdr/drohnen-spionage-sabotage-100.html, letzter Abruf: 25. November 2024). Ausländische Staaten nehmen auch ganz direkt Einfluss auf die politische Willensbildung, indem sie beispielsweise deutsche Politiker oder deren Mitarbeiter anwerben (vgl. www.tagesschau.de/investigativ/wdr/spionage-china-deutschland-100.html, letzter Abruf 25. November 2024) oder anderweitig in die politische Willensbildung in Deutschland eingreifen. Auch ausländisch beeinflusste Institutionen dienen dabei immer häufiger als Eintrittstor für fremde Mächte (vgl. www.deutschlandfunk.de/ditib-ankaras-einfluss-auf-deutschen-moscheeverband-100.html, letzter Abruf 25. November 2024). Zunehmend setzt sich das Konzept der „Foreign Information Manipulation and Interference“ (FIMI) durch und meint gezielte Aktivitäten ausländischer Akteure, die darauf abzielen, durch Manipulation und gezielte Desinformation das öffentliche Meinungsbild, demokratische Prozesse oder die gesellschaftliche Stabilität in anderen Staaten zu beeinflussen (vgl. www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en; letzter Abruf: 28. November 2024). Die Gefahr hybrider Einflussnahme besteht insbesondere mit Blick auf die vorgezogene Bundestagswahl am 23. Februar 2025 (vgl. www.tagesspiegel.de/politik/naturlich-hat-das-auswirkungen-bnd-chef-kahl-wa

rnt-vor-einflussversuchen-moskaus-auf-bundestagswahl-12782207.html; letzter Abruf: 28.11.2024).

Die Bundesrepublik Deutschland ist insbesondere für die hybriden Aktivitäten der Russischen Föderation ein wichtiges und gleichzeitig leichtes Ziel. Das Parlamentarische Kontrollgremium (PKGr) des Deutschen Bundestages hat in seiner Öffentlichen Bewertung vom 13. März 2024 festgestellt, dass Deutschland im Mittelpunkt russischer Einflussoperationen steht. Russland versuche aktiv und erfolgreich, auf verschiedenen Ebenen illegitim auf Politik, Wirtschaft und Gesellschaft einzuwirken. Dabei werde die Tragweite der Bedrohung weder von allen politisch Verantwortlichen noch in der Gesellschaft in Deutschland insgesamt erkannt. Der Instrumentenkasten hybrider Angriffe reicht von umfangreichen Desinformationskampagnen in Medien, sozialen Netzwerken und auf Plattformen, massiver Propaganda über Hack- and Leak-Operationen, Spionage und Cyberangriffe, gezielte Instrumentalisierung und Förderung von Migration, Wahlbeeinflussung und Beeinflussung der politischen Willensbildung bis hin zur – auch finanziellen – Unterstützung extremistischer Gruppierungen. Ziele der Angriffe seien Destabilisierung, Verunsicherung und gesellschaftliche Spaltung (vgl. Öffentliche Bewertung des Parlamentarischen Kontrollgremiums gemäß § 10 Absatz 2 Satz 1 des Kontrollgremiumgesetzes vom 13. März 2024 – Russische Einflussnahme in Deutschland, Bundestagsdrucksache 20/10655).

Anders als FIMI und Desinformationen, die ihre Wirkung oft erst schleichend entfalten und sich erst im Laufe der Zeit materialisieren, führen hybride Angriffe auch zu ganz konkreten und unmittelbaren Schäden in Deutschland. Deutsche Unternehmen und staatliche Einrichtungen sind konstant Ziel von Cyberattacken. Alleine der Schaden für die deutsche Wirtschaft betrug 2023 einen dreistelligen Milliardenbetrag (www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2024/2024-08-28-studie-bitkom.html#:~:text=Aktuell%20sind%20Cyberattacken%20f%C3%BCr,betrug%20der%20Schaden%20durch%20Cybercrime., letzter Abruf 25. November 2024). Daneben kommt es aber immer häufiger auch zu Sabotage, Spionage und ganz konkreten Angriffen auf kritische Infrastruktur, sei es bei Seekabeln oder im Logistikbereich. Die Dreistigkeit der Täter wächst, während es den deutschen Sicherheitsbehörden schwerfällt, die Täter dingfest zu machen. So waren es beispielsweise dänische Marineschiffe, die einen chinesischen Frachter festsetzten, der im großen Umfang Unterseekabel beschädigt hatte, während die deutsche Bundespolizei erst verspätet ausrückte (vgl. www.ndr.de/nachrichten/mecklenburg-vorpommern/Moegliche-Kabel-Sabotage-in-Ostsee-Bundespolizei-schickt-Schiff,kabelsabotage100.html, letzter Abruf 25. November 2024).

Wir fragen die Bundesregierung:

1. Wie erfasst die Bundesregierung hybride Angriffe auf Deutschland oder deutsche Infrastruktur, und welche Kriterien legt die Bundesregierung bei dieser Erfassung zugrunde?
2. Wie viele hybride Angriffe auf Deutschland oder deutsche Infrastruktur hat die Bundesregierung seit dem Jahr 2010 jeweils jährlich festgestellt, welche Entwicklungen sind bei diesen Zahlen aus Sicht der Bundesregierung zu beobachten, und wie erklärt sich die Bundesregierung einen eventuellen Anstieg hybrider Angriffe in den letzten Jahren?
3. Welche Akteure führen hybride Angriffe auf Deutschland oder deutsche Infrastruktur aus, wie stellt die Bundesregierung diese Akteure fest, welche Konzepte zur Identifizierung von Urhebern solcher Angriffe hat die Bundesregierung entwickelt, und wie wendet sie diese an?

4. Welcher Schaden entsteht nach Kenntnis der Bundesregierung durch hybride Angriffe jährlich in Deutschland (bitte jährlich seit 2010 aufschlüsseln), und wie erklärt sich die Bundesregierung die Kostenentwicklung dieser Angriffe?
5. Welche Schadensereignisse stechen aus Sicht der Bundesregierung durch ihre besonders hohen Kosten insoweit heraus?
6. Wie viele Cyberangriffe auf deutsche Unternehmen, staatliche Einrichtungen und Infrastruktur hat es seit 2021 jeweils jährlich gegeben, welche Schäden haben diese Angriffe jeweils jährlich verursacht, und welchen Anteil haben dabei die Angriffe staatlicher Akteure nach Kenntnis der Bundesregierung?
7. Wie plant die Bundesregierung, hybriden Angriffen mit Bezug zur Bundestagswahl zu begegnen?
8. Sieht die Bundesregierung Bedarf an einem Lagebild zur hybriden Gefährdungslage Deutschlands, und auf welche Art und Weise unterrichtet die Bundesregierung die Bevölkerung, Länder und Kommunen sowie Unternehmen über mögliche Gefährdungen und die richtige Verhaltensweise zum Schutz vor hybriden Angriffen?
9. Bei wie vielen und welchen untergesetzlichen Normen sieht die Bundesregierung Anpassungsbedarf im Rahmen der Nationalen Sicherheitsstrategie, und inwieweit wurden Punkte der Nationalen Sicherheitsstrategie in Bezug auf hybride Angriffe bereits umgesetzt?
10. Wie organisiert die Bundesregierung den Informationsaustausch der verschiedenen beteiligten Behörden bei der Erkennung und Abwehr hybrider Angriffe, welche Behörden stehen hierbei im Austausch, welche Austauschformate gibt es, wie oft findet der Austausch statt, und wie viele Fälle werden hierbei jeweils besprochen?
11. Welche Rolle spielen insoweit die gemeinsamen Zentren des Bundes und der Länder (Gemeinsames Terrorismusabwehrzentrum (GTAZ), Gemeinsames Terrorismus- und Extremismusabwehrzentrum (GETZ), Gemeinsames Internetzentrum (GIZ), Nationales Cyber-Abwehrzentrum (NCAZ) und andere)?
12. Welche Maßnahmen hat die Bundesregierung ergriffen, um den illegalen Überflügen mit Drohnen über deutsche Bundeswehrstandorte und die Militäreinrichtungen befreundeter ausländischer Staaten in Deutschland entgegenzuwirken, und welche Maßnahmen hat die Bundesregierung ergriffen, um die Urheber dieser Überflüge zu ermitteln?
13. Welche Maßnahmen hat die Bundesregierung ergriffen, um die Sicherheit von Transportwegen in Deutschland und von bzw. nach Deutschland zu gewährleisten, welche Gefahr geht aus Sicht der Bundesregierung insoweit von Angriffen auf Transportwege auf dem Land-, Luft- und Seeweg jeweils aus, und welche Arten von Angriffen sind hierbei wahrscheinlich, und wie können diese jeweils verhindert werden?
14. Inwiefern erfasst die Bundesregierung gezielte Desinformation ausländischer staatlicher Akteure in Deutschland oder im deutschsprachigen Internet, welche Kriterien legt die Bundesregierung dieser Erfassung zugrunde, und welche Kriterien legt die Bundesregierung zugrunde, um relevante Fälle von Desinformation zu identifizieren, auf die eine koordinierte Erwiderung erfolgen muss?

15. Wie viele Fälle gezielter Desinformation ausländischer staatlicher Akteure in Deutschland oder im deutschsprachigen Internet hat die Bundesregierung seit dem Jahr 2010 jeweils jährlich festgestellt, welche Entwicklungen sind bei diesen Zahlen aus Sicht der Bundesregierung zu beobachten, und wie erklärt sich die Bundesregierung einen eventuellen Anstieg von Desinformation in den letzten Jahren?

16. Welche ausländischen staatlichen oder staatsnahen Akteure verbreiten Desinformation in Deutschland oder im deutschsprachigen Internet, wie stellt die Bundesregierung diese Akteure fest, welche Konzepte zur Identifizierung von Urhebern solcher Verbreitung hat die Bundesregierung entwickelt, und wie wendet sie diese an?

17. Wie arbeitet die Bundesregierung mit Betreibern von Social-Media-Plattformen zusammen, um Desinformationskampagnen und hybride Angriffe frühzeitig zu erkennen und effektiv einzudämmen?

18. Welcher Schaden entsteht nach Kenntnis der Bundesregierung durch Desinformation jährlich (bitte jährlich seit 2010 aufschlüsseln), welche Kosten verursachen insbesondere Gegenmaßnahmen der Bundesregierung, und wie erklärt sich die Bundesregierung die Kostenentwicklung?

19. Welche Desinformationsereignisse stechen aus Sicht der Bundesregierung durch ihre besonders weitreichenden Folgen heraus, und wie plant die Bundesregierung, solchen Ereignissen zukünftig zu begegnen?

20. Wie viele Versuche, die Verbreitung des Programms der in Deutschland verbotenen Fernsehsender RT und Sputnik hat die Bundesregierung seit dem Verbot festgestellt, und wie geht die Bundesregierung gegen die Verbreitung dieser Inhalte vor?

21. Plant die Bundesregierung eine Öffnung für fremdsprachige Inhalte der Deutschen Welle auch in Deutschland, und welche Bedeutung misst die Bundesregierung einem solchen Schritt bei der Bekämpfung von FIMI in Deutschland bei?

22. Ist der von Russland hergestellte Impfstoff „Sputnik V“ seit 2020 in Deutschland verimpft worden, und wenn ja, wie viele Dosen dieses Impfstoffs wurden verabreicht, wird dieser Impfstoff weiterhin in Deutschland verwendet, und wenn ja, wo und in welchem Umfang?

23. Wie bewertet die Bundesregierung die Einflussnahme ausländischer Akteure und Regierungen auf deutsche Parteien, hat die Bundesregierung dahin gehend Erkenntnisse, dass eine finanzielle Einflussnahme auf deutsche Parteien oder Politiker im Vorfeld der bevorstehenden Bundestagswahl geplant ist oder bereits durchgeführt wird?

24. Wie erfasst die Bundesregierung Desinformation, wie bewertet sie diese inhaltlich, und nach welchen Kriterien entscheidet sie, auf welche Desinformation gezielt geantwortet werden muss, wie betreibt die Bundesregierung sogenanntes Debunking, also das Entkräften falscher Informationen, und welche nationalen Stellen des Bundes und der Länder bzw. Kommunen stehen insoweit im Austausch?

25. Welche technologischen Innovationen und KI-gestützten Lösungen setzt die Bundesregierung ein, um hybride Angriffe und Desinformation frühzeitig zu erkennen?

26. Welche Maßnahmen ergreift die Bundesregierung, um zivilgesellschaftliche Organisationen, Wissenschaft und Medien in die Erkennung und Bekämpfung von hybriden Angriffen und Desinformation einzubinden, und welche Kooperationen existieren hierzu?

27. Wann nimmt die Zentrale Stelle zur Erkennung ausländischer Informationsmanipulation (ZEAM) ihre Arbeit voraussichtlich auf, hat die ZEAM bereits konkrete Fälle von Desinformation bearbeitet, welche Kapazität für die Bearbeitung von Desinformation wird die ZEAM wann voraussichtlich haben, und wie viele Fälle von Desinformation kann diese Stelle voraussichtlich bearbeiten?

28. Welche Mechanismen nutzt die Bundesregierung, um die Wirksamkeit ihrer Maßnahmen gegen hybride Angriffe und Desinformation zu evaluieren und auf Basis dieser Erkenntnisse Strategien anzupassen?

29. Mit welchen Institutionen des Bundes und der Länder soll die ZEAM in Austausch treten, und wie wird der Prozess zur Analyse und Information bezüglich Desinformation bei der ZEAM aussehen?

30. Wie bewertet die Bundesregierung die deutsche Resilienz gegen ausländische Einflussnahme, welche Bedeutung kommt hierbei der Prävention in beispielsweise türkisch- oder russischstämmigen Communitys in Deutschland zu, und welche Maßnahmen unternimmt die Bundesregierung, um migrantische Communitys vor illegitimer Einflussnahme aus dem Ausland, insbesondere aus den Herkunftsstaaten, zu schützen?

31. Welche Bedeutung haben hierbei aus Sicht der Bundesregierung religiöse Einrichtungen und Organisationen, und welche Maßnahmen unternimmt die Bundesregierung, um den ausländischen Einfluss auf religiöse Organisationen zu begrenzen?

32. Welche Strategien anderer EU-Mitgliedstaaten zur Bekämpfung von hybriden Angriffen und Desinformation hat die Bundesregierung im Rahmen einer Best-Practice-Auswertung ausgewertet, und um welche Mitgliedstaaten handelt es sich insoweit?

33. Welche Maßnahmen dieser Staaten zur Bekämpfung von hybriden Angriffen und Desinformation sind aus Sicht der Bundesregierung auf Deutschland übertragbar und würden einen Mehrwert bei der Abwehr solcher Angriffe ergeben, und wie bewertet die Bundesregierung insbesondere

    a) die französische Beobachtungsstelle für digitale Einflussnahme aus dem Ausland „Viginum“,

    b) die schwedische Behörde für psychologische Verteidigung,

    c) die schwedische Initiative, die Zivilbevölkerung auch durch Flugblätter über Zivil- und Katastrophenschutz aufzuklären,

    d) das finnische Programm zur Schaffung und zum Erhalt von Schutzräumen für große Teile der Zivilbevölkerung,

    e) die Strategie der Königlich Dänischen Marine zur Festsetzung von Schiffen, die im Verdacht stehen, Unterseekabel in der Ostsee beschädigt zu haben,

    f) das niederländische Programm „Mediawijsheid“ (Medienkompetenz), durch welches die Medienkompetenz in Schulen und Kindergärten gefördert wird,

    g) die in Polen eingerichtete Task Force zur strategischen Kommunikation „Departament Komunikacji Strategicznej i Przeciwdziałania Dezinformacji Międzynarodowej“ zur Bekämpfung internationaler Desinformation?

34. Wie bewertet die Bundesregierung die Strategie der britischen Nachrichtendienste und des britischen Verteidigungsministeriums, durch sogenannte strategic declassification Fake News und Desinformation entgegenzuwirken und insbesondere mit Blick auf die Ukraine faktenbasierte Informationen zu veröffentlichen, plant die Bundesregierung vergleichbare Informationskampagnen?

35. Welche Erkenntnisse hinsichtlich ausländischer Einflussnahme hat die Bundesregierung aus den letzten beiden US-Präsidentschaftswahlen und der letzten Wahl zum Deutschen Bundestag gezogen, welche Angriffsmuster hat die Bundesregierung hierbei identifiziert, und welche Akteure stecken hinter den festgestellten Angriffen?

36. Mit welcher Art von Beeinflussung und ausländischer Einflussnahme auf die kommende Wahl zum Deutschen Bundestag rechnet die Bundesregierung, welches Konzept zur Verhinderung dieser Einflussnahme verfolgt die Bundesregierung, und welche Maßnahmen hat sie insoweit bereits getroffen bzw. wird diese bis zum Wahltermin noch treffen?

37. Welche Maßnahmen hat die Bundesregierung getroffen, um der Gefahr durch sogenannte Deepfakes und andere KI-generierte Inhalte im Vorfeld der kommenden Wahl zum Deutschen Bundestag zu begegnen?

Berlin, den 4. Dezember 2024

Christian Dürr 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