

Kleine Anfrage

der Abgeordneten Dr. Konstantin von Notz, Britta Haßelmann, Agnieszka Brugger, Claudia Roth (Augsburg), Tabea Rößner, Omid Nouripour, Manuel Sarrazin, Franziska Brantner, Renate Künast, Dr. Frithjof Schmidt, Dr. Irene Mihalic, Margit Stumpp, Margarete Bause, Kai Gehring, Uwe Kekeritz, Katja Keul, Dr. Tobias Lindner, Cem Özdemir, Filiz Polat, Dr. Manuela Rottmann, Jürgen Trittin, Ottmar von Holtz und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Aktivitäten der Bundesregierung gegen illegitime Beeinflussung demokratischer Willensbildungsprozesse

Die große Stärke westlicher Demokratien sind ihre offenen und pluralistischen Gesellschaften. Genau diese aber bieten auch vielfältige Angriffsflächen und sind damit in besonderem Maße durch hybride Aktivitäten verwundbar.

Belege gibt es genug: Für Einflussnahmen im Vorfeld und im Kontext demokratischer Wahlen (US-Wahl, www.tagesschau.de/ausland/einflussnahme-us-wahl-101.html; Brexit, www.deutschlandfunk.de/soziale-medien-und-das-brexit-referendum-propaganda-luegen.724.de.html?dram:article_id=430936) oder Referenden (<https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32018R0842&from=DE>), weitreichende IT-Angriffe auf Politikerinnen und Politiker (IT-Angriff auf den Bundestag www.tagesschau.de/thema/bundestag/index.html Doxing-Fall www.zeit.de/digital/datenschutz/2019-01/privatsphaere-doxing-daten-sammeln-datensicherheit-politiker), Medien (www.haz.de/Nachrichten/Digital/Verfassungsschutz-warnt-vor-Cyber-Angriffen-auf-deutsche-Medienhaeuser) sowie demokratische Institutionen. Auch die intransparente Verbreitung von Falschnachrichten mit dem Ziel, demokratische Diskurse bewusst zu manipulieren, das Vorgaukeln von Diskursmacht im Digitalen durch Bots und ganze Troll-Armeen oder die bewusste Parteinahme und Unterstützung politischer Kräfte, die das Ziel verfolgen, öffentliche Diskurse zu vergiften und die Demokratie in Frage zu stellen (www.zeit.de/politik/ausland/2018-12/us-wahl-2016-russland-einmischung-soziale-medien) – all dies sind Phänomene einer neuen hybriden Bedrohungslage über die gesamtgesellschaftlich seit Langem diskutiert wird, ohne dass die Bundesrepublik Deutschland nach Ansicht der Fragesteller bisher ihrem Anspruch einer wehrhaften Demokratie adäquat gerecht geworden wäre und Antworten auf diese neuen Strategien bewusster Destabilisierung und Zersetzung gefunden hätte.

Während in anderen Ländern und auf Ebene der Europäischen Union Politik und Zivilgesellschaft versuchen, zurückliegende Einflussnahmen und Manipulationsversuche (https://ec.europa.eu/germany/news/20181126-umfrage-einflussnahme-auf-wahlen_de) zu analysieren und intensiv an Gegenstrategien gearbeitet wird, bleiben vergleichbare Handlungen von Seiten der Bundesregierung nach Ansicht der fragestellenden Fraktion bislang weitgehend aus. Trotz zahlreicher Hinweise

auf weitreichende Manipulationsversuche staatlicher und nichtstaatlicher Akteure, trotz nachgewiesener Versuche bewusster Diskursverschiebungen im Zuge von (Landtags-)Wahlen, beispielsweise durch rechte Netzwerke (www.br.de/nachrichten/bayern/kampf-um-bayern-online-kampagnen-zur-landtagswahl-2018,RI7e9qg), trotz erfolgreicher IT-Angriffe auf Privatpersonen und demokratische Institutionen wie den Deutschen Bundestag, trotz durch Medienberichte aufgedeckter Einflussnahmen auf Abgeordnete des Deutschen Bundestages, die nach Angabe ausländischer Akteure unter „totaler Kontrolle“ stehen (vgl. DER SPIEGEL 6. April 2019), trotz massiver Stimmungsmache in erfundenen Fällen wie dem sogenannten Fall Lisa (www.spiegel.de/politik/ausland/russland-deutsche-geheimdienste-werfen-moskau-gezielte-stimmungsmache-vor-a-1129853.html) durch ausländische Regierungen, trotz einer an Intensität zuletzt stark zugenommenen öffentlichen Debatte über diese Problemlagen (www.gruen-digital.de/2018/11/6-netzpolitische-soire-hacked-democracy-demokratie-schuetzen-am-4-dezember-in-berlin/) und trotz vielfacher Warnungen von Seiten der Nachrichtendienste vermisst die fragestellende Fraktion noch immer die notwendige Sensibilität auf Seiten der Bundesregierung.

Wenn bewusst und intransparent Zweifel gesät werden und wenn versucht wird, das Vertrauen in öffentliche Debatten, in demokratische Wahlen und auch in die internationale Kooperation von Staaten zu untergraben, braucht es nach Ansicht der Fragesteller nationale und internationale Gegenstrategien.

Auch zahlreiche parlamentarische Nachfragen im Deutschen Bundestag, vorgelegte Initiativen (vgl. exemplarisch Anträge der Fraktion BÜNDNIS 90/DIE GRÜNEN „IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern“ auf Bundestagsdrucksache 19/1328 und „Für wehrhafte Demokratien in Europa – Rechtsstaatlichkeit und Grundrechte in den Mitgliedsländern der EU stärken“ auf Bundestagsdrucksache 19/7436) und durch die Fachausschüsse durchgeführte Expertengespräche (www.bundestag.de/ausschuesse/a23_digital/anhoerungen?url=L2F1c3NjaHVlc3NIL2EyM19kaWdpdGFsL2FuaG9lcnVuZ2VuL2FuaG9lc nVuZy01OTIzNzA=&mod=mod557988) haben bislang nicht dazu geführt, dass die Bundesregierung sich nach Meinung der fragestellenden Fraktion der Problematik mit der notwendigen Ernsthaftigkeit zugewendet und entsprechende Gegenstrategien für diese unterschiedlich gelagerten Phänomene und Problemlagen entwickelt hätte.

Bei der Abwehr hybrider Bedrohungen sind aus demokratischer Sicht gewichtige Güterabwägungen zu treffen. Im Bereich der Bekämpfung von Desinformation geht es oftmals nicht um eindeutig rechtswidrige Inhalte wie Volksverhetzung oder den Aufruf zu Straftaten, sondern nachweislich falsche oder irreführende Informationen, die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und öffentlichen Schaden anrichten können. Hier muss aus Sicht der Fragesteller ein Gleichgewicht gefunden werden zwischen der Notwendigkeit, Bürgerinnen und Bürger sachlich korrekt zu informieren, und dem Recht auf freie Meinungsäußerung. In Aussicht gestellte Maßnahmen wie beispielsweise veränderte Strukturen zur verbesserten Erkennung neuer hybrider Bedrohungen wurden aus Sicht der Fragesteller bislang nicht angegangen.

Während die EU-Kommission sich seit Jahren mit den neuen hybriden Bedrohungen beschäftigt und im Vorfeld der kommenden Europawahlen einen entsprechenden Aktionsplan zum Schutz (https://eeas.europa.eu/headquarters/headquarters-homepage/56267/aktionsplan-gegen-desinformation_de) derselben verabschiedet hat, vermisst die fragestellende Fraktion eine angemessene Beschäftigung mit der Thematik seitens der Bundesregierung bis heute. Eine solche ist allerdings angesichts der relevanten Gefahr für demokratische Diskurse auch sicherheitspolitisch dringend geboten.

Wir fragen die Bundesregierung:

1. Sieht sich die Bundesregierung weiterhin lediglich „Desinformations- und Propagandamaßnahmen“ und keinen belegbaren „hybriden Bedrohungen“ ausgesetzt (vgl. u. a. die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN „Rechtspopulismus, Rechtsextremismus und Politische Desinformation im Netz“ auf Bundestagsdrucksache 19/2224 sowie die Antwort auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/9388) oder liegen der Bundesregierung mittlerweile Erkenntnisse für den Einsatz darüber hinausgehender hybrider Kampagnen in Deutschland vor, und für wie groß hält die Bundesregierung die derzeitige Bedrohung durch hybride Kampagnen insgesamt?
2. Liegen der Bundesregierung gegenwärtig konkrete Erkenntnisse bezüglich gezielter Beeinflussungsmaßnahmen der EU-Wahlen 2019 bis hin zu aggressiven Cyberkampagnen (APTs) durch Drittstaaten vor, und wenn ja, welche?
3. Welche Vorkommnisse der vergangenen fünf Jahre zählt die Bundesregierung als Elemente einer hybriden Bedrohung und/oder Bestandteil hybrider Kampagnen?
4. Welche Position vertritt die Bundesregierung im Hinblick auf den Vorschlag der EU-Kommission für die Schaffung nationaler Netze der Zusammenarbeit bei Wahlen speziell im Hinblick auf Wahlfragen, IT-Sicherheit, Datenschutz, Strafverfolgung usw. (vgl. PM EU-KOM vom 29. Januar 2019, IP/19/746), und welche Behörde soll als Kontaktstelle für ein europäisches Kooperationsnetz für Wahlen benannt werden?
5. Welche konkreten Möglichkeiten unterstützt die Bundesregierung für die verstärkte Beteiligung der Forschung, um Ausbreitung und Auswirkungen von Desinformation besser nachvollziehen zu können?
6. Welche konkreten Anstrengungen hat die Bundesregierung in Vorbereitung auf die nationale Sicherheit der EU-Wahlen unternommen, etwa in Gestalt von Sicherheitsprogrammen von Akteuren im konkreten Wahlprozess, in Vorbereitung von Kommunikationsstrategien bei Zwischenfällen oder in Gestalt der Durchführung von Informationskampagnen in der Bevölkerung (zu gebotenen Maßnahmen nach Ansicht der Fragesteller instruktiv: Der Schutz von Wahlen in vernetzten Gesellschaften, Papier der Stiftung Neue Verantwortung, Oktober 2018)?
7. Welche internationalen Netzwerke, die illegitime Beeinflussung demokratischer Willensbildungsprozesse in Deutschland vorantreiben oder einsetzen, sind der Bundesregierung bekannt?
Welche Reiseaktivität aus Deutschland hat die Bundesregierung in diesem Zusammenhang beobachten können?
8. Welche inländischen Gruppen oder Strukturen sind der Bundesregierung bekannt, die mit diesen internationalen Netzwerken in Verbindung stehen und zusammenarbeiten?

9. Hält die Bundesregierung auch angesichts der Tatsache, dass neue hybride Bedrohungslagen bereits in dem im Juli 2016 vorgestellten „Weißbuch der Bundesregierung zur Sicherheitspolitik und zur Zukunft der Bundeswehr“ als eine zentrale sicherheitspolitische Herausforderung charakterisiert werden, bestehende Strukturen zur Erkennung derartiger Bedrohungen für ausreichend, und ist die Bundesregierung der Ansicht, dass eine wirksame ressortgemeinsame und gesamtstaatliche Sicherheitsvorsorge zur Unterbindung und Abwehr hybrider Angriffe derzeit gegeben ist?

Welche Schritte wurden diesbezüglich bisher unternommen bzw. sind gegenwärtig in der Umsetzung oder Planung?

10. Sollte die Bundesregierung bestehende Strukturen für nicht ausreichend erachten, wie will man sich national zukünftig besser aufstellen, und welche Rolle sollen hierbei Cyberabwehrzentrum (plus), das Bundesamt für Verfassungsschutz, das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr und der Beauftragte im Auswärtigen Amt für Cyber-Außenpolitik spielen?
11. Sollte die Bundesregierung bestehende Strukturen für nicht ausreichend erachten, wie möchte sie sich in Zukunft europäisch besser aufstellen, und welche Rolle kommen hierbei den bei Europol angesiedelten Zentren gegen Cyberkriminalität sowie gegen Terrorismus oder dem Computersicherheits-Ereignis- und Reaktionsteam der EU (CERT-EU) jeweils zu?
12. Welche konkreten Schritte hat die Bundesregierung bisher und wird sie in Zukunft auf internationaler Ebene unternehmen, um einen besseren Schutz vor Desinformationskampagnen und der Beeinflussung von demokratischen Prozessen zu erreichen?
- a) Welche internationalen Regeln und Vereinbarungen will die Bundesregierung erreichen?
- b) Welche diesbezüglichen Initiativen plant die Bundesregierung im Rahmen der gegenwärtigen Mitgliedschaft im Sicherheitsrat der Vereinten Nationen?
- c) Plant die Bundesregierung, das Thema auch im Rahmen des dieses Jahr in Deutschland stattfindenden Internet Governance Forums zu thematisieren?
- Falls ja, in welcher konkreten Form, und falls nicht, warum nicht?
13. Welche Bundesministerien, Behörden und Stellen sollen an der Erkennung und Abwehr hybrider Bedrohungen nach dem Willen der Bundesregierung beteiligt sein (bitte auflisten), und wie wird die Bundesregierung ein rechtsstaatliches und verlässliches Zusammenwirken dieser gewährleisten?
14. Wie beurteilt die Bundesregierung die Arbeit des NATO Cooperative Cyber Defence Centres in der Abwehr hybrider Bedrohungen, und in welcher Weise fließen die Ergebnisse der Arbeit des Zentrums in die deutsche Sicherheitsvorsorge ein?
15. In welcher Weise hat sich die Bundesregierung an der NATO-Übung Locked Shields 2019 beteiligt, und wenn ja, mit welchen Ergebnissen?

16. Hat die Bundesregierung bereits in allen Ressorts, in deren Zuständigkeit mögliche Einzelmaßnahmen zur Abwehr komplexer hybrider Bedrohungen liegen, Kopfstellen benannt, die im Eventualfall eine schnelle gesamtstaatliche Reaktion ermöglichen (vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/9388)?

Falls ja, in welchen Bundesministerien genau?

Falls nein, warum noch nicht, und in welchen Ressorts aus welchem konkreten Grund noch nicht?

17. Bleibt die Bundesregierung bei ihrer Ansicht, dass vor allem die „frühzeitige Aufklärung einer hybriden Bedrohung sowie die Stärkung von Resilienz“ von entscheidender Bedeutung sind (vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/9388), um auf neue Bedrohungslagen angemessen reagieren zu können?

Falls ja, wie passt das mit derzeitigen Plänen der Bundesregierung zusammen, die das Ziel verfolgen, offensive Kapazitäten zu stärken und digitale Gegenschläge und sogenannte Hackbacks zu ermöglichen?

18. Sind durch die Bundesregierung oder ihr unterstellte Behörden bereits sogenannte Hackbacks durchgeführt worden (wenn ja, bitte auflisten nach Art des Angriffs, Attribution, Zeitpunkt der Attribution, Auswahl des Ziels, beteiligten Behörden und Art der Beteiligung)?

19. Bleibt die Bundesregierung bei der bislang von ihr vertretenen Meinung, dass es für derartige Hackbacks keines Mandats des Deutschen Bundestages bedarf, dies vielmehr nur im jeweiligen Einzelfall entschieden werden kann (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/3420)?

Falls ja, wer entscheidet im Einzelfall?

20. Ist im Hinblick auf die „aktive Abwehr“ von IT-Angriffen der Prüfvorgang innerhalb der Bundesregierung zur Frage, wie man mit der Attributionsproblematik bei IT-Angriffen und ihrer Abwehr umzugehen gedenkt, bereits abgeschlossen (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/3420)?

Falls ja, mit welchem Ergebnis?

21. Welche Versuche einer illegitimen Einflussnahme durch ausländische staatliche und nichtstaatliche Akteure hat es nach Kenntnis der Bundesregierung bei Wahlgängen in Deutschland seit September 2013 gegeben?

22. Welche Versuche illegitimer Einflussnahme durch ausländische staatliche und nichtstaatliche Akteure hat es nach Kenntnis der Bundesregierung bei Wahlkämpfen in Deutschland seit September 2013 gegeben?

23. Teilt die Bundesregierung die Ansicht der Fragesteller, dass die Stärkung von Resilienz nur dadurch zu erreichen sein wird, die eigene IT-Sicherheitspolitik grundlegend zu überdenken und beispielsweise bestehende Sicherheitslücken schnellstmöglich im Zusammenspiel von staatlichen Stellen und Privatwirtschaft zu schließen, und wenn nein, warum nicht?

24. Ist die entsprechende Prüfung innerhalb der Bundesregierung bereits abgeschlossen, und wenn ja, was ist das konkrete Ergebnis, und plant die Bundesregierung, nunmehr eine Meldepflicht für Sicherheitslücken für staatliche Stellen zu schaffen (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/3420), und wenn nein, warum nicht?

25. Welche Anstrengungen hat die Bundesregierung bislang mit welchen Staaten unternommen, um zu einem Capacity Building zur weltweiten Schließung von Sicherheitslücken zu kommen?
26. Welche Pläne hat die Bundesregierung für die anstehende EU-Ratspräsidentschaft im Hinblick auf die Stärkung des EU-Rahmens gegen hybride Bedrohungen?
27. Bleibt die Bundesregierung bei der bisher vertretenen Ansicht, dass Schwachstellen, deren Nutzung weitreichende Auswirkungen auf die Sicherheit der Bevölkerung bzw. des Staates haben, auch durch staatliche Stellen gemeldet werden sollen, andere aber nicht (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/3420), und wer soll nach Ansicht der Bundesregierung zukünftig prüfen und entscheiden, ob dies für eine entdeckte Lücke zutrifft oder nicht, und wie kann eine solche Entscheidung nach Ansicht der Bundesregierung gerichtlich überprüft und parlamentarisch kontrolliert werden?
28. Welche Szenarien und Maßnahmen sind während der „Live-Fire-Cyber-Abwehr Übung“ Locked Shields 2019 vom 9. bis 12. April 2019 des NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn/Estland zur „Abwehr von Fake News“ geplant oder geübt worden, an denen sich die Bundeswehr beteiligte (vgl. <https://cir.bundeswehr.de/portal/poc/cir?uri=ci%3Abw.cir.service.archiv.2019.apr&de.conet.contentintegrator.portlet.current.id=01DB16000000001%7CBAXA9Q092DIBR>)?
29. Welche Rolle kann und sollte die Bundeswehr nach Auffassung der Bundesregierung in der Abwehr von „Desinformation“ spielen?
30. Welche rechtlichen Befugnisse hat die Bundeswehr nach Auffassung der Bundesregierung, um gegen die Verbreitung von Informationen und Desinformationen im Inland oder im Ausland vorzugehen?
31. Welche Erkenntnisse hat die Bundesregierung zu Anwerbungs- und Infiltrationsversuchen von Mandatsträgerinnen und Mandatsträgern und Kandidatinnen und Kandidaten für öffentliche Ämter in Deutschland durch ausländische Nachrichtendienste?
 - a) Wie viele Fälle von Anwerbungs- und Infiltrationsversuchen von Bundestagsabgeordneten durch ausländische Nachrichtendienste in den letzten fünf Jahren sind der Bundesregierung bekannt (bitte nach Staat, Parteizugehörigkeit, Art und Intensität der Einflussnahme aufschlüsseln)?
 - b) Wie viele Ermittlungsverfahren hat der Generalbundesanwalt wegen der §§ 94 ff. des Strafgesetzbuchs in den letzten fünf Jahren im Zusammenhang mit Mandatsträgerinnen und Mandatsträgern und Kandidatinnen und Kandidaten für öffentliche Ämter geführt (bitte in Bezug auf Staaten und Parteizugehörigkeit aufschlüsseln)?
32. Welche eigenen Erkenntnisse hat die Bundesregierung über „materielle und mediale Unterstützung“ von Bundestagsabgeordneten durch Russland (vgl. DER SPIEGEL, 6. April 2019), und wie ordnet sie eine solche mögliche Unterstützung rechtlich ein?
33. Inwiefern sind der Bundesregierung Einflussnahmeversuche von anderen Staaten als Russland auf Bundestagsabgeordnete bekannt?
34. Welche Erkenntnisse hat die Bundesregierung zu Anwerbungs- und Infiltrationsversuchen von Mitarbeitern von Abgeordneten im Deutschen Bundestag durch ausländische Nachrichtendienste, und wie viele Fälle in den letzten fünf Jahren sind der Bundesregierung bekannt (bitte nach Staat, Fraktionszugehörigkeit, Art und Intensität der Einflussnahme aufschlüsseln)?

35. Wie oft haben Bundestagsabgeordnete während der 19. Wahlperiode für Reisen nach Russland die diplomatischen Institutionen der Bundesrepublik Deutschland um Unterstützung gebeten bzw. vorab konsultiert (bitte nach Fraktionen aufschlüsseln)?
36. Gibt es in der Bundesregierung eine Stelle, die für die Identifizierung von durch ausländische Regierungen gesteuerte Medienunternehmen in Deutschland zuständig ist, und wenn ja, welche?
37. Hat die Bundesregierung über die in der Kleinen Anfrage „Rechtspopulismus, Rechtsextremismus und Politische Desinformation im Netz“ (Bundestagsdrucksache 19/2224, Frage 25) genannten hinausgehende Erkenntnisse über von ausländischen Regierungen gesteuerte Medienunternehmen, welche gezielt in Deutschland Desinformationen verbreiten?
38. Welche Strategie hat die Bundesregierung, insbesondere in Zusammenarbeit mit den Bundesländern, zur Verhinderung von gezielter Desinformation durch von ausländischen Regierungen gesteuerte Medienunternehmen?
39. Vertritt die Bundesregierung die Ansicht, dass die Aufsicht der Medien verbessert werden muss in Anbetracht der Gefahr von Desinformation durch von ausländischen Regierungen gesteuerte Medienunternehmen, und wenn ja, durch welche Maßnahmen?
40. Wie beurteilt die Bundesregierung Berichte über gezielte Einflussnahmen Chinas, die der ehemalige Präsident des Verfassungsschutzes Hans-Georg Maaßen als „breit angelegten Versuch der Infiltration insbesondere von Parlamenten, Ministerien und Behörden“ bezeichnet hat (vgl. ntv.de vom 6. Juli 2018 „Agenten Chinas in Deutschland Spione infiltrierten offenbar den Bundestag“, abrufbar unter www.n-tv.de/politik/Spione-infiltrierten-offenbar-den-Bundestag-article20516278.html)?
 - a) Welche Strategien und Formen der Beeinflussung einzelner Mandatsträger und der Mitarbeiter von Behörden sind nach Kenntnis der Bundesregierung Teil dieser chinesischen Strategie?
 - b) Welche Rolle spielt nach Kenntnis der Bundesregierung gezielte Falschinformation zu Gunsten Chinas?
 - c) Welche Intentionen und konkreten Interessen verfolgen chinesische Sicherheitsbehörden nach Ansicht der Bundesregierung mit diesen gezielten Einflussnahmen?
 - d) Sind nach Kenntnis der Bundesregierung alle Fraktionen des Deutschen Bundestages von solchen Versuchen der Einflussnahme in gleichem Maß betroffen?
41. Hält die Bundesregierung den Verhaltenskodex für die Selbstregulierung im Bereich Online-Desinformation, den die EU-Kommission im April 2018 mit zahlreichen Stakeholdern ausgehandelt hatte, für hinreichend, um die wichtigsten Parameter wie die Transparenz politischer Werbung, die Schließung von Scheinkonten und die Kennzeichnung für automatisierte Bots zu erreichen?

Wenn nicht, welche zusätzlichen Maßnahmen möchte die Bundesregierung in Deutschland durchsetzen und in Zukunft auf europäischer Ebene anstreben (vgl. hierzu unter anderem die Antwort der Bundesregierung auf die Schriftliche Frage 27 der Abgeordneten Dr. Franziska Brantner auf Bundestagsdrucksache 19/6961)?

42. Inwieweit wird nach Kenntnis der Bundesregierung der Verhaltenskodex für die Selbstregulierung im Bereich Online-Desinformation, den die EU-Kommission im April 2018 mit zahlreichen Stakeholdern ausgehandelt hatte, in Deutschland und in anderen europäischen Mitgliedstaaten umgesetzt?

Wann und wie hat die Bundesregierung der EU-Kommission die Informationen über die Umsetzung des Verhaltenskodex für die Selbstregulierung im Bereich Online-Desinformation bereitgestellt, und welche Schlussfolgerungen ergeben sich im Hinblick auf die Integrität der Europawahl 2019 aus dem Bericht der Bundesregierung?

Berlin, den 25. April 2019

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion