Deutscher Bundestag **Drucksache 20/13937**

20. Wahlperiode 22.11.2024

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/13660 –

Digitale Technologien – Neue Aufklärungs- und Wirkmöglichkeiten

Vorbemerkung der Fragesteller

Neue digitale Anwendungen für Technologien führen zu neuen Herausforderungen, neuen Konstellationen und Veränderungen in vielen Bereichen. Beispielsweise wird durch neue technische Möglichkeiten und daraus entstehende Bedarfe der Weltraum zunehmend eine Sphäre geopolitischer Interessen. Unsere vernetzten Ökonomien und Gesellschaften fragen immer mehr Satellitendienstleistungen nach und auch das militärische Potenzial zur Nutzung des Weltraums steigt mit neuen technologischen Möglichkeiten (siehe u. a. hier: www.zeit.de/digital/datenschutz/2024-03/starshield-us-militaer-spacex-satelliten-ueberwachung und www.tagesschau.de/ausland/amerika/starlink-internet-musk-100.html und www.sueddeutsche.de/projekte/artikel/politik/militaer-weltall-szenarien-e969752/?reduced=true). Auch in anderen Bereichen, wie Drohnen, Chips, künstliche Intelligenz (KI), Quanten, Fahrzeugen, Satelliteninternet u.v.m. gibt es neue Entwicklungen, die mit weitreichenden Änderungen verbunden sind – insbesondere, wenn die neuen Technologien oder die neuen digitalen Anwendungsmöglichkeiten mit künstlicher Intelligenz verbunden sind oder durch Cyberangriffe neue Angriffsvektoren entstehen können.

1. Wie stark wird nach Einschätzung der Bundesregierung der Energiebedarf in Deutschland in den nächsten Jahren durch KI-Entwicklungen und KI-Anwendungen steigen (www.welt.de/wirtschaft/article253629860/Wegen-KI-US-Reaktor-soll-fuer-Microsoft-wieder-ans-Netz.html und www.tagesspiegel.de/berlin/berliner-wirtschaft/kunftige-rechenzentren-fressen-unmengen-energie-netzbetreiber-will-stromanschlusse-in-berlin-bald-fairer-verteilen-12517235.html), und welche Maßnahmen sind nach Einschätzung der Bundesregierung notwendig, um die Bereitstellung der erforderlichen Energie sicherzustellen?

Der in den nächsten Jahren zu erwartende Anstieg des Energiebedarfs durch KI-Entwicklungen und KI-Anwendungen unterliegt erheblichen Unsicherheiten. Es ist grundsätzlich davon auszugehen, dass die fortschreitende Digitalisierung zu einem Anstieg des Stromverbrauchs führt. Am objektiv sichtbarsten ist dies am Stromverbrauch von Rechenzentren, der Basis für KI-Anwendungen. Auf Basis einer Marktabfrage schätzen die Übertragungsnetzbetreiber im aktuellen Entwurf des Szenariorahmens Strom einen Stromverbrauch für 2037 und

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Wirtschaft und Klimaschutz vom 21. November 2024 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

2045 von 39 bis 88 Terawattstunden durch Rechenzentren. Die Bestätigung des Szenariorahmens durch die Bundesnetzagentur steht noch aus. Auch Studien von Bitkom und dem Borderstep-Institut sehen den Strombedarf von Rechenzentren in Deutschland bis 2030 zwischen 25 und 35 Terawattstunden pro Jahr. Aktuell liegt der Verbrauch deutscher Rechenzentren bei ca. 20 Terawattstunden pro Jahr.

2. Inwieweit beabsichtigt die Bundesregierung, Energienetzbetreiber bei der Sicherstellung der zusätzlichen Energiebereitstellung zu unterstützen – Bezug nehmend zu Frage 1?

Um die Energieversorgung von Rechenzentren sicherzustellen, sollten potentielle Standorte möglichst frühzeitig in der Stromnetzplanung berücksichtigt werden. Die Bundesregierung begrüßt daher den Prozess der Marktabfrage im Rahmen der Netzentwicklungsplanung. Der daraus resultierende Netzausbau wird mit dem Bundesbedarfsplan auf eine gesetzliche Grundlage gestellt.

3. Plant auch die Bundesregierung ein Verbot chinesischer Hard- und Softwarekomponenten für in Deutschland zugelassene Fahrzeuge (www.sueddeutsche.de/wirtschaft/autoindustrie-usa-wollen-chinesische-und-russische-autosysteme-verbieten-dpa.urn-newsml-dpa-com-20090101-240923-930-240918), und wenn ja, für welche Fahrzeuge, und ab wann?

Nein. Ein solches Verbot könnte die Bundesregierung auch nicht im Alleingang beschließen, da die EU-Typgenehmigungsvorschriften der Verordnung (EU) 2018/858 einen harmonisierten Rechtsrahmen für die Genehmigung aller Fahrzeuge der Klasse M in der EU festlegen. Dieser Rahmen enthält Verwaltungsvorschriften und technische Anforderungen für die Genehmigung aller in ihren Geltungsbereich fallenden Neufahrzeuge. Die Verordnung (EU) 2019/2144 ergänzt die Verordnung (EU) 2018/858 um sicherheitsrelevante Anforderungen. Die Verordnung (EU) 2019/2144 sieht in Anhang II die Anwendung der UN-Regelung 155 zum Schutz des Fahrzeugs gegen Cyberangriffe vor. Ein entsprechendes nationales Verbot würde diesen harmonisierten Vorschriften widersprechen.

4. Sieht die Bundesregierung potenzielle Gefahren durch mögliche Fernzugriffe aus anderen Staaten auf Fahrzeuge in Deutschland – sei es durch Fahrzeugsoftware, oder durch Apps (vgl. Antwort zu Frage 34 auf Bundestagsdrucksache 20/12872)?

Ja. Es wird im Übrigen auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/8338 verwiesen.

5. Was unternimmt die Bundesregierung, um den Gefahren von Massenüberwachung, Spionage und Sabotage durch Fahrzeuge zu begegnen (www.nzz.ch/mobilitaet/nationale-sicherheit-usa-erwaegen-verbot-von-vernetzten-autos-aus-china-ld.1850055)?

Die Bundesregierung prüft ressortübergreifend Fragen, die sich bei der Erhebung, Speicherung und dem Transfer von Kfz-Daten stellen können, mit dem Ziel, konkrete Vorschläge zu erarbeiten, um die Wirksamkeit bestehender Kontroll- und Schutzmaßnahmen für Daten- und Cybersicherheit bei vernetzten Fahrzeugen zu überprüfen und gegebenenfalls neue und verbesserte Anforde-

rungen auf nationaler und europäischer Ebene zu entwickeln. Im Übrigen schützen auch die bisher existierenden europäischen Vorschriften vor entsprechenden Gefahren, vgl. Antwort zu Frage 3.

6. Möchte die Bundesregierung den Abfluss von Daten, die von Fahrzeugen in Deutschland generiert werden (durch Kameras, Mikrofone, Satellitensysteme oder andere Technologien) auf Server in außereuropäische Staaten einschränken oder verhindern, und wenn ja, wie?

Es wird auf die Antworten zu den Fragen 3 und 5 verweisen. Im Übrigen sind hier auch weitere europäische Vorschriften, wie die Datenschutz-Grundverordnung und der Data Act, die den Datentransfer in außereuropäische Staaten begrenzen, maßgeblich.

7. Wurde der in der Raumfahrtstrategie der Bundesregierung (www.bmwk.de/Redaktion/DE/Publikationen/Technologie/20230927-raumfahrtstrategie-breg.pdf?__blob=publicationFile&v=10) angekündigte Space Innovation Hub bereits gegründet, und wenn nein, wann soll er im Geschäftsbereich welches Ressorts gegründet und angesiedelt werden?

Der Space Innovation Hub wird in der Raumfahrtstrategie der Bundesregierung im Handlungsfeld „Raumfahrt als Wachstumsmarkt, Hightech und NewSpace“ als Schlüsselprojekt ausgewiesen.

Hierbei geht es um den Aufbau einer Anlaufstelle für die NewSpace-Szene, um Ideen für innovative Projekte und Umsetzungsmöglichkeiten gemeinsam mit zivilen und militärischen Akteuren zu entwickeln. Die dafür notwendige Plattform soll über die Deutsche Raumfahrtagentur im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) aufgebaut werden.

Das Schlüsselprojekt Space Innovation Hub muss neu initiiert werden. Die Bundesregierung, konkret das BMWK, befindet sich mit der Deutschen Raumfahrtagentur im Austausch und in der konzeptionellen Erstellung der Aufgaben des Space Innovation Hub und des Aufbaus einer Plattform. Ziel ist, bis Ende des Jahres 2024 erste Angebote der Space-Innovation-Hub-Plattform vorzustellen.

8. Hat der Vertragsschluss zum EU-Programm für sichere Konnektivität 2023 bis 2027 der EU mit dem Namen „Infrastruktur für Resilienz, Interkonnektivität und Sicherheit durch Satelliten“ (IRIS^2)“ unter Bezugnahme auf die Antwort der Bundesregierung zu Frage 1f auf Bundestagsdrucksache 20/12487, wonach die Bundesregierung mit einer Verschiebung des Vertragsschlusses bis zum dritten Quartal 2024 plant, inzwischen stattgefunden?

   a) Wenn nein, wann rechnet die Bundesregierung stattdessen mit einem Vertragsschluss?

Die Fragen 8 und 8a werden gemeinsam beantwortet.

Nein, die Vertragsvergabe steht noch aus. Als wichtiger Zwischenschritt wurde am 31. Oktober ein sogenannter „Award“ an das Industriekonsortium (SES, Eutelsat, Hispasat) vergeben mit der Absicht, den Vertrag bis Ende des Jahres zu unterzeichnen. Es wird mit einer erfolgreichen Verkündung des Vertragsabschlusses zum 13. Dezember 2024 gerechnet.

b) Wenn ja, umfasst der Vertrag nach Kenntnis der Bundesregierung bereits alle Unterauftragnehmer, an die Aufträge durch das Konsortium zum Aufbau von IRIS^2 vergeben werden sollen?

d) Wenn ja, umfasst das Angebot nach Kenntnis der Bundesregierung die Integration von technologischen Innovationen im Bereich künstlicher Intelligenz (KI) in den Aufbau von IRIS^2?

e) Wenn ja, wie hoch werden nach Kenntnis der Bundesregierung die Betriebskosten für IRIS^2 pro Jahr sein?

f) Wenn ja, welche finanziellen Anteile sollen nach Kenntnis der Bundesregierung von der Privatwirtschaft geleistet werden?

g) Wenn ja, wie sieht die Verteilung von Arbeitspaketen unter den beteiligten Industrien und Unternehmen aus?

Die Fragen 8b und 8d bis 8g werden gemeinsam beantwortet.

Nicht zutreffend, siehe Antwort zu Frage 8a.

c) Wenn das Best and Final Offer nicht bereits alle Unterauftragnehmer, an die Aufträge durch das Konsortium zum Aufbau von IRIS2 vergeben werden sollen, umfasst, in welchem Zeitraum sollen nach Kenntnis der Bundesregierung Angebote von Unterauftragnehmern durch das Konsortium eingeholt werden?

Das „best and final offer“ sowie auch das finale Angebot umfasst noch nicht sämtliche Unterauftragnehmer. Eine Auswahl und Vertragsvergabe an die Unterauftragnehmer stehen noch aus. Nach Kenntnis der Bundesregierung soll im Rahmen der nach Vertragsabschluss anschließenden 12-monatigen Designphase die Auswahl der Unterauftragnehmer umgesetzt werden.

9. Ist nach Kenntnis der Bundesregierung unter Bezugnahme auf die Antwort zu Frage 10 auf Bundestagsdrucksache 20/12487, die Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 20/10953 und zu Frage 14 auf Bundestagsdrucksache 20/11539 das Auswahlverfahren zum GOVSATCOM-Hub im EU-Programm für sichere Konnektivität 2023 bis 2027 der EU mit dem Namen „Infrastruktur für Resilienz, Interkonnektivität und Sicherheit durch Satelliten“ (IRIS^2)“ bereit abgeschlossen?

a) Wenn ja, welche zwei der drei in der Antwort zu Frage 14c auf Bundestagsdrucksache 20/11539 genannten Bewerber wurden Bezug nehmend auf die Antwort zu Frage 14a auf Bundestagsdrucksache 20/11539 ausgewählt?

Die Fragen 9 und 9a werden gemeinsam beantwortet.

Nein, das Vergabeverfahren ist noch nicht abgeschlossen.

b) Wenn nein, wann ist der Abschluss des Auswahlverfahrens nach Kenntnis der Bundesregierung stattdessen geplant?

Der Abschluss des Vergabeverfahrens wird unmittelbar erwartet.

10. Hat die Bundeswehr Zugang zu den Diensten von Starshield (www.zeit.de/digital/datenschutz/2024-03/starshield-us-militaer-spacex-satellitenueberwachung), und wenn nein, plant die Bundesregierung, der Bundeswehr ein eigenes System analog zu Starshield im Weltraum zur Verfügung zu stellen?

Die Bundeswehr hat derzeit keinen Zugang zu den Diensten von Starshield. Das Bundesministerium der Verteidigung (BMVg) plant derzeit nicht, der Bundeswehr ein eigenes System, analog zu Starshield, im Weltraum zur Verfügung zu stellen.

11. Plant die Bundesregierung, privatwirtschaftliche Initiativen zu fördern, die der Bundeswehr ein System analog zu Starlink zur Verfügung stellen könnten?

In ziviler Hinsicht ist im nationalen Programm keine Starlink-Alternative geplant. Im Übrigen wird auf die Antwort zu Frage 10 verwiesen.

12. Wie plant die Bundeswehr, Schwärme von Kampfdrohnen zu steuern bzw. eine Änderung des Ziels auch noch aus großer Entfernung zu ermöglichen, wenn gleichzeitig kein Aufbau eines Satelliteninternets für die Bundeswehr vorgesehen ist (Bezug nehmend auf die Antwort zu den Fragen 14 und 15 auf Bundestagsdrucksache 20/12824)?

Die Entwicklung und der Einsatz von Schwärmen, die „Kampfdrohnen“ einschließen, sind derzeit nicht geplant.

13. Welche Position vertritt die Bundesregierung bei der Verwendung von KI zu militärischen Zwecken (siehe u. a. hier: www.faz.net/aktuell/wirtschaft/kuenstliche-intelligenz/wie-ki-militaerisch-verantwortungsvoll-eingesetzt-werden-kann-110001292.html)?

Wie in der Strategie Künstliche Intelligenz der Bundesregierung (Fortschreibung) ausgeführt, prüft die Bundeswehr die Nutzung von KI einerseits zur Erfüllung des Kernauftrages ihrer Streitkräfte und zur Gewinnung von Informations-, Entscheidungs- und Wirkungsüberlegenheit, andererseits in der Optimierung von administrativen und logistischen Prozessen und in der vorausschauenden Wartung von komplexen Systemen. Zudem kommt KI zur Unterstützung des Fachpersonals im Rahmen der zivil-militärischen, ressortübergreifenden Krisenfrüherkennung bei der Analyse von Massendaten und für Prognosen zum Einsatz. KI ist integraler Bestandteil wesentlicher Rüstungsprojekte, welche auch im europäischen Kontext umgesetzt werden und somit zum Erhalt und zur Förderung europäischer, technologischer Exzellenz beitragen. KI dient mit Blick auf die nationale und internationale technologische Entwicklung im Rüstungsbereich der Sicherstellung der für die Landes- und Bündnisverteidigung künftig erforderlichen Fähigkeiten.

14. Plant die Bundesregierung, einen Regulierungsrahmen für KI zur Verwendung bei militärischen Zwecken zu schaffen?

Die Bundesregierung bekennt sich zur verantwortungsvollen Nutzung von KI im militärischen Bereich und setzt sich auf internationaler Ebene aktiv dafür ein, entsprechende Normen zu setzen und zu implementieren.

15. Plant die Bundesregierung, auch eine KI-Strategie für Sicherheitsbehörden und Militär zu erstellen (www.whitehouse.gov/briefing-room/statements-releases/2024/10/24/fact-sheet-biden-harris-administration-outlines-coordinated-approach-to-harness-power-of-ai-for-u-s-national-security/)?

Ob Strategien weitergeführt werden oder wie diese ausgestaltet werden, wird der künftigen Bundesregierung obliegen.

16. Wie viele Finanzmittel hat die Bundesregierung 2024 sowie in ihrem Haushaltsentwurf 2025 für den Aufbau von Kompetenzen zur Erkennung und Abwehr von Deepfakes vorgesehen (bitte für 2024 und 2025 angeben, background.tagesspiegel.de/it-und-cybersicherheit/briefing/kriegsparteien-testen-deepfakes)?

Im Bundesministerium für Bildung und Forschung (BMBF) beträgt im Jahr 2024 die Summe der bewilligten Fördermittel mit unmittelbarem Bezug zur Erkennung von Deep Fakes 1 586 228,14 Mio. Euro. Am 19. Juli 2024 wurde die Förderrichtlinie „Vertrauen in Demokratie und Staat: Digitale Desinformation erkennen und abwehren“ durch das BMBF veröffentlicht. Hierfür sind Finanzmittel für 2025 vorbehaltlich der Haushalts-Aufstellung vorgesehen. Darüber hinaus haben die institutionell geförderten Cybersicherheitsforschungseinrichtungen wie Athene oder CISPA mit Bundesmitteln erhebliche Kompetenzen hierzu aufgebaut.

Seitens des Bundesministeriums für die Digitales und Verkehr (BMDV) sind bei der Bundesagentur für Sprunginnovationen SPRIND für den Funken „Deepfake Detection and Prevention" im Jahr 2024 6 243 870,50 Euro und im Jahr 2025 4 002 038 Euro vorgesehen.

17. Plant die Bundesregierung, digitale Souveränität als ein Vergabekriterium im Vergaberecht aufzunehmen (www.handelsblatt.com/politik/deutschland/wirtschaftspolitik-reform-des-vergaberechts-13-milliarden-euro-entlastung/100074745.html), um den Aufbau eines eigenen deutschen und europäischen Technologie-Ökosystems durch die Einkaufsmacht staatlicher Behörden zu stärken?

Die Bundesregierung erarbeitet ein „Vergabetransformationspaket“, mit dem der bisher strenge Grundsatz der Gleichbehandlung von Drittstaatsanbietern in Vergabeverfahren auch in Umsetzung der aktuellen Rechtsprechung des EuGH („Kolin“ – Rs. C-652/22) eingeschränkt wird. Neben den bereits bestehenden Möglichkeiten des Vergaberechts, bei öffentlichen Aufträgen Vorgaben zur Informations- und Cybersicherheit zu machen, würde dies die Möglichkeiten zur Gewährleistung der Digitalen Souveränität im Öffentlichen Auftragswesen zusätzlich erweitern.

18. Unterstützt die Bundesregierung das Anliegen der Digitalministerkonferenz, „auf europäischer Ebene auf eine Änderung des Vertrages über die Arbeitsweise der Europäischen Union derart hinzuwirken, dass in Artikel 346 des Vertrages die Cybersicherheit und Informationssicherheit mindestens aufgenommen wird“ (www.berlin-brandenburg.de/wp-content/uploads/TOP_9_NW_Beschluss_Leistungsbeschaffung_Info-_und-Cybersicherheit.pdf), und wenn ja, wie möchte die Bundesregierung das Ziel erreichen?

Das geltende Vergaberecht sieht bereits Möglichkeiten vor, die Informations- und Cybersicherheit betreffende Leistungen, die wesentliche Sicherheitsinteres-

sen berühren, vereinfacht oder beschleunigt zu beschaffen. Die Bundesregierung wird prüfen, inwieweit bei der anstehenden Überarbeitung der Europäischen Vergaberichtlinien in dieser Hinsicht zusätzliche Handlungsspielräume geschaffen werden müssen.

Eine Änderung des Artikels 346 AEUV ist aus Sicht der Bundesregierung zur Stärkung der Digitalen Souveränität nicht erforderlich. Zudem wären die juristischen Hürden für eine erforderliche Änderung des europäischen Primärrechts zur Umsetzung der von der Digitalministerkonferenz geforderten Aufnahme der „Cybersicherheit und Informationssicherheit“ sehr hoch.

19. Unterstützt die Bundesregierung beim Mobilfunkstandard 6G einen weltweit einheitlichen Standard, der ggf. eine Zusammenarbeit mit Huawei beinhaltet, oder unterstützt die Bundesregierung einen separaten Mobilfunkstandard, wie es vor 4G der Fall war (background.tagesspiegel.de/digitalisierung-und-ki/briefing/wie-die-geopolitik-6g-spalten-wird)?

Die Bundesregierung befürwortet die Etablierung eines weltweit einheitlichen Standards für 6G. Die Vorteile einer globalen Standardisierung sind dabei für Hersteller und Nutzer unstrittig, da Systemtechnik und Endgeräte weltweit und ohne technische Barrieren von jedem zu jeder Zeit und an jedem Ort genutzt werden können.

Die Mobilfunkstandardisierung wird spätestens seit 4G primär global erarbeitet und vorangetrieben; dies vorrangig in dem 1998 gegründeten 3rd Generation Partnership Project (3GPP). 3GPP besteht im Wesentlichen aus einer Partnerschaft zwischen verschiedenen Standardisierungsorganisationen (u. a. aus Europa, USA und China) auf der einen Seite und Unternehmen auf der anderen Seite. Behörden sind keine direkten Partner des 3GPP. 3GGP-Standards sind nicht rechtlich bindend. Ihnen kommt für Unternehmen jedoch faktische Bindungswirkung zu („Industriestandard“).

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