Deutscher Bundestag **Drucksache 21/5898**

21. Wahlperiode 11.05.2026

Kleine Anfrage

der Abgeordneten Dr. Anton Hofreiter, Dr. Sandra Detzer, Dr. Konstantin von Notz, Jeanne Dillschneider, Omid Nouripour, Chantal Kopf, Sara Nanni, Deborah Düring, Ayse Asar, Julian Joswig, Katrin Göring-Eckardt, Michael Kellner, Dr. Alaa Alhamwi, Victoria Broßart, Claudia Müller, Karl Bär und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Sicherheitsrisiken durch chinesische Technologien und Investitionen in der kritischen Infrastruktur Deutschlands

De-Risking steht zunehmend im Mittelpunkt der China-Debatte in Deutschland und der EU. Die Regierung unter SPD, BÜNDNIS 90/DIE GRÜNEN und FDP hatte im Juli 2023 erstmals eine nationale China-Strategie veröffentlicht. Darin wird die Bedeutung des De-Risking hervorgehoben, um Abhängigkeiten in kritischen Bereichen zu verringern; zudem werden entsprechende Maßnahmen der Risikominderung und Diversifizierung aufgeführt. In ihrem Koalitionsvertrag hat die Bundesregierung unter CDU/CSU und SPD festgehalten, die China-Strategie nach dem Prinzip des De-Risking zu überarbeiten und im Bundestag eine Expertinnen- und Expertenkommission einzusetzen, die in einem jährlichen Bericht Risiken, Abhängigkeiten und Vulnerabilitäten in den wirtschaftlichen Beziehungen analysiert, darstellt und Maßnahmen zum De-Risking empfiehlt.

De-Risking muss aus Sicht der Fragestellerinnen und Fragesteller neben wirtschaftlichen Aspekten maßgeblich auch die große sicherheitspolitische Dimension berücksichtigen. Im Rahmen der jährlich stattfindenden Anhörung des Parlamentarischen Kontrollgremiums (PKGr) warnen die Präsidentinnen und Präsidenten der Nachrichtendienste des Bundes regelmäßig vor den sicherheitspolitischen Gefahren, die von autoritären Staaten wie China für unsere Demokratie ausgehen (vgl. www.bundestag.de/presse/hib/kurzmeldungen-916626). Die massive Ausweitung staatlicher Kontrolle über chinesische Unternehmen ist vor diesem Hintergrund aus Sicht der Fragestellerinnen und Fragesteller besorgniserregend. Angesichts der in China geltenden, weitgehenden Kooperationsverpflichtungen mit staatlichen Stellen – etwa nach dem Nationalen Geheimdienstgesetz von 2017 (www.verfassungsschutz.de/SharedDocs/hintergruende/DE/praevention_wirtschafts-_und_wissenschaftsschutz/chinas-neue-wege-der-spionage.html) –, muss davon ausgegangen werden, dass jedes chinesische Unternehmen oder Produkt, welches in Deutschland tätig oder eingesetzt wird, ein potenzielles Sicherheitsrisiko darstellt.

Sicherheitsrisiken durch chinesische Produkte lassen sich in praktisch allen Sektoren kritischer Infrastruktur feststellen und machen diesen Bereich damit besonders verwundbar. Dabei ist die kritische Infrastruktur elementar wichtig für die Versorgungssicherheit Deutschlands. Eine vom Bundesministerium der Verteidigung in Auftrag gegebene Studie des Instituts für Verteidigung und Strategie (GIDS) weist beispielsweise auf eine Bandbreite an Sicherheitsrisiken

chinesischer Windkraftanlagen hin: Politische Einflussnahme, Spionage durch Sensorik, Zugang zu Sicherheitsprotokollen kritischer Infrastruktur und Störung der Energieversorgung seien ernst zu nehmende realistische Risiken (www.handelsblatt.com/unternehmen/energie/windraeder-aus-china-militaerexperten-warnen-vor-spionage/100109846.html).

Bei vernetzten Autos, die von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellt werden, bestehen ebenfalls große Sicherheitsrisiken. Ein geheimer Test der öffentlichen Verkehrsbetriebe in Norwegen ergab, dass etwa 850 im Land eingesetzte Elektrobusse vollständig aus China kontrolliert werden können (www.focus.de/panorama/welt/norweger-stellen-fest-dass-china-850-ih-rer-elektrobusse-fernsteuern-und-sogar-stoppen-kann_ba3c10a0-fa18-48a7-8f47-2670f49304c2.html). Israelische Verteidigungsstreitkräfte haben in den letzten Jahren 700 chinesische Autos zurückgerufen aufgrund der Befürchtung, dass die in den Fahrzeugen installierten Sensoren und Kameras dazu genutzt werden könnten, sensible Informationen zu sammeln (www.focus.de/politik/angst-vor-spionage-israelisches-militaer-entzieht-hochrangigen-offizieren-chinesische-autos335c4348-14a3-4478-b116-4f8bacc8e10e.html). In sicherheitsrelevanten Bereichen wie Bundeswehr, Polizei, kritische Infrastrukturen und das Regierungsumfeld stuft der Präsident des Thüringer Verfassungsschutzes, Stephan Kramer, das Risiko von vernetzten Autos als „hoch“ ein (www.handelsblatt.com/politik/deutschland/spionage-dobrindt-warnt-vor-risiken-vernetzter-autos-aus-china/100192429.html). Trotz dieser Sicherheitsbedenken werden – auch öffentliche – Aufträge immer wieder an chinesische Auftraggeber vergeben.

Auch ausländische Direktinvestitionen (FDI) aus China bergen spezifische sicherheitspolitische Risiken, die über rein wirtschaftliche Aspekte hinausgehen. Solche Investitionen sind nicht prinzipiell abzulehnen, gesetzt den Fall, sie generieren lokale Wertschöpfung, wie etwa die Schaffung von Arbeitsplätzen (https://merics.org/en/report/chinese-investment-rebounds-despite-growing-frictions-chinese-fdi-europe-2024-update). Die enge Verflechtung chinesischer Unternehmen mit staatlichen Interessen und die gesetzliche Verpflichtung zur Kooperation mit chinesischen Geheimdiensten werfen jedoch Fragen hinsichtlich Datensicherheit, Technologietransfer und potenzieller Spionage auf (www.gov.uk/government/publications/overseas-business-risk-china/overseas-business-risk-china). So könnten ausländische Unternehmen durch das „Foreign Investment Screening Mechanism“ und das „Counter-Espionage Law“ gezwungen werden, Daten oder Technologien herauszugeben. Der Präsident a. D. des unter anderem für die Spionageabwehr zuständigen Bundesamts für Verfassungsschutz (BfV), Thomas Haldenwang, verwies insbesondere auf das extrem strategische Vorgehen der Volksrepublik China beim Ein- bzw. Aufkauf von Teilen deutscher und europäischer Kritischer Infrastrukturen, die zum Teil offenkundig auch Spionagezwecken und der umfassenden Analyse von innereuropäischen und weltweiten Warenströmen dient (vgl. www.bundestag.de/presse/hib/kurzmeldungen-916626).

Diese Beispiele unterstreichen erneut die dringende Notwendigkeit eines strategisch geplanten De-Riskings, besonders im Bereich kritischer Infrastruktur. Im Gegensatz dazu weisen aktuelle Zahlen aus Sicht der Fragestellerinnen und Fragesteller jedoch auf einen gegenläufigen Trend in Deutschland hin. China ist im Jahr 2025 wieder der wichtigste Handelspartner Deutschlands und Importe aus China sind gestiegen – insbesondere bei Elektronik- und Informationstechnologien (www.destatis.de/DE/Presse/Pressemitteilungen/2026/02/PD26_056_51.html). Gleichzeitig verzeichnete FDI aus China nach Europa und UK im Jahr 2024 eine deutliche Steigerung auf 10 Mrd. Euro (+ 47 Prozent zu 2023), getrieben durch neue Greenfield-Investitionen, insbesondere in den Sektoren Elektrofahrzeuge und Batterietechnologie (https://merics.org/en/report/chinese-

investment-rebounds-despite-growing-frictions-chinese-fdi-europe-2024-update).

Die EU ist die treibende Kraft, wenn es darum geht, die Resilienz ihrer Mitgliedstaaten gegenüber China zu erhöhen. Im Oktober 2024 verabschiedete die EU den Cyber Resilience Act – die erste europäische Verordnung, die ein Mindestmaß an Cybersicherheit für alle vernetzten Produkte festlegt, die auf dem EU-Markt erhältlich sind (www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html). Ebenso schlägt die EU-Kommission im Rahmen des Industrial Accelerator Act (IAA), vor, FDI in strategischen Sektoren an strenge Bedingungen wie einen maximalen Auslandsanteil von 49 Prozent, Joint-Venture-Pflichten und verbindlichen Technologietransfer zu knüpfen (https://merics.org/en/report/chinese-investment-rebounds-despite-growing-frictions-chinese-fdi-europe-2024-update). Doch europäische Maßnahmen bleiben fragmentiert und unkoordiniert, und vielen EU-Mitgliedstaaten fehlt der politische Wille, Maßnahmen umzusetzen, geschweige denn proaktiv zu ergreifen (https://merics.org/de/studie/member-states-resilience-efforts-fall-short-looming-challenges-europe-china-resilience-audit).

Vor diesem Hintergrund wollen die Fragestellerinnen und Fragesteller von der Bundesregierung wissen, welche Kenntnisse sie über Sicherheitsrisiken verbunden mit chinesischen Produkten und Investitionen in deutscher kritischer Infrastruktur hat und welche nationalen und europäischen Maßnahmen sie ergreift und umsetzt, um die Resilienz unserer Gesellschaft angesichts stark gestiegener Bedrohungen zu stärken.

Wir fragen die Bundesregierung:

1. Verfügt die Bundesregierung über ein aggregiertes Lagebild über kritische Komponenten, die von chinesischen Herstellern und/oder in China hergestellt wurden, die in kritischer Infrastruktur gemäß der bisherigen Regelung BSI-KritisV in Deutschland verbaut sind?

   a) Falls ja, welche Daten und Erkenntnisse liegen der Bundesregierung vor (bitte aufschlüsseln nach Sektoren unter Angabe folgender Daten: Anteil, Kategorie der Komponenten, Name des Herstellers, Zeitpunkt des Einbaus, Risikobewertung)?

   b) Plant die Bundesregierung nach der Umsetzung der NIS II und CER-Richtlinie sowie der Vorlage entsprechender Umsetzungsgesetze bzw. noch vorzulegender Verordnungen und der damit einhergehenden Regelung, was zur kritischen Infrastruktur gehört, ein solches Lagebild zu erstellen und ein fortlaufendes systematisches Monitoring einzurichten?

2. Welche Erkenntnisse liegen der Bundesregierung über folgende Sicherheitsrisiken verbunden mit von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten und in deutschen Windparks installierten Turbinen vor

   a) Fernzugriffsmöglichkeiten durch chinesische Akteure,

   b) Datenabgriff und- Weitergabe an den chinesischen Staat,

   c) Weitere Sicherheitsrisiken?

3. Wie bewertet die Bundesregierung die Sicherheitsrisiken verbunden mit von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten und in deutschen Windparks installierten Turbinen?

4. Welche Schlussfolgerungen zieht die Bundesregierung für ihr Handeln auf nationaler und europäischer Ebene aus der vom Bundesministerium der Verteidigung in Auftrag gegebenen Studie des Instituts für Verteidigung und Strategie (GIDS) zu chinesischem Einfluss in nationaler Windkraftenergieinfrastruktur, in der es heißt, die Nutzung chinesischer Windkraftanlagen sei „zu verhindern“, falls Sicherheitsrisiken nicht ausgeschlossen werden können (www.handels-blatt.com/unternehmen/energie/windraeder-aus-china-militaerexperten-warnen-vor-spionage/100109846.html)?
5. Plant die Bundesregierung, die vom BMVg in Auftrag gegebenen GIDS-Studie zu chinesischem Einfluss in Windkraftenergieinfrastruktur zu veröffentlichen?
   a) Falls ja, wann?
   b) Falls nein, warum nicht?
6. Welche Schlussfolgerungen zieht die Bundesregierung aus dem vom Hamburger Vermögensverwalter Luxcara geplanten und schließlich verworfenen Aufbau von 16 Turbinen des chinesischen Produzenten Mingyang im Windpark Waterkant vor Borkum (www.handels-blatt.com/unternehmen/energie/windraeder-aus-china-militaerexperten-warnen-vor-spionage/100109846.html) vor dem Hintergrund möglicher Sicherheitsrisiken (z. B. Fernzugriff des Herstellers, Spionage durch Sensorik im Wasser, auf Boden und in der Luft) für zukünftige derartige Projekte, unter Berücksichtigung des zuletzt im KRITIS-Dachgesetz angepassten § 41 BSIG sowie unter Berücksichtigung der Tatsache, dass im Falle des Windparks Waterkant der im KRITIS-Dachgesetz festgelegte Schwellenwert von 500 000 betroffenen Personen nicht erreicht worden wäre (https://taz.de/Sicherheitsrisiken-bei-Erneuerba-ren/!6087416/)?
7. Welche Erkenntnisse liegen der Bundesregierung über folgende Sicherheitsrisiken verbunden mit von chinesischen Herstellern und/oder in China hergestellten und in deutschen Wind- und Solarparks installierten Wechselrichtern vor
   a) Fernzugriffsmöglichkeiten durch chinesische Akteure,
   b) Datenabgriff und- Weitergabe an den chinesischen Staat,
   c) Weitere Sicherheitsrisiken?
8. Wie bewertet die Bundesregierung die Sicherheitsrisiken verbunden mit von chinesischen Herstellern und/oder in China hergestellten und in deutschen Wind- und Solarparks installierten Wechselrichtern?
9. Welche Schlussfolgerungen zieht die Bundesregierung aus den Warnungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vor möglicher „Manipulation von Energieinfrastruktur“ bis hin zu gezielten Stromausfällen durch Cyberangriffe, auch über Wechselrichter (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Si-cherheit/Positionspapier_Cybersicherheit_Energiesek-tor.pdf?__blob=publicationFile&v=2) für ihr Handeln auf nationaler und/oder europäischer Ebene?
10. Wie bewertet die Bundesregierung die Tatsache, dass 78 Prozent der in Europa verbauten Solar-Wechselrichter aus China kommen, die Mehrheit davon produziert von Huawei, dessen Bauteile aufgrund von Sicherheitsbedenken derzeit aus den öffentlichen 5G-Mobilfunknetzen entfernt werden (https://api.solarpowereurope.org/uploads/SPE_2025_Soluti-ons_for_PV_Cyber_Risks_to_Grid_Stability_032dc2ae5a.pdf?up-dated_at=2025-04-29T07:11:32.315Z)?

11. Wie hoch ist nach Kenntnis der Bundesregierung der Marktanteil von Wechselrichtern, die von chinesischen Herstellern und/oder in China hergestellt werden (jeweils in Deutschland und in der EU), und wie hat sich dieser Marktanteil in den vergangenen fünf Jahren verändert?
12. Inwiefern zieht die Bundesregierung in Betracht, entsprechend des Vertrags mit Telekommunikationsunternehmen, auch mit Wind- und Solarparkbetreibern einen öffentlich-rechtlichen Vertrag über den Rückbau von Wechselrichtern chinesischer Hersteller zu schließen?
13. Welche Erkenntnisse liegen der Bundesregierung über folgende Sicherheitsrisiken verbunden mit von chinesischen Herstellern und/oder in China hergestellten und in Deutschland installierten Netztransformatoren vor?
    a) Fernzugriffsmöglichkeiten durch chinesische Akteure
    b) Datenabgriff und- Weitergabe an den chinesischen Staat
    c) Weitere Sicherheitsrisiken
14. Wie bewertet die Bundesregierung die Sicherheitsrisiken verbunden mit von chinesischen Herstellern und bzw. oder in China hergestellten und in Deutschland installierten Netztransformatoren?
15. Wie hoch ist nach Kenntnis der Bundesregierung der Marktanteil von Netztransformatoren, die von chinesischen Herstellern und/oder in China hergestellt werden (jeweils in Deutschland und in der EU), und wie hat sich dieser Marktanteil in den vergangenen fünf Jahren verändert?
16. Inwiefern zieht die Bundesregierung in Betracht, entsprechend des Vertrags mit Telekommunikationsunternehmen, auch mit Wind- und Solarparkbetreibern einen öffentlich-rechtlichen Vertrag über den Rückbau von Netztransformatoren chinesischer Hersteller zu schließen?
17. Gehören Wechselrichter und Netztransformatoren im Rahmen des EU Cyber Resilience Acts, der ab Ende 2027 höhere Sicherheitsstandards für vernetzte Geräte vorschreibt, zu der Kategorie „wichtige“ oder „kritische“ Produkte?

    Falls nein
    a) Hält die Bundesregierung es für sinnvoll, Wechselrichter und Netztransformatoren jeweils als „wichtiges“ oder „kritisches“ Produkt zu klassifizieren?
    b) Setzt sich die Bundesregierung auf EU-Ebene dafür ein, Wechselrichter und Netztransformatoren jeweils als „wichtiges“ oder „kritisches“ Produkt zu klassifizieren?
18. Wird die Bundesregierung vor dem Inkrafttreten des EU Cyber Resilience Acts Ende 2027 Maßnahmen ergreifen – die über die in der Verordnung vorgesehenen Zwischenmeilensteine hinausgehen –, um sicherzustellen, dass in Energieinfrastruktur verbaute chinesische Komponenten den europäischen Cybersicherheitsanforderungen entsprechen?
    a) Falls ja, welche Maßnahmen?
    b) Falls nein, warum nicht?
19. Wie bewertet die Bundesregierung die im EU Cyber Resilience Act festgelegte Zertifizierung von Produkten angesichts der Warnungen, dass eine Zertifizierung aufgrund ständig möglicher Softwareupdates wirkungslos sein könnte (www.welt.de/wirt-schaft/plus256128114/Gefahr-fuer-die-Net

zsicherheit-Wie-chinesische-Wechselrichter-unser-Stromsystem-beeinflussen-koennten.html)?

20. Wie bewertet die Bundesregierung den Vorschlag des BSI, nicht vertrauenswürdige Hersteller im Energiesektor aus dem europäischen Binnenmarkt auszuschließen (www.bsi.bund.de/SharedDocs/Down-loads/DE/BSI/Cyber-Sicherheit/Positionspapier_Cybersicherheit_Ener-giesektor.pdf?__blob=publicationFile&v=2)?

21. Welche Position hat die Bundesregierung in den Sitzungen der Horizontalen Ratsarbeitsgruppe „Fragen des Cyberraums“ zum Cybersecurity Package vertreten, die am 2. und 9. Februar 2026 sowie am 2. März 2026 stattfanden?

22. Unterstützt die Bundesregierung den Vorschlag der Kommission, im Rahmen des Cybersecurity Packages bzw. der Überarbeitung des Cyber Security Acts 2.0 eine Liste sogenannter „Hochrisiko“-Hersteller einzuführen, die vom Zugang zum europäischen Markt ausgeschlossen werden könnten?

    a) Falls ja, befürwortet die Bundesregierung, dass bestimmte chinesische Hersteller (z. B. Huawei) auf die Liste sogenannter „Hochrisiko“-Hersteller gesetzt werden?

    b) Falls nein, warum unterstützt die Bundesregierung den Vorschlag nicht?

23. Unterstützt die Bundesregierung den Vorschlag der Kommission, im Rahmen des Cybersecurity Packages bzw. der Überarbeitung des Cyber Security Acts 2.0, die EU Toolbox for 5G security verpflichtend umzusetzen?

24. Welche Kenntnis hat die Bundesregierung über den Anteil von Hochrisiko-Anbietern in kritischen Komponenten deutscher Mobilinfrastruktur 2025 im Vergleich zu den letzten fünf Jahren und geht die Bundesregierung davon aus, dass die Ausbaufrist für Hochrisikokomponenten bis 2029 im Mobilfunknetzwerk erfolgreich erreicht wird?

25. Wie stellt die Bundesregierung sicher, dass Fördermaßnahmen aus dem Infrastruktur-Sondervermögen nicht in den weiteren Verbau von Hochrisikokomponenten im Mobilfunknetz fließen?

26. Wie stellt die Bundesregierung sicher, dass bei der geplanten Ausrüstung der Bahnstrecken mit dem Future Railway Mobile Communication System (FRMCS) chinesische Hersteller wie Huawei vollständig ausgeschlossen werden, und wie ist der aktuelle Sachstand der Beratungen mit der DB InfraGO AG (in der Antwort des parlamentarischen Staatssekretärs Christian Hirte vom 14. Januar 2026 auf die Mündliche Frage 27 des Abgeordneten Matthias Gastel (BÜNDNIS 90/DIE GRÜNEN) wurde erklärt, dass im Rahmen dieser Beratungen derzeit Lösungswege beim Umgang mit hybriden Bedrohungslagen sowie den potenziellen Sicherheitsrisiken durch den Einsatz von Kommunikationskomponenten und Software aus Drittstaaten in kritischen Infrastrukturen erarbeitet werden, hier: Plenarprotokoll 21/52)?

27. Welche Erkenntnisse liegen der Bundesregierung über folgende Sicherheitsrisiken verbunden mit von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten und in Deutschland zugelassenen vernetzten Autos (Verbrenner, Elektro und hybrid) vor

    a) Fernzugriffsmöglichkeiten durch chinesische Akteure,

    b) Datenabgriff und- Weitergabe an den chinesischen Staat,

c) Weitere Sicherheitsrisiken?

28. Wie bewertet die Bundesregierung die Sicherheitsrisiken verbunden mit von chinesischen Herstellern, in China und bzw. oder mit chinesischer Software und/oder Hardware hergestellten und in Deutschland zugelassenen vernetzten Autos (Verbrenner, Elektro und hybrid)?

29. Welche Erkenntnisse ergaben sich aus dem gemeinsamen Projekt des Bundesamtes für Verfassungsschutz (BfV) und der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) (www.tagesschau.de/investigativ/ndr-wdr/chinesische-hersteller-sicherheitsbehoerden-100.html), bei dem Fahrzeuge mehrerer chinesischer Hersteller untersucht wurden und analysiert wurde, welche Daten die Autos sammeln, in welchem Umfang dies geschieht und ob Informationen ins Ausland fließen, und welche Schlussfolgerungen zieht die Bundesregierung dar-aus?

30. Welche Erkenntnisse ergaben sich aus dem BSI-Projekt zur Sicherheit von fahrzeuggenerierten Daten, bei dem fünf Fahrzeugmodelle, darunter drei Fahrzeuge von Nicht-EU-Herstellern untersucht werden (Antwort der Bundesregierung auf Bundestagsdrucksache 21/732 vom 1. Juli 2025 auf die Kleine Anfrage der Fraktion Die Linke auf Bundestagsdrucksache 21/70 zum Stand der Auswertung der China-Strategie der Bundesregierung, hier: Bundestagsdrucksache 21/732), und welche Schlussfolgerungen zieht die Bundesregierung daraus?

31. Verfügt die Bundesregierung über ein aggregiertes Lagebild über die Nutzung bzw. Präsenz der von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten und in Deutschland zugelassenen vernetzten Autos (Verbrenner, Elektro und hybrid) in Liegenschaften von Behörden und Einrichtungen der Bundesregierung und der Bundeswehr sowie in unmittelbarer Nähe von KRITIS-Anlagen und -Unternehmen?

a) Falls ja, welche Daten und Erkenntnisse liegen der Bundesregierung vor (bitte aufschlüsseln nach: Behörden und Einrichtungen der Bundesregierung, Bundeswehr und KRITIS-Anlagen und -Unternehmen)?

b) Falls nein, warum nicht?

32. Plant die Bundesregierung eine einheitliche, behördliche Regelung für von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten und in Deutschland zugelassenen vernetzten Autos (Verbrenner, Elektro und hybrid) in Liegenschaften von Behörden und Einrichtungen der Bundesregierung, der Bundeswehr sowie in KRITIS-Anlagen und -Unternehmen vor dem Hintergrund, dass die Zufahrt chinesischer Autos auf dem Parkplatz des Operatives Führungskommandos in Schwielowsee und auf den Liegenschaften des Bundesnachrichtendienstes laut Berichten bereits verboten ist (www.tagesschau.de/investigativ/ndr-wdr/chinesische-hersteller-sicherheitsbehoerden-100.html)?

33. Wie bewertet die Bundesregierung ein Verbot der von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten und in Deutschland zugelassenen vernetzten Autos (Verbrenner, Elektro und hybrid) in Liegenschaften von Behörden und Einrichtungen der Bundesregierung und der Bundeswehr sowie in der Nähe von KRITIS-Anlagen und -Unternehmen?

34. Wie bewertet die Bundesregierung die Entscheidung der Tochtergesellschaft der Deutschen Bahn, DB Regio, knapp 200 E-Busse des chinesischen Herstellers BYD bestellen zu wollen (www.merkur.de/wirt-schaft/w

irbel-um-china-busse-der-deutschen-bahn-so-nimmt-peking-die-deutsche-infrastruktur-ins-visier-zr-94101555.html)?

35. Werden bei der öffentlichen Ausschreibung und Vergabe von Gütern und Dienstleistungen, die Behörden und Einrichtungen der Bundesregierung, die Bundeswehr sowie KRITIS-Anlagen und -Unternehmen betreffen, sicherheitspolitische Faktoren berücksichtigt und/oder Risikoanalysen durchgeführt?

    a) Falls ja, welche konkreten sicherheitspolitischen Faktoren werden berücksichtigt und wie werden diese gegenüber anderen Kriterien wie Preis, Qualität und Nachhaltigkeit gewichtet?

    b) Falls nein, wie bewertet die Bundesregierung dies und sieht die Bundesregierung hier Handlungsbedarf auf nationaler und/oder europäischer Ebene?

36. Wie bewertet die Bundesregierung verbindliche vergaberechtliche EU-Regelungen, nach denen Bieter aus Drittstaaten, mit denen keine internationale Beschaffungsvereinbarung besteht, von Vergabeverfahren von Auftraggebern aus der EU ausgeschlossen werden?

37. Wie bewertet die Bundesregierung das zur Vermeidung von Umgehungen vorgesehene Erfordernis, auch indirekte Beteiligungen von Drittstaatsunternehmen an Vergabeverfahren auszuschließen?

38. Wie bewertet die Bundesregierung EU-Präferenzmaßnahmen zum Schutz sicherheitsrelevanter kritischer Infrastruktur sowie zur Stärkung der digitalen und technologischen Souveränität der EU, insbesondere beim Aufbau einer souveränen Cloud- und KI-Infrastruktur?

39. Wie bewertet die Bundesregierung die von der EU-Kommission geplante Heranziehung der Kommissionsempfehlung C(2023) 6689 von Oktober 2023 zu kritischen Technologiebereichen für die Wirtschaftssicherheit der EU (https://defence-industry-space.ec.europa.eu/document/download/67446b95-3992-461b-a02a-e9426d97626b_en?filename=C_2023_6689_1_DE_annexe_acte_auto-nome_part1_v2_0.pdf) als Grundlage für die Festlegung der Sektoren, die für eine EU-Präferenz in Frage kommen?

40. Erwägt die Bundesregierung, Mitarbeiterinnen und Mitarbeitern von Ministerien und/oder ihren nachgeordneten Behörden, Bundeswehrangehörigen und/oder Mitarbeiterinnen und Mitarbeitern von Unternehmen im Bereich der kritischen Infrastruktur aufzufordern, keine Diensthandys oder Computer mit chinesischen Fahrzeugen zu verbinden – wie teilweise in Großbritannien bereits geschehen (www.tagesschau.de/investigativ/ndr-wdr/chinesische-hersteller-sicherheitsbehoerden-100.html)?

41. Welche Erkenntnisse liegen der Bundesregierung über folgende Sicherheitsrisiken verbunden mit von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten Routern vor (hier: Router für den Verbrauchermarkt),

    a) Fernzugriffsmöglichkeiten durch chinesische Akteure,

    b) Datenabgriff und-Weitergabe an den chinesischen Staat,

    c) Weitere Sicherheitsrisiken?

42. Wie bewertet die Bundesregierung Sicherheitsrisiken verbunden mit von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten Routern?

43. Welche Schlussfolgerung zieht die Bundesregierung aus der Entscheidung der US-Telekommunikationsaufsicht, den Import von im Ausland herge-

stellten Routern für den Verbrauchermarkt zu untersagen (www.heise.de/news/USA-verbieten-alle-neuen-Router-fuer-Verbraucher-11222044.html)?

44. Verfügt die Bundesregierung über ein aggregiertes Lagebild über die Nutzung von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten Routern in Liegenschaften von Behörden und Einrichtungen der Bundesregierung, der Bundeswehr sowie in KRITIS-Anlagen und -Unternehmen?

    a) Falls ja, welche Daten und Erkenntnisse liegen der Bundesregierung vor (bitte aufschlüsseln nach: Behörden und Einrichtungen der Bundesregierung, Bundeswehr und in KRITIS-Anlagen und -Unternehmen)?

    b) Falls nein, warum nicht?

45. Plant die Bundesregierung eine einheitliche, behördliche Regelung für von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten Routern in Liegenschaften von Behörden und Einrichtungen der Bundesregierung, der Bundeswehr sowie in KRITIS-Anlagen und -Unternehmen?

46. Welche Erkenntnisse liegen der Bundesregierung über folgende Sicherheitsrisiken verbunden mit von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten Hafenkränen und sonstigen Logistikeinrichtungen (wie z. B. automatisierte Verlade- und Transportstraßen) vor

    a) Fernzugriffsmöglichkeiten durch chinesische Akteure,

    b) Datenabgriff und- Weitergabe an den chinesischen Staat,

    c) Weitere Sicherheitsrisiken?

47. Wie bewertet die Bundesregierung Sicherheitsrisiken verbunden mit von chinesischen Herstellern, in China und/oder mit chinesischer Software und bzw. oder Hardware hergestellten Hafenkränen und sonstigen Logistikeinrichtungen?

48. Welche Schlussfolgerungen zieht die Bundesregierung aus Warnungen von Experten, dass der hohe Automatisierungsgrad und die Fernwartungssysteme von Kränen und sonstigen Logistikeinrichtungen „ein leichtes Einfallstor für externe machtpolitische Manipulation“ seien (https://taz.de/Sicherheitsrisiken-bei-Erneu-erbaren/!6087416/) für ihr Handeln auf nationaler und europäischer Ebene?

49. Welche Schlussfolgerung zieht die Bundesregierung aus der Untersuchung des US-Repräsentantenhauses, bei der auf einigen in US-Häfen eingesetzten Kränen chinesischer Herkunft Kommunikationsgeräte gefunden wurden, dessen Einsatz in keinem Vertrag zwischen US-Häfen und dem chinesischen Staatsunternehmen Shanghai Zhenhua Heavy Industries Company (ZPMC) standen (https://edition.cnn.com/2024/03/07/politics/congressional-probe-communications-gear-chinese-cranes) für ihr Handeln auf nationaler und europäischer Ebene?

50. Wie hoch ist nach Kenntnis der Bundesregierung der Marktanteil von Hafenkränen und sonstigen Logistikeinrichtungen, die von chinesischen Herstellern, in China und bzw. oder mit chinesischer Software und/oder Hardware hergestellt werden (jeweils in Deutschland und in der EU), und wie hat sich dieser Marktanteil in den vergangenen fünf Jahren verändert?

51. Wie lautet der konkrete Zeitplan der Bundesregierung für die nationale Umsetzung der novellierten EU-FDI-Screening-Verordnung in das natio-

nale Recht, und wie stellt sie sicher, dass hierbei insbesondere die Prüfung von Investitionen durch in der EU ansässige Tochterunternehmen drittstaatlich kontrollierter Investoren (sogenannte „Xella-Lücke“) lückenlos verankert wird, um Umgehungstatbestände durch chinesische Staatskonzerne auf dem europäischen Binnenmarkt künftig wirksam zu unterbinden?

52. Zieht die Bundesregierung angesichts der zunehmenden Nutzung von Energie- und Transportinfrastruktur als geopolitische Waffe die Schaffung eines eigenständigen, modernen Investitionsprüfungsgesetzes (IPG) in Betracht, das die Investitionsprüfung aus dem Außenwirtschaftsgesetz (AWG) herauslöst, und inwiefern plant sie, in diesem Zuge die Prüfschwelle für systemische Abhängigkeiten im Bereich der Kritischen Infrastruktur (KRITIS) analog zu entsprechenden Forderungen auf 10 Prozent zu senken sowie atypische Kontrollerwerbe (z. B. durch Vetorechte oder Technologielizenzen) einer zwingenden vertieften Prüfung zu unterziehen?

53. Welche Schlussfolgerungen zieht die Bundesregierung aus der im Rahmen des EU Industrial Accelerator Acts (IAA) vorgesehenen FDI-Konditionierung – insbesondere der diskutierten 49-Prozent-Eigentumsobergrenze und Joint-Venture-Pflicht in strategischen Sektoren – für ihre eigene nationale Prüfpraxis, und wie begründet sie ordnungspolitisch, dass im deutschen Infrastruktursektor weiterhin Mehrheitsübernahmen durch staatlich gelenkte Akteure aus autoritären Staaten genehmigt werden, während auf EU-Ebene für die Neuproduktion strategischer Güter strikte Minderheitsgrenzen eingezogen werden sollen?

54. Inwiefern wird die Bundesregierung bei künftigen Übernahmen sicherstellen, dass die in der novellierten EU-FDI-Verordnung explizit genannten Risikofaktoren – wie die direkte oder indirekte Kontrolle eines Investors durch einen ausländischen Staat sowie der potenzielle Zugang zu sensiblen Daten – in Kombination mit wettbewerbsrechtlichen Bewertungen des Bundeskartellamts künftig strenger gewichtet werden, um den Ausverkauf kritischer Infrastruktur und eine neue asymmetrische Erpressbarkeit Deutschlands präventiv zu verhindern?

55. Verfügt die Bundesregierung über ein aggregiertes Lagebild über die Nutzung von chinesischen Herstellern, in China und/oder mit chinesischer Software und bzw. oder Hardware hergestellten Kleinstdrohnen in der Bundeswehr?

    a) Falls ja, welche Daten und Erkenntnisse liegen der Bundesregierung vor?

    b) Falls nein, warum nicht?

56. Plant die Bundesregierung eine einheitliche, behördliche Regelung für von chinesischen Herstellern, in China und/oder mit chinesischer Software und bzw. oder Hardware hergestellten Kleinstdrohnen in der Bundeswehr?

57. Bei welchen Vergabeprozessen von verteidigungs- und sicherheitsspezifischen Aufträgen im Rahmen von Beschaffungen der Bundeswehr wurde die Beteiligung von chinesischen (Unter-) Auftragnehmern verhindert?

58. Plant die Bundesregierung Maßnahmen, um bei der Beschaffung von Sicherheitsdraht durch die Bundeswehr eine Vergabe an chinesische

(Unter-) Auftragnehmer zu verhindern und eine europäische Lieferkette sicherzustellen?

Berlin, den 20. April 2026

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