Deutscher Bundestag **Drucksache 21/6433**

21. Wahlperiode 10.06.2026

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Anton Hofreiter, Dr. Sandra Detzer, Dr. Konstantin von Notz, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 21/5898 –

Sicherheitsrisiken durch chinesische Technologien und Investitionen in der kritischen Infrastruktur Deutschlands

Vorbemerkung der Fragesteller

De-Risking steht zunehmend im Mittelpunkt der China-Debatte in Deutschland und der EU. Die damalige Bundesregierung unter SPD, BÜNDNIS 90/DIE GRÜNEN und FDP hatte im Juli 2023 erstmals eine nationale China-Strategie veröffentlicht. Darin wird die Bedeutung des De-Riskings hervorgehoben, um Abhängigkeiten in kritischen Bereichen zu verringern; zudem werden entsprechende Maßnahmen der Risikominderung und Diversifizierung aufgeführt. In ihrem Koalitionsvertrag zwischen der CDU, CSU und SPD hat die Bundesregierung festgehalten, die China-Strategie nach dem Prinzip des De-Riskings zu überarbeiten und im Deutschen 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

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 10. Juni 2026 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

für die Versorgungssicherheit Deutschlands. Eine vom Bundesministerium der Verteidigung (BMVg) 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 verzeichneten FDI aus China nach Europa und dem Vereinigten Königreich (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.

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 der KRITIS (Kritische Infrastrukturen)-Rechtsverordnung (BSI-KritisV) in Deutschland verbaut sind?

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

Die Fragen1 und 1a werden gemeinsam beantwortet.

Der Bundesregierung liegt kein aggregiertes Lagebild im Sinne der Fragestellung vor.

   b) Plant die Bundesregierung nach der Umsetzung der NIS (Netz- und Informationssysteme)-2- und der CER (Critical Entities Resilience)-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?

Das Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz), welches die Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen umsetzt und erstmalig sektorübergreifende Mindestanforderungen für den physischen Schutz von kritischen Infrastrukturen festlegt, ist am 17. März 2026 in Kraft getreten. Eine Regelung zu kritischen Komponenten ist nicht enthalten. Die systematische Erfassung durch die Registrierung nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSIG) hat seit März 2026 begonnen. Hierdurch wird sukzessive eine Übersicht über kritische Komponenten nach BSIG entstehen.

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 Datenweitergabe 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?

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 Datenweitergabe 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?

10. Wie bewertet die Bundesregierung die Tatsache, dass 78 Prozent der in Europa verbauten Solarwechselrichter 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?

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 Datenweitergabe an den chinesischen Staat,

   c) weitere Sicherheitsrisiken?

14. Wie bewertet die Bundesregierung die Sicherheitsrisiken verbunden mit von chinesischen Herstellern und/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 dem Vertrag mit Telekommunikationsunternehmen auch mit Wind- und Solarparkbetreibern einen öffentlich-rechtlichen Vertrag über den Rückbau von Netztransformatoren chinesischer Hersteller zu schließen?

Die Fragen 2, 3, 7, 8, 10, 11, 13 bis 16 werden zusammen beantwortet:

Die Bundesregierung bewertet die Cybersicherheit und Resilienz vernetzter Energieanlagen als ein zunehmend relevantes Thema für die Sicherheit des Elektrizitätsversorgungssystems Deutschlands und Europas.

Vernetzte Energieanlagen und Netzbetriebsmittel, insbesondere Wechselrichter, Windenergieanlagen, Speicher, Ladeinfrastruktur, Wärmepumpen, Netztransformatoren sowie weitere digitalisierte Komponenten des Energiesystems, verfügen regelmäßig über Kommunikationsschnittstellen, Fernwartungsfunktionen und softwarebasierte Steuerungsmöglichkeiten. Teilweise erfolgt die Kommunikation über cloudbasierte Dienste oder IT-Systeme der Hersteller.

Ein koordinierter Zugriff auf große Mengen solcher Anlagen, die für sich genommen nicht die für die Einordnung als kritische Anlage maßgeblichen Schwellenwerte überschreiten, kann grundsätzlich Auswirkungen auf die Stabilität der Stromversorgung haben, insbesondere wenn große Mengen gleichartiger und zentral administrierbarer Komponenten betroffen sind.

Die Bundesregierung teilt die Einschätzung, dass mit der zunehmenden Digitalisierung und Vernetzung des Energiesystems erhebliche cybersicherheits- und wirtschaftssicherheitspolitische Risiken verbunden sind.

Dies betrifft neben Cyberrisiken im Sinne des Hackings auch strukturelle Risiken durch die Möglichkeit staatlicher Einflussnahme auf Hersteller vernetzter Energiekomponenten aus Drittstaaten.

In China bestehen weitreichende gesetzliche Verpflichtungen für Unternehmen und Privatpersonen zur Zusammenarbeit mit staatlichen Stellen, deren Bestehen den sicherheitspolitischen Interessen der Bundesrepublik Deutschland, der EU und der NATO zuwiderläuft. Es wird auf die Antwort der Bundesregierung auf die Frage 27b Bezug genommen. Digitale Plattform- und Wartungsstrukturen können dabei grundsätzlich Einflussmöglichkeiten auf Betrieb, Wartung und Aktualisierung entsprechender Systeme eröffnen.

Nach Kenntnis der Bundesregierung stammen erhebliche Teile der derzeit in Europa eingesetzten PV-Wechselrichter von Herstellern aus Drittstaaten, insbesondere China. Je nach Marktsegment und Bezugsgröße wird der Marktanteil chinesischer Hersteller in Europa auf etwa 70 bis 80 Prozent geschätzt. Gleichzeitig bestehen weiterhin europäische Produktionskapazitäten.

Die Analyse und Bewertung der Risiken vernetzter Energieanlagen sowie möglicher Gegenmaßnahmen sind derzeit Gegenstand eines ressortübergreifenden Arbeitsprozesses zwischen dem Bundesministerium für Wirtschaft und Energie (BMWE), dem Bundesministerium des Innern (BMI), der Bundesnetzagentur (BNetzA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Dabei fließen auch vorliegende Analysen, wie die des BSI zur Cybersicherheitslage im Energiesektor ein. Das BSI weist ausdrücklich auf Risiken durch digital vernetzte Energieanlagen, Lieferkettenabhängigkeiten, Manipulationsmöglichkeiten über Kommunikationsschnittstellen sowie staatlich unterstützte Cyberoperationen gegen Energieinfrastrukturen hin. Als Ergebnis der Risikoanalysen werden derzeit unterschiedliche technische und regulatorische Handlungsoptionen geprüft.

Auch auf europäischer Ebene wird die Thematik intensiv behandelt. Die Europäische Kommission führt beispielsweise zurzeit eine Risikobewertung zu den von vernetzten Energieanlagen ausgehenden Risiken durch und hat jüngst u. a.

die Europäische Investitionsbank angewiesen, zukünftig keine neuen Projekte mehr zu fördern, die Wechselrichter aus China, Russland, Iran und Nordkorea nutzen.

Zudem hat die Europäische Kommission einen Vorschlag für die Weiterentwicklung des Cyber Security Acts (CSA) vorgelegt, der auch die Risiken in der Lieferkette für kritische Komponenten in den Blick nimmt.

Die Bundesregierung befürwortet einen EU-weit stärker harmonisierten Umgang mit den Risiken von IT-Komponenten. Eine harmonisierte Regelung verhindert eine Zersplitterung des Binnenmarkts und schafft zugleich einen ausreichend großen Markt für sichere Produkte. Ebenso wird begrüßt, dass sich die Bewertung der Informations- und Kommunikationstechnik-Lieferkette (IKT-Lieferkette) nicht mehr ausschließlich auf technische Sicherheitsaspekte beschränken soll, sondern ausdrücklich auch nicht-technische Risikofaktoren – etwa die Rechtslage, geopolitische Faktoren oder organisatorische Abhängigkeiten – einbezogen werden sollen. Die Bundesregierung sieht dabei die Vorteile eines europäisch abgestimmten Vorgehens, auch wenn kompetenzrechtliche Fragen noch zu prüfen sind. Vor diesem Hintergrund wird die Bundesregierung auch die Verhandlungen zum CSA konstruktiv begleiten.

4. Welche Schlussfolgerungen zieht die Bundesregierung für ihr Handeln auf nationaler und europäischer Ebene aus der vom Bundesministerium der Verteidigung (BMVg) 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)?

Die Bundesregierung wird weiterhin prüfen, ob etwa beim Bau und Betrieb kritischer- oder verteidigungswichtiger Infrastruktur die Sicherheit bei der Landes- und Bündnisverteidigung gefährdet ist und bei Bedarf entsprechende Maßnahmen ergreifen.

5. Plant die Bundesregierung, die vom BMVg in Auftrag gegebenen GIDS-Studie zu chinesischem Einfluss in Windkraftenergieinfrastruktur zu veröffentlichen?

   a) Wenn ja, wann?

   b) Wenn nein, warum nicht?

Die Fragen 5 bis 5b werden gemeinsam beantwortet.

Eine Veröffentlichung ist nicht geplant. Die Studie diente lediglich als Beitrag zur internen Positionsbestimmung der Bundesregierung.

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 des BSI-Gesetzes (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/)?

Die Bundesregierung evaluiert die gesetzlichen Grundlagen zum Schutz kritischer- und verteidigungswichtiger Infrastruktur kontinuierlich und wird bei Bedarf eine Anpassung einbringen, um die Handlungsfähigkeit und -sicherheit des deutschen Staates und der deutschen Wirtschaft zu gewährleisten. Entsprechende Überlegungen bringt die Bundesregierung auch in Gesetzgebungsvorhaben auf EU-Ebene ein.

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?

Das BSI hat mit dem herausgegebenen Positionspapier das Ziel verfolgt, eine breitere Aufmerksamkeit auf die Problematik mit teilweise unregulierten Wechselrichtern zu lenken. Im Übrigen wird auf die Antwort zu Frage 2 verwiesen.

12. Inwiefern zieht die Bundesregierung in Betracht, entsprechend dem Vertrag mit Telekommunikationsunternehmen auch mit Wind- und Solarparkbetreibern einen öffentlich-rechtlichen Vertrag über den Rückbau von Wechselrichtern chinesischer Hersteller zu schließen?

Die Bundesregierung prüft derzeit, welche Handlungsoptionen auf der Grundlage des § 41 BSIG bezüglich der möglichen Untersagung des Einsatzes kritischer Komponenten für den Energiebereich bestehen.

17. Gehören Wechselrichter und Netztransformatoren im Rahmen des EU Cyber Resilience Act, der ab Ende 2027 höhere Sicherheitsstandards für vernetzte Geräte vorschreibt, zu der Kategorie „wichtige“ oder „kritische“ Produkte, und wenn nein,

   a) hält die Bundesregierung es für sinnvoll, Wechselrichter und Netztransformatoren jeweils als „wichtiges“ oder „kritisches“ Produkt zu klassifizieren, und

   b) setzt sich die Bundesregierung auf EU-Ebene dafür ein, Wechselrichter und Netztransformatoren jeweils als „wichtiges“ oder „kritisches“ Produkt zu klassifizieren?

Wechselrichter und Netztransformatoren sind als Endprodukt nicht in Anhang III und Anhang IV der Verordnung (EU) 2024/2847 gelistet. Die Bundesregie-

rung prüft fortwährend, ob Änderungen des Anhangs III und Anhang IV geboten sind und weitergehende Maßnahmen getroffen werden müssen. Dazu befindet sich die Bundesregierung im kontinuierlichen Austausch mit europäischen Partnern.

18. Wird die Bundesregierung vor dem Inkrafttreten des EU Cyber Resilience Act 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) Wenn ja, welche Maßnahmen?

    b) Wenn nein, warum nicht?

Die Fragen 18 bis 18b werden gemeinsam beantwortet.

Die Bundesregierung prüft fortwährend, ob Änderungen des CRA geboten sind und weitergehende Maßnahmen getroffen werden müssen. Die Bundesregierung prüft derzeit, welche Handlungsoptionen auf der Grundlage des § 41 BSIG bezüglich der möglichen Untersagung des Einsatzes kritischer Komponenten für den Energiebereich bestehen.

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

Die Verordnung (EU) 2024/2847 legt fest, dass je nach Klassifikation des jeweiligen Produktes mit digitalen Elementen eine Konformitätsbewertung durch eine notifizierte Stelle beispielsweiseeine Zertifizierung verpflichtend wird. Handelt es sich bei einem Softwareupdate um eine wesentliche Änderung, ist eine neue Konformitätsbewertung erforderlich. Des Weiteren ist ein Hersteller dazu verpflichtet, etwaige Schwachstellen innerhalb des Unterstützungszeitraums zu schließen. Eine Zertifizierung wird als sinnvolles Konformitätsbewertungsverfahren angesehen, um die Konformität eines Produktes zum CRA und damit ein erhöhtes Maß an IT-Sicherheit zu bestätigen.

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)?

Es wird auf die Antwort der Bundesregierung zu Frage 17 verwiesen.

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 Package bzw. der Überarbeitung des Cyber Security Act 2.0 eine Liste sogenannter „Hochrisiko“-Hersteller einzuführen, die vom Zugang zum europäischen Markt ausgeschlossen werden könnten?

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

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

Die Fragen 21 bis 22b werden gemeinsam beantwortet.

Die Bundesregierung erkennt die Bedrohungen durch nicht vertrauenswürdige Anbieter und Drittstaaten sowie die Notwendigkeit schnellen Handelns an. Die Bundesregierung nimmt die Bemühungen zur Kenntnis, dieses Problem im Rahmen des CSA 2.0 anzugehen, und prüft derzeit die Vorschläge.

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

Die internen Abstimmungen innerhalb der Bundesregierung zu diesem Vorschlag der EU-Kommission laufen aktuell noch.

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?

Der Bundesregierung liegen Erkenntnisse vor, wonach in den 5G-Mobilfunknetzen der drei größten in Deutschland tätigen Mobilfunkbetreiber eine hohe Durchdringung mit kritischen Komponenten des chinesischen Herstellers Huawei besteht. Den diesbezüglich bestehenden erheblichen Abhängigkeiten wurde mit dem Abschluss der öffentlich-rechtlichen Verträge mit den Mobilfunkbetreibern und den daraus resultierenden Verpflichtungen zum Ausbau der kritischen Komponenten wirksam begegnet. Die Bundesregierung geht davon aus, dass die mit den Mobilfunkbetreibern vereinbarte Ausbaufrist der als kritisch identifizierten Komponenten aus den jeweiligen Teilen des 5G-Mobilfunknetzes entsprechend umgesetzt wird.

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

Die Bewilligungsphase des Mobilfunkförderprogramms der Bundesregierung ist Ende 2024 ausgelaufen, weitere Projekte werden nicht gefördert. Zuwendungsempfänger sind die sog. Tower-Companies, die die passiven Infrastrukturen errichten.

Hierbei kommen keine kritischen Komponenten zum Einsatz. Die Mobilfunknetzbetreiber errichten die aktive Technik eigenwirtschaftlich und unterliegen daher keinen gesonderten Auflagen durch die Mobilfunkförderung. Es gelten

daher die im eigenwirtschaftlichen Ausbau relevanten gesetzlichen und regulatorischen Regelungen, Vorgaben und unternehmensstrategischen Erwägungen.

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, Plenarprotokoll 21/52)?

Es wird auf die Antwort der Bundesregierung auf das Plenarprotokoll 21/52 der 52. Sitzung vom 14. Januar auf die Antwort der Frage 27 verwiesen. Die ressortübergreifenden Abstimmungsprozesse innerhalb der Bundesregierung werden fortgeführt.

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,

Vernetzte Kraftfahrzeuge besitzen externe Schnittstellen, die Fernzugriffe ermöglichen. Über diese kann auf Daten und Ressourcen des Kraftfahrzeuges zugegriffen werden. Für die Aktualisierung von Fahrzeugkomponenten und deren Software sind diese erforderlich. Technisch besteht das Risiko, dass solche Schnittstellen z. B. durch Dritte auch missbraucht werden. Möglichkeiten des Missbrauchs können durch IT-Sicherheitsvorschriften reduziert werden. Im Rahmen der Typgenehmigung werden daher in Deutschland hierfür die UN-Regelung Nr. 155 und UN-Regelung Nr. 156 angewendet. Kraftfahrzeughersteller ermöglichen sich grundsätzlich Zugriff auf Schnittstellen im Kraftfahrzeug. Eine Möglichkeit, den Fernzugriff rechtlich ausschließlich für bestimmte Hersteller zu verbieten, besteht zurzeit nicht, würde indes auch das IT-Komponenten stets immanente Restrisiko eines missbräuchlichen Zugriffs nicht ausschließen können.

Die Typgenehmigung und Marktüberwachung von Kraftfahrzeugen für den deutschen Markt ist herstellerübergreifend geregelt. Im Übrigen wird auf die gemeinsame Beantwortung der Fragen 2, 3, 7, 8, 10, 11, 13 bis 16 verwiesen.

b) Datenabgriff und Weitergabe an den chinesischen Staat,

Vernetzte Fahrzeuge erfassen Daten. Technisch besteht die Möglichkeit, dass solche Daten abgegriffen und an Dritte weitergegeben werden. Die chinesische Gesetzgebung verpflichtet Unternehmen und Privatpersonen mit staatlichen chinesischen Stellen, einschließlich der chinesischen Regierung und ihren Nachrichtendiensten, zusammenzuarbeiten und gewährt staatlichen chinesischen Stellen weitereichende Einsicht in ihre IT-Systeme. Es können durch vernetzte Fahrzeuge gesammelte und generierte Daten an staatliche chinesische

Stellen abfließen. Im Übrigen wird auf die gemeinsame Beantwortung der Fragen 2, 3, 7, 8, 10, 11, 13 bis 16 verwiesen.

c) weitere Sicherheitsrisiken?

Angriffsflächen vernetzter Kraftfahrzeuge entstehen beispielsweise durch Anbindungen an externe Netzwerke. IT-Angriffe können Datenverlust, Fahrzeugmanipulation oder Betriebsstörungen verursachen. Hersteller behalten bei modernen Kraftfahrzeugarchitekturen teilweise Fernkontrolle über bestimmte Kernfunktionen. Sensorik von vernetzten Kraftfahrzeugen (Kameras, Mikrofone) kann zur Ausspähung genutzt werden. Eine Möglichkeit, diese Sicherheitsrisiken gezielt für bestimmte Hersteller auszuschließen, besteht zurzeit nicht. Die Typgenehmigung und Marktüberwachung von Kraftfahrzeugen für den deutschen Markt sind herstellerübergreifend geregelt. Im Übrigen wird auf die gemeinsame Beantwortung der Fragen 2, 3, 7, 8, 10, 11, 13 bis 16 verwiesen.

28. Wie bewertet die Bundesregierung die 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)?

Der Betrieb vernetzter Fahrzeuge erzeugt, insbesondere bei nicht ordnungsgemäßer Verwendung, grundsätzlich bestimmte IT-Risiken. Bei chinesischen Fahrzeugen besteht die Möglichkeit der staatlichen Einflussnahme. (siehe insb. zur chinesischen Rechtslage die gemeinsame Beantwortung der Fragen 2, 3, 7, 8, 10, 11, 13 bis 16). Sicherheitsrisiken wie etwa die staatliche Einflussnahme auf einen Hersteller, z. B. über dementsprechende rechtliche Vorschriften aber auch rein politischer Art, können mit technischen Mitteln nicht ausgeschlossen werden. Die Typgenehmigung und Marktüberwachung von Kraftfahrzeugen für den deutschen Markt sind herstellerübergreifend geregelt.

Ein entsprechender Gesamtüberblick über einige Sicherheitsrisiken vernetzter Fahrzeuge wurde in der europäischen und in der nationalen Risikoanalyse erarbeitet.

Das europäische Dokument ist öffentlich verfügbar (https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security). Eine nationale Risikoanalyse wird derzeit durch die Bundesregierung erarbeitet. Konkrete Vorfälle sind der Bundesregierung nicht bekannt. Bei Fahrzeugen mit E-Ladeschnittstellen ergeben sich potentiell weitere Risiken, s. a. www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/2026/Sicherheit_oeffentliche_Ladeinfrastruktur_260507.html

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 daraus?

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage aufgrund entgegenstehender überwiegender Belange des Staatswohls nicht erfolgen kann, auch nicht in eingestufter Form. Aufklärungsprofile der Sicherheitsbehörden des Bundes, sind – auch im Hinblick auf deren künftige Aufgabenerfüllung – besonders schutzbedürftig.

Durch die Beantwortung derartig gelagerter Fragen könnten Rückschlüsse auf den Aufklärungsbedarf, den Erkenntnisstand sowie die generelle Arbeitsweise der Sicherheitsbehörden gezogen werden. Eine Veröffentlichung der in Rede stehenden Informationen würde den Kenntnisstand und die Arbeitsweise sowie die Aufklärungsaktivitäten und Analysemethoden der Sicherheitsbehörden offenlegen. Dies würde deren Funktionsfähigkeit nachhaltig beeinträchtigen und damit einen Nachteil für die Interessen der Bundesrepublik Deutschland bedeuten.

Nach sorgfältiger Abwägung der Informationsrechte des Deutschen Bundestags und seiner Abgeordneten mit den negativen Folgen für die künftige Arbeitsfähigkeit und Aufgabenerfüllung der Sicherheitsbehörden sowie den daraus resultierenden Beeinträchtigungen der Sicherheit der Bundesrepublik Deutschland folgt, dass auch eine Auskunft nach Maßgabe der Geheimschutzordnung und damit einhergehende Einsichtnahme über die Geheimschutzstelle des Deutschen Bundestages ausscheidet. Eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern wird dem Schutzbedarf nicht gerecht. Dies gilt umso mehr, als bei einem Bekanntwerden die betroffenen nachrichtendienstlichen Methoden und Werkzeuge nur noch eingeschränkt oder gar nicht mehr eingesetzt werden können. Hieraus ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsinteresse überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber den Geheimhaltungsinteressen der Bundesregierung zurückstehen.

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 die Kleine Anfrage auf Bundestagsdrucksache 21/732), und welche Schlussfolgerungen zieht die Bundesregierung daraus?

Das BSI hat im Jahr 2025 ein Projekt zur IT-Sicherheit fahrzeuggenerierter Daten durchgeführt. Ziel des Projekts war es, einen Gesamtüberblick über den aktuellen Sachstand zur Generierung, Speicherung und Übertragung von Daten im Fahrzeug zu erhalten. Unter anderem sammelt dieses Fahrzeug folgende Informationen: Daten zum Fahrverhalten (z. B. Geschwindigkeit, Bremsverhalten, Lenkwinkel). Die stichprobenartige Prüfung im genannten Projekt zeigt den großen Umfang an Fahrzeugnutzungsdaten, auf den die Fahrzeughersteller Zugriff haben. Unter anderem sammelten die untersuchten Fahrzeuge Daten zum Fahrverhalten, Standortdaten und Daten zum Fahrzeugstatus sowie Nutzungsdaten. Für ein umfassendes Bild hinsichtlich des Datensendeverhaltens und der sich ergebenden Gefährdungen sind fortlaufende Prüfungen von Fahrzeugen notwendig und weitere Ressourcen erforderlich.

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 KRITIS-Unternehmen?

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

b) Wenn nein, warum nicht?

Die Fragen 31 bis 31b werden gemeinsam beantwortet.

Es liegt kein 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 vor.

In den Fuhrparks der einzelnen Bundesministerien einschließlich des nachgeordneten Bereichs sowie der Bundeswehr befinden sich keine Kraftfahrzeuge chinesischer Hersteller im Einsatz.

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 KRITIS-Unternehmen, vor dem Hintergrund, dass die Zufahrt chinesischer Autos auf dem Parkplatz des Operativen 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)?

Die Bundesregierung hat bisher keine grundsätzliche Regelung in Bezug auf die o. g. Fahrzeuge und die Zufahrt zu den einzelnen Liegenschaften erlassen. Die Bundesregierung arbeitet kontinuierlich daran, die Resilienz der einzelnen Liegenschaften zu stärken, um auf aktuelle Bedrohungsszenarien reagieren zu können. Das KRITIS-Dachgesetz sieht für die in § 2 Nummer 10 KRITIS-Dachgesetz genannten Einrichtungen der Bundesverwaltung neben den Betreibern kritischer Anlagen ebenso Mindestanforderungen zur Stärkung der Resilienz vor. Eine Rechtsverordnung mit sektorenübergreifenden Mindestanforderungen wird dazu derzeit erarbeitet. Die passgenauen Maßnahmen für die einzelnen Einrichtungen der Bundesverwaltung sollen auf Grundlage der eigenen Risikoanalysen und Risikobewertungen erfolgen.

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 KRITIS-Unternehmen?

Es wird auf die Antwort der Bundesregierung zu Frage 32 verwiesen.

34. Wie bewertet die Bundesregierung die Entscheidung der Tochtergesellschaft der Deutschen Bahn AG, DB Regio, knapp 200 E-Busse des chinesischen Herstellers BYD bestellen zu wollen (www.merkur.de/wirtschaft/wirbel-um-china-busse-der-deutschen-bahn-so-nimmt-peking-die-deutsche-infrastruktur-ins-visier-zr-94101555.html)?

Die Bundesregierung weist darauf hin, dass es sich bei der Deutschen Bahn AG (DB AG) um ein privatrechtlich organisiertes Unternehmen handelt, dessen Vorstand das Unternehmen gemäß § 76 Absatz 1 Aktiengesetz (AktG) eigen-

verantwortlich führt und eigenständig über operative Entscheidungen wie Fahrzeugbeschaffungen entscheidet.

Die Beschaffung der Busse erfolgte im Rahmen einer europaweiten Ausschreibung zur Modernisierung und Elektrifizierung der Flotte. Hauptlieferant ist ein deutscher Hersteller, während der Beitrag des chinesischen Herstellers BYD mit rund fünf Prozent der Fahrzeuge vergleichsweise gering ist und aus europäischer Produktion stammt. Zudem erfüllen die Busse alle geltenden Zulassungs- und Sicherheitsanforderungen, einschließlich der einschlägigen Normen zur Cyber- und Softwaresicherheit. Nach Angaben der DB AG wurden ausschließlich Anbieter berücksichtigt, deren Fahrzeuge keine zusätzliche Hard- oder Software enthalten, die eigenständig Daten senden oder empfangen kann, sodass die Datenhoheit gewahrt bleibt und unautorisierte Datenübertragungen ausgeschlossen werden.

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

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

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

Die Fragen 35 bis 35b werden gemeinsam beantwortet.

Die sicherheitspolitischen Anforderungen an den konkreten Auftragsgegenstand werden von der vergebenden Stelle bestimmt. Dabei berücksichtigt die Bundesregierung bei der Beschaffung möglicherweise als sicherheitsrelevant eingestufter Güter die im nationalen und europäischen (Vergabe-)Recht zur Verfügung stehenden Möglichkeiten, um höchstmögliche Sicherheit zu erreichen.

Dazu zählen beispielsweise die Möglichkeit der Geheimhaltungseinstufung nach § 4 des Sicherheitsüberprüfungsgesetzes oder des Verschlusssachenauftrags nach § 104 Absatz 3 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB). Auch die Losaufteilung bzw. die Los-/ und Zuschlagslimitierung können als Instrument genutzt werden, um einer Monopolstellung oder einer Abhängigkeit von einzelnen Unternehmen entgegenzuwirken. Ebenso bietet die Ausgestaltung von Verträgen die Möglichkeit, den Sicherheitsanforderungen gerecht zu werden. Ferner steht es im Ermessen der einzelnen Auftraggeber, Unternehmen aus Drittstaaten, die mit der EU keine internationale Übereinkunft über den Zugang zu öffentlichen Aufträgen abgeschlossen haben, zuzulassen, eine Bewertungsanpassung vorzunehmen oder diese auszuschließen.

Die Bundeswehr berücksichtigt im Vorlauf von Vergabeverfahren und Vertragsgestaltung sicherheitspolitische Faktoren in Form von Eignungs- und Resilienzkriterien. Im Rahmen dieser Prüfungen finden auch Risikoanalysen statt.

Das KRITIS-Dachgesetz sieht in § 11 Nationale Risikobewertungen und Risikoanalysen für die kritischen Dienstleistungen vor.

Für die einzelnen kritischen Dienstleistungen werden nationale Risikobewertungen durchgeführt, um einen Gesamtüberblick über die Gefahren und gegenseitigen Abhängigkeiten für KRITIS in Deutschland zu erhalten. Diese bilden die Grundlage für spezifische Risikoanalysen und Risikobewertungen der Be-

treiber. Hierbei verfolgt das KRITIS-Dachgesetz einen breiten Ansatz: Es geht um alle denkbaren Risiken, die durch die Natur oder den Menschen verursacht werden können – den sogenannten „All-Gefahren-Ansatz“. Spezielle Regelungen zu öffentlichen Ausschreibungen und zu Vergabeverfahren enthält das KRITIS-Dachgesetz nicht.

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?

Aus Sicht der Bundesregierung können solche Regelungen nur in Ausnahmefällen notwendig sein. Dabei muss eine praktikable und bürokratiearme Ausgestaltung sichergestellt sein.

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

Nach der Vergabestatistik war der Anteil an Auftragnehmern mit Sitz in Drittstaaten in den letzten Jahren sehr gering. Sofern der Ausschluss von Bietern aus Drittstaaten für ein Vergabeverfahren als sinnvoll erachtet wird, kann es daher im Einzelfall geboten sein, den Ausschluss auch auf indirekte Beteiligungen zu erstrecken. Der Nutzen sollte dabei mit dem Aufwand abgewogen werden, den die Überprüfung der Eigentümer- und Kontrollstrukturen mit sich bringt.

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?

Hinsichtlich der Stärkung der digitalen Souveränität der EU, insbesondere beim Ausbau einer souveränen Cloud- und KI-Infrastruktur, erwartet die Bundesregierung den angekündigten Vorschlag der Europäischen Kommission für einen EU-Cloud and AI Development Act (CADA). Die Bundesregierung wird darin enthaltene Maßnahmen bewerten, sobald der Vorschlag vorliegt.

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 infrage kommen?

Die Bundesregierung begrüßt, dass die EU-Kommission eine Stärkung der EU im Bereich kritischer Technologien anstrebt. Die Liste unter der EU-Wirtschaftssicherheitsstrategie deckt wichtige Technologiebereiche ab und ist unter anderem Grundlage für laufende Risikoanalysen. Wirtschaftspolitische Maßnahmen, einschließlich möglicher Präferenzmaßnahmen, müssen bedarfsgerecht und verhältnismäßig ausgestaltet sein. Das kann auch einen präzisen Zuschnitt der erfassten Technologien erfordern.

40. Erwägt die Bundesregierung, Mitarbeiterinnen und Mitarbeiter von Bundesministerien und/oder ihren nachgeordneten Behörden, Bundeswehrangehörige und/oder Mitarbeiterinnen und Mitarbeiter 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)?

Für die Bundesverwaltung gelten insb. die Vorgaben der BSI-Standards 200-1 – 200-3, der BSI-Mindeststandards und der Technischen Richtlinien des BSI für die Bundesverwaltung zwecks Gewährleistung eines angemessenen und wirksamen Informationssicherheitsmanagements nach BSI IT-Grundschutz. Diese sind von den Behörden auf deren IT-Betriebsumgebung anzuwenden, eigenverantwortlich umzusetzen und aufrechtzuerhalten. Hierzu gehört insbesondere auch eine entsprechende IT-Risikoanalyse und -behandlung (siehe insb. BSI-Standard 200-3) unter Beachtung von vorliegenden konkreten Warnungen und Handlungsempfehlungen (z. B. zu Verschlüsselung) des BSI/CISO Bund zu z. B. bekannten Sicherheitslücken und -Risiken. Das KRITIS-Dachgesetz sieht für die Einrichtungen der Bundesverwaltung neben den Betreibern kritischer Anlagen ebenso Mindestanforderungen zur Stärkung der Resilienz vor. Eine Rechtsverordnung mit sektorenübergreifenden Mindestanforderungen wird dazu derzeit erarbeitet. Die passgenauen Maßnahmen für jeden einzelnen KRITIS-Betreiber und jede Einrichtung der Bundesverwaltung sollen auf Grundlage der eigenen Risikoanalysen und Risikobewertungen erfolgen.

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?

Fernzugriffe, Datenabflüsse und andere Sicherheitsrisiken können grundsätzlich nicht ausgeschlossen werden, unabhängig von Hersteller oder Land. Zur Minimierung der Angriffsfläche sollten ungenutzte Schnittstellen und Services immer deaktiviert werden. Konkrete Erkenntnisse zu Fernzugriffen aus oder Datenabflüssen nach CHN bezüglich für den Verbrauchermarkt hergestellter Router liegen der Bundesregierung nicht vor. Im Übrigen wird auf die gemeinsame Beantwortung der Fragen 2, 3, 7, 8, 10, 11, 13 bis 16 verwiesen.

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

In Einzelfällen (u. a. auch bei Geräten aus CHN) konnten Schwachstellen aufgedeckt werden. Diese wurden dem jeweiligen Hersteller gemeldet und durch diesen geschlossen.

43. Welche Schlussfolgerung zieht die Bundesregierung aus der Entscheidung der US-Telekommunikationsaufsicht, den Import von im Ausland hergestellten Routern für den Verbrauchermarkt zu untersagen (www.heise.de/news/USA-verbieten-alle-neuen-Router-fuer-Verbraucher-11222044.html)?

Die Bundesregierung verfolgt aufmerksam die Entscheidung der US-Telekommunikationsaufsicht. Mit der Verordnung (EU) 2024/2847 (Cyber Resilience Act) werden erstmals verpflichtende Cybersicherheitsanforderungen für das Inverkehrbringen auf den EU-Binnenmarkt auch von Routern formuliert. Router für den Verbrauchermarkt werden hierzu als wichtige Produkte klassifiziert. Neben nationalen und internationalen Vorgaben für die Routersicherheit (BSI TR-03148 und ETSI TS 103 848), gestaltet das BSI auf EU-Ebene verpflichtende Standards im Rahmen des Cyber Resilience Act (CRA) mit, deren Umsetzung für einen Marktzugang Voraussetzung sind; darunter auch ein Standard für Router, Modems und Switches (ETSI EN 304 627, derzeit im Entwurfsstatus). Über Marktaufsichtsmechanismen kann der Import von nicht konformen Produkten verhindert werden. Die Bundesregierung bewertet kontinuierlich, inwieweit beim CRA ein Anpassungsbedarf besteht.

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 KRITIS-Unternehmen?

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

    b) Wenn nein, warum nicht?

Die Fragen 44 bis 44b werden gemeinsam beantwortet.

Die Bundesregierung verfügt über kein aggregiertes Lagebild im Sinne der Fragestellung. Die Bundesregierung beachtet bei der Beschaffung von sicherheitsrelevanter IT die geltenden Vorgaben und Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) und weiterer sicherheitsrelevanter Regelungen. Aggregierte Lagebilder im Sinne der Fragestellung werden nicht erhoben.

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 KRITIS-Unternehmen?

Für die Bundesverwaltung gelten insb. die Vorgaben der BSI-Standards 200-1 – 200-3, der BSI-Mindeststandards und der Technischen Richtlinien des BSI für die Bundesverwaltung zwecks Gewährleistung eines angemessenen und wirksamen Informationssicherheitsmanagements nach BSI IT-Grundschutz. Diese sind von den Behörden auf deren IT-Betriebsumgebung anzuwenden, eigenverantwortlich umzusetzen und aufrechtzuerhalten. Hierzu gehört insbesondere auch eine entsprechende IT-Risikoanalyse und -behandlung (siehe insb. BSI-Standard 200-3) unter Beachtung von vorliegenden konkreten Warnungen und Handlungsempfehlungen (z. B. zu Verschlüsselung) des BSI/CISO Bund zu z. B. bekannten Sicherheitslücken und -Risiken. Für die Bundesverwaltung

stehen verschiedene durch BSI zertifizierte, zugelassene oder einsatzempfohlene IT-Produkte zu Verfügung, deren Sicherheitseigenschaften im Rahmen eines entsprechenden Prüfprozesses verifiziert wurden. Zum Einsatz der sicheren zentralen mobilen Lösungen und dem Anschluss an die sicheren Regierungsnetze bestehen zudem konkrete Nutzungs- und Einsatzbedingungen, die ein hohes Sicherheitsniveau gewährleisten.

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 Datenweitergabe an den chinesischen Staat,

    c) weitere Sicherheitsrisiken?

Im Allgemeinen wird auf die gemeinsame Beantwortung der Fragen 2, 3, 7, 8, 10, 11, 13 bis 16 verwiesen.

Ein wesentlicher Bestandteil moderner Hafeninfrastruktur sind große Containerkräne, mit denen Containerschiffe be- und entladen werden.

Ein Abhängigkeitsverhältnis von einem einzelnen chinesischen Hersteller ist nicht nur aus wirtschaftlicher Sicht problematisch, sondern stellt auch ein Sicherheitsrisiko dar. So wurde im März 2023 bekannt, dass die US-Regierung China verdächtigt, die Hafenkräne von ZPMC für Spionagezwecke zu nutzen. Die darin verbaute Technik enthalte neben Sensoren, die den Laufweg von Containern und weitere Informationen dokumentieren, auch Modems, die nicht für den alltäglichen Betrieb notwendig seien. Dadurch könnten auch sicherheitsrelevante Informationen abgefangen werden, etwa über militärische Transporte. Zudem bestehe das Risiko, dass China die Kräne im Extremfall abschalten und dadurch Hafeninfrastruktur lahmlegen könne, da die Steuerungssoftware ebenfalls aus China stamme.

Diese Verdächtigungen wurden im September 2024 durch einen Bericht eines Untersuchungsausschusses des US-Kongresses weiter erhärtet. In diesem Bericht wird u. a. dargelegt, dass ZPMC mehrere US-Hafenbetreiber unter Druck gesetzt habe, einen Fernzugriff auf die Containerkräne zu erlauben, was viele auch zuließen.

Auch hiesige Unternehmen sind anfällig für Cyberangriffe. Diese Sicherheitslücken könnten durch andere staatliche und nichtstaatliche Akteure ausgenutzt werden. Gerade kleine und mittlere Unternehmen sollten diesbezüglich einen deutlich stärkeren Fokus auf das Thema Cybersicherheit legen.

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

Im Allgemeinen wird auf die gemeinsame Beantwortung der Fragen 2, 3, 7, 8, 10, 11, 13 bis 16 verwiesen. Sicherheitsrisiken verbunden mit von chinesischen Herstellern, in China und/oder mit chinesischer Software und/oder Hardware hergestellten Hafenkränen und sonstigen Logistikeinrichtungen sind vielschichtig. Hier sind insbesondere Fernzugriffsmöglichkeiten über Wartungssoftware oder integrierte Netzwerkschnittstellen, Datenabfluss über Warenströme, Ha-

fenbewegungen oder militärisch relevante Transporte, potenzielle Sabotage- oder Abschaltmöglichkeiten im Krisenfall, versteckte Schwachstellen (sog. Backdoors) in Hard- oder Software und starke technologische Abhängigkeiten von einzelnen Herstellern oder Ersatzteilen aus China zu nennen. Eine generelle Sensibilisierung von Zulieferern zum Thema Cybersicherheit sollte regelmäßig durchgeführt werden. Insbesondere sollten Zulieferer darauf hingewiesen werden, äußerst vertraulich mit Informationen im Zusammenhang mit KRITIS-Projekten, wie etwa Hafenanlagen, umzugehen. Eine Sicherheitsbewertung aller verwendeten Technologien und Komponenten sollte regelmäßig durchgeführt werden, gegebenenfalls durch unabhängige Experten. Außerdem sollten in regelmäßigen Abständen Penetrationstests und Schwachstellenscans in kritischen Bereichen ausgeführt werden. Ebenso sollte eine zyklische Sicherheitsevaluation von Zulieferern erwogen und bei Bedarf gegebenenfalls auf andere Zulieferer zurückgegriffen werden.

Für den Fall eines erfolgreichen Angriffs sollte ein Notfallplan eingerichtet werden, einschließlich klarer Verantwortlicher und Prozesse zur Wiederherstellung der Betriebsfähigkeit.

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?

Der Bundesregierung liegen keine Erkenntnisse im Sinne der Fragestellung vor.

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, deren 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/con-gressional-probe-communications-gear-chinese-cranes), für ihr Handeln auf nationaler und europäischer Ebene?

Es wird auf die Antwort der Bundesregierung zu Frage 46 verwiesen.

50. Wie hoch ist nach Kenntnis der Bundesregierung der Marktanteil von Hafenkränen und sonstigen Logistikeinrichtungen, die von chinesischen Herstellern, in China und/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?

Der weltweit mit Abstand größte Hersteller dieser Kräne ist das chinesische Staatsunternehmen Shanghai Zhenhua Heavy Industries (ZPMC), welches innerhalb der letzten 30 Jahre durch umfassende staatliche Subventionierung einen globalen Marktanteil von ca. 70-80 Prozent erreichen konnte.

Auch in Deutschland nimmt ZPMC eine marktbeherrschende Stellung ein. Von insgesamt rund 122 Hafenkränen, die in den Häfen von Hamburg, Bremerhaven und Wilhelmshaven für die Containerverladung genutzt werden, stammen 82 von ZPMC, also etwa 67 Prozent. In den Häfen von Wilhelmshaven liegt der Anteil sogar bei 80 Prozent. Es liegen keine Erkenntnisse über den Markt-

anteil chinesischer Softwareprodukte im Bereich von Hafenkränen und sonstigen Logistikeinrichtungen vor.

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

Der aus der Revision der EU-Screening Verordnung resultierende Anpassungsbedarf für das deutsche Recht soll direkt in das Investitionsprüfungsgesetz (IPG) integriert werden, an dessen Referentenentwurf das BMWE derzeit arbeitet. Das BMWE strebt einen Kabinettbeschluss zum IPG in der zweiten Hälfte dieses Jahres an.

Bereits nach derzeitigem deutschen Recht sind Beteiligungen an deutschen Unternehmen, die Unternehmen aus Drittstaaten mittelbar über EU-Tochterunternehmen erwerben wollen, ebenso prüffähig wie unmittelbare Erwerbe durch Unternehmen aus Drittstaaten. Im deutschen Recht besteht daher die sogenannte „Xella-Lücke“ nicht. Das IPG wird diese schon bestehende Prüfmöglichkeit für mittelbare Beteiligungserwerbe beibehalten. Die Bundesregierung hat sich im Verfahren zur Revision der EU-Screening-Verordnung erfolgreich dafür eingesetzt, dass diese Lücke, die derzeit noch in Bezug auf den EU-Kooperationsmechanismus zur Investitionsprüfung und gegebenenfalls in manchen sonstigen EU-Mitgliedstaaten besteht, mit der Neufassung der Verordnung geschlossen wird.

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 analog zu entsprechenden Forderungen auf 10 Prozent zu senken sowie atypische Kontrollerwerbe (z. B. durch Vetorechte oder Technologielizenzen) einer zwingenden vertieften Prüfung zu unterziehen?

Entsprechend der Vereinbarung im Koalitionsvertrag erarbeitet die Bundesregierung derzeit ein eigenständiges Investitionsprüfungsgesetz (IPG), in dem unter anderem die im Außenwirtschaftsgesetz und in der Außenwirtschaftsverordnung enthaltenen Regelungen zur Investitionsprüfung konsolidiert und systematisiert werden sollen.

Die Prüfschwelle für Beteiligungen an deutschen Unternehmen, die Kritische Infrastruktur betreiben, beträgt bereits nach geltendem Recht zehn Prozent. Dies ist in § 56 Absatz 1 Nummer 1 in Verbindung mit § 55 Absatz 1 Nummer 1 der Außenwirtschaftsverordnung geregelt.

Die konkreten Inhalte des IPG, dessen Referentenentwurf derzeit vom BMWE erarbeitetet wird, stehen noch nicht im Detail fest, sondern sind innerhalb der Bundesregierung im Rahmen der Ressortabstimmung zu besprechen. Dies betrifft auch Fragen im Zusammenhang mit atypischen Kontrollerwerben.

53. Welche Schlussfolgerungen zieht die Bundesregierung aus der im Rahmen des EU Industrial Accelerator Act (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?

Der von der EU-Kommission vorgelegte Entwurf eines Industrial Accelerator Act (IAA) wird von der Bundesregierung geprüft. Eine finale Positionierung bezüglich der FDI-Konditionierung steht noch aus. Der IAA-Vorschlag hat im Schwerpunkt eine industriepolitische Zielrichtung, während die Investitionsprüfung ausschließlich vor voraussichtlichen Beeinträchtigungen der öffentlichen Ordnung oder Sicherheit schützt, so dass die dem IAA-Vorschlag zugrundeliegenden Erwägungen nicht ohne Weiteres auf die Investitionsprüfung übertragbar sind.

Die Bundesregierung genehmigt im Rahmen der Investitionsprüfung Mehrheitsbeteiligungen aus Drittstaaten an deutschen Unternehmen, die Kritische Infrastruktur betreiben, nur, wenn sich daraus keine voraussichtliche Beeinträchtigung der öffentlichen Ordnung oder Sicherheit ergibt. Falls es zur Abwendung einer solchen voraussichtlichen Gefährdung erforderlich ist, erteilt sie die Genehmigung nur unter Auflagen oder untersagt die Beteiligung. Welche Maßnahmen erforderlich sind, hängt von den Umständen des konkreten Einzelfalls ab.

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?

Auch ohne ausdrücklich kodifiziert zu sein, werden die in der Frage genannten Risikofaktoren bereits heute in der Praxis bei Investitionsprüfungen berücksichtigt, wenn sie im konkreten Einzelfall für die Beurteilung einschlägig sind, ob der geprüfte Erwerb eine voraussichtliche Beeinträchtigung der öffentlichen Ordnung oder Sicherheit darstellt. Die Bundesregierung wird diese Praxis fortsetzen, so dass die künftig explizite Benennung dieser Risikofaktoren in der novellierten EU-Screening Verordnung faktisch die bereits gängige Prüfpraxis unterstützt.

In Bezug auf Erwerbe von deutschen Unternehmen, die Kritische Infrastruktur betreiben, wird zunächst auf die Antwort zu Frage 53 verwiesen. Im Übrigen wird die Bundesregierung auch künftig bei der Prüfung von derartigen Erwerben eine Genehmigung nur dann erteilen, wenn sich aus dem Erwerb keine voraussichtliche Beeinträchtigung der öffentlichen Ordnung oder Sicherheit ergibt. Anderenfalls wird die Bundesregierung im Rahmen der Investitionsprüfung auch künftig die im konkreten Einzelfall erforderlichen Maßnahmen ergreifen.

Die Investitionsprüfung schützt ausschließlich vor voraussichtlichen Beeinträchtigungen der öffentlichen Ordnung oder Sicherheit. Rein wettbewerbsrechtliche Aspekte dürfen in der Investitionsprüfung nicht berücksichtigt werden. Das Bundeskartellamt entscheidet im Rahmen seiner Zuständigkeit in

einem separaten Verfahren eigenständig über den Schutz des freien und fairen Wettbewerbs in Deutschland.

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

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

    b) Wenn nein, warum nicht?

Die Fragen 55 bis 55b werden gemeinsam beantwortet.

Die Bundeswehr führt ein Register für alle verwendeten unbemannten Drohnensysteme, in dem u. a. der jeweilige Typ, die Seriennummer und die haltende Dienststelle dokumentiert wird. Anhand dieser Daten lassen sich auf Systemebene Herstellungsländer ableiten.

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

Die Erfüllung des Kernauftrags der Bundeswehr zur Landes- und Bündnisverteidigung ist auch bei Ausschreibung und Vergabe von Aufträgen für Kleinstdrohnen handlungsleitend. Dies beinhaltet auch die Vereinbarung von Maßnahmen, um resiliente Lieferketten für die Entwicklung und Beschaffung der materiellen Ausstattung und für die Versorgung eingeführter Produkte in deren Nutzungsphase zu gewährleisten.

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

In der Bundeswehr werden keine Statistiken im Sinne der Fragestellung geführt.

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?

Ja, die Bundesregierung plant entsprechende Maßnahmen. Diesbezügliche künftige Ausschreibungen werden auf der Grundlage von § 11 des Bundeswehrbeschaffungsbeschleunigungsgesetzes (BwBBG) erfolgen.

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