

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Eugen Schmidt, Barbara Benkstein, Edgar Naujok, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 20/9450 –**

Digitalpolitische Aspekte der China-Strategie der Bundesregierung

Vorbemerkung der Fragesteller

Die Bundesregierung veröffentlichte im Sommer dieses Jahres ihre China-Strategie (Bundestagsdrucksache 20/7770). Darin werden auch zahlreiche digitalpolitische Aspekte behandelt, wie z. B. technologische Souveränität (ebd., S. 17), der Schutz kritischer Infrastrukturen (ebd., S. 21) oder die Sicherheit im Cyberraum (ebd., S. 22). Gleichwohl taucht der geläufige Begriff der chinesischen „digitalen Seidenstraße“, die laut Chinas Außenminister Wang Yi spätestens seit Ende des Jahres 2020 das Kernstück der seit 2015 von der Volksrepublik unter dem Titel „Belt and Road Initiative“ betriebenen Seidenstraßeninitiative ist (<https://www.golem.de/news/internetinfrastruktur-chinas-digitale-seidenstrasse-2205-164888.html>), mit keinem Wort in dem 32-seitigen Strategiepapier der Bundesregierung auf. Vielmehr erklärt die Bundesregierung explizit, dass sie sich nicht an der Seidenstraßeninitiative beteiligt aufgrund der Nichteinhaltung sozialer und ökologischer Standards (ebd., S. 25).

Die Sicherung ausländischer Rohstoffmärkte in Afrika, Südamerika und im Südpazifik durch milliardenschwere Investitionen sowie die Finanzierung des Aufbaus weltweiter physischer und digitaler (5G-Netze) Infrastrukturen durch die Seidenstraßeninitiative gehen jedoch Hand in Hand mit direkter oder indirekter politischer Einflussnahme durch die Volksrepublik China (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 19/28086). Dessen ungeachtet wurde noch im Jahr 2019 an den Exportweltmeister China Entwicklungshilfe gezahlt (vgl. Bundestagsdrucksache 19/15567; <https://www.faz.net/aktuell/wirtschaft/fdp-geht-gegen-deutsche-entwicklungshilfe-fuer-china-vor-16540625.html>).

In der China-Strategie verfolgt die Bundesregierung auch zu den genannten digitalpolitischen Aspekten mittlerweile ein Konzept des De-Risking mit dem Ziel, technologische, wirtschaftliche und politische Abhängigkeiten von China zu verringern (<https://www.tagesschau.de/inland/innenpolitik/china-strategie-bundesregierung-100.html>). Nach Auffassung der Fragesteller werden dazu jedoch zu wenige konkrete Ziele mit messbaren Indikatoren und Maßnahmen hinterlegt, vielmehr handelt es sich um eine erwartbare Aufreihung von Absichtserklärungen, die teilweise bekannt, teilweise bereits überholt sind, wie die angekündigte Ausgestaltung des EU Chips Act (ebd., S. 17), der bereits verabschiedet wurde und am 21. September 2023 in Kraft trat (<https://commis>

sion.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_de).

So genehmigte das Bundeskabinett unter Vorsitz des Bundeskanzlers und ehemaligen Hamburger Bürgermeisters Olaf Scholz auch die Beteiligung des chinesischen Staatskonzerns Cosco am Betreiberunternehmen HHLA des größten deutschen Seehafens, dem Hamburger Hafen, obwohl der Wirtschaftsausschuss des Deutschen Bundestages und selbst sechs Bundesministerien erhebliche Bedenken gegen die Beteiligung äußerten (<https://www.tagesschau.de/inland/regional/hamburg/ndr-china-investition-in-hamburg-falsche-einstufung-durch-hhla-100.html>).

Auch wird in der China-Strategie der Bundesregierung nach Auffassung der Fragesteller deren wirtschaftsfeindlicher Kurs deutlich, indem sie sich für ein besseres Verständnis Chinas für die Anliegen des Lieferkettengesetzes einsetzt (ebd., S. 10) und Investitions Garantien für deutsche Unternehmen einer vertieften Prüfung unterziehen wird, während 71 Prozent der deutschen Unternehmen ihre Investitionen in China weiter steigern möchten (<https://kpmg.com/de/de/home/themen/2022/01/deutsche-unternehmen-in-china.html>). Bereits im Jahr 2021 überstiegen die Direktinvestitionen deutscher Unternehmen in China 100 Mrd. Euro (vgl. www.iwkoeln.de/studien/juergen-matthes-kaum-diversifizierung.html).

1. Welche digitalpolitischen Erkenntnisse und digitalpolitischen Absichten in Bezug auf China wurden im Rahmen der Strategieentwicklung von der Bundesregierung neu gewonnen bzw. neu entworfen, und welche digitalpolitischen Erkenntnisse und digitalpolitischen Absichten der Bundesregierung in Bezug auf China waren bereits bekannt bzw. waren bereits umrissen?

Die China-Strategie legt die Sichtweise der Bundesregierung auf den Stand und die Perspektiven der Beziehungen mit China dar und setzt den Rahmen, innerhalb dessen die Ressorts der Bundesregierung ihre Politik gegenüber China kohärent gestalten. Dies trifft auch auf die digitalpolitischen Themenaspekte zu, vor allem mit Blick auf die Unterstützung und Stärkung der technologischen und digitalen Souveränität Deutschlands und Europas. Handlungsleitendes Ziel der Bundesregierung ist, dass die Europäische Union in Schlüsselbereichen nicht abhängig werden darf von Technologien aus Drittstaaten, die die fundamentalen europäischen Werte nicht teilen. Wie in Abschnitt 4.3 der Strategie dargelegt, gilt es, solche Abhängigkeiten insbesondere in kritischen Bereichen der Informationstechnologie durch die Sicherung und den Ausbau von technologischen Kompetenzen und Kapazitäten einerseits sowie andererseits durch die Diversifizierung von Lieferketten und Bezugsquellen zu vermeiden; immer unter Berücksichtigung der Innovationskraft und Resilienz technologischer und digitaler Ökosysteme insgesamt.

2. Wurden, aus Sicht der Fragesteller angesichts der Syntax zahlreicher Textpassagen zur Formulierung des Strategiepapiers Anwendungen generativer künstlicher Intelligenz (KI) angewendet wie z. B. ChatGPT, und wenn ja, welche, und welche Textpassagen wurden damit verfasst?

Nein.

3. Als wie tragfähig betrachtet die Bundesregierung ihre Prognose „Wir können weltweit Standards für energieeffiziente, langlebige, reparaturfreundliche und kreislauffähige Produkte setzen“, angesichts der Tatsache, dass die weltweite Normung und Standardisierung, z. B. in Gremien wie die Internationale Organisation für Normung (ISO), die Internationale Fernmeldeunion (ITU) oder die Internationale Elektronische Kommission (IEC), der Bundesregierung nicht weisungsgebunden ist (Bundestagsdrucksache 20/7770, S. 22)?

Welche Kenntnisse liegen der Bundesregierung über die Beliebtheit von energieeffizienten, langlebigen, reparaturfreundlichen und kreislauffähigen Produkten in Afrika, Asien, Australien und Südamerika vor (bitte nach Produktkategorie und Kontinent getrennt erläutern)?

Die Bundesregierung setzt sich, unter Berücksichtigung der im New Legislative Framework und im Normungsvertrag festgehaltenen Arbeitsteilung, für eine Stärkung des deutschen Einsatzes in internationalen Gremien der Normung und Standardisierung ein, gemeinsam mit der im Wesentlichen privatwirtschaftlich betriebenen Normung. Die Vorbildfunktion harmonisierter europäischer Normen spielt dabei eine Rolle und wird von der Bundesregierung unterstützt. Darüber hinaus stützen sich die Erwartungen der Bundesregierung in den angesprochenen Produktbereichen auf die Beobachtung, dass international tätige Unternehmen, die auf dem EU-Binnenmarkt aktiv sind, Normen aus der Europäischen Union aus Kostengründen auch auf anderen Märkten anwenden. Kenntnisse über den Einsatz oder Absatz bestimmter Produktgruppen liegen der Bundesregierung nur im Rahmen der Kriterien und Statistiken der veröffentlichten nationalen Außenhandelsstatistik oder von OECD-Zahlenwerken vor.

4. Welche Methoden der Strategischen Vorausschau beabsichtigt die Bundesregierung anzuwenden, um aufkommende Schlüsseltechnologien im Konkurrenzkampf mit China frühzeitig zu identifizieren, wurden diese bereits angewendet, und wenn ja, welche Schlüsseltechnologien wurden damit bereits identifiziert (ebd., S. 17)?

In verschiedenen Bundesbehörden kommen unterschiedliche Methoden der Strategischen Vorausschau zum Einsatz, um zukünftige Entwicklungen zu antizipieren, besser auf sie vorbereitet zu sein und sie zu gestalten. Im Rahmen des Foresight-Prozesses im Bundesministerium für Bildung und Forschung werden derzeit Ansätze zum Monitoring bestehender und zur Identifikation möglicher zukünftiger Schlüsseltechnologien entwickelt, die eine entscheidende Rolle im globalen Wettbewerb spielen werden. Hierbei kommen sowohl experten- als auch datenbasierte Methoden zum Einsatz. Diese Ansätze befinden sich derzeit noch im Entwicklungs- und Erprobungsstadium.

5. Welche Schlüsseltechnologien sind für die Bundesregierung im Konkurrenzkampf mit China aktuell von Bedeutung?

Im globalen Wettbewerb werden Technologien, die für die Dekarbonisierung von Produktionsprozessen aber auch die eigene technologische Souveränität zentral sind, künftig eine Schlüsselrolle einnehmen. Dies betrifft unter anderem die Bereiche Halbleiter, Energie/grüne Technologien, Digitalisierung/Informations- und Kommunikationstechnologien (IKT), künstliche Intelligenz (KI), Quanten- und Bio-Technologien.

6. Welche konkreten Zielvorstellungen hat die Bundesregierung hinsichtlich ihrer Absicht, sich für die gleichberechtigte Teilhabe deutscher Unternehmen in Normungs- und Standardisierungsaktivitäten in China einzusetzen, und welche konkreten Maßnahmen sollen dazu ergriffen werden (ebd., S. 18)?

An Aktivitäten in welchen chinesischen Normungs- und Standardisierungsgremien bzw. Normungs- und Standardisierungsausschüssen denkt die Bundesregierung hier insbesondere?

In Rücksprache mit einzelnen Akteuren der privatwirtschaftlichen Normung kann eine Flankierung der Interessen deutscher Unternehmen zur Teilnahme an chinesischen Normungsgremien erfolgen. Diese Möglichkeit beschränkt sich nicht auf einzelne Gremien. Die Bundesregierung unterstützt Expertinnen und Experten aus deutschen Unternehmen darüber hinaus darin, sich in bilateralen Dialogen mit chinesischen Expertinnen und Experten zu relevanten Normungsfragen auszutauschen, so dass deutsche Unternehmen leichter Kenntnisse der chinesischen Normungsaktivitäten gewinnen können. Die Bundesregierung wirkt dabei auf faire Teilnahmebedingungen hin, die denjenigen entsprechen sollten, die für die Teilnahme von Unternehmen aus Drittländern an der Normung in Europa und Deutschland gelten.

7. Wurden bereits Maßnahmen ergriffen, ein europäisches Open-Source-Ökosystem aufzubauen, und wenn ja, warum, und welche Maßnahmen wurden ergriffen (ebd., S. 18)?

Welche Erfolge wurden durch die Maßnahmen bereits erzielt?

Zur Stärkung des Open-Source-Ökosystems hat das Bundesministerium für Wirtschaft und Klimaschutz den Sovereign Tech Fund (STF) initiiert. Der Sovereign Tech Fund identifiziert kritische digitale Basistechnologien und vergibt Aufträge, um in deren Absicherung und Weiterentwicklung zu investieren. Seit dem Start des STF im September 2022 wurden 40 kritische Technologieprojekte unterstützt und drei Open-Source-Challenges sowie das Bug-Resilience-Projekt gestartet. Darüber hinaus wurde mit der Gründung des Zentrums für Digitale Souveränität (ZenDiS) ein erster Schritt zum Aufbau eines innovationsfördernden OSS-Ökosystems für die öffentliche Verwaltung gegangen. Dabei wird auch die Kooperation auf europäischer Ebene adressiert. Die Mitarbeit in entsprechenden EU-Gremien erfolgt bereits. Auch gibt es eine erste gezeichnete Absichtserklärung mit Österreich zur kollaborativen Weiterentwicklung spezifischer Open Source Lösungen sowie Gespräche mit weiteren EU-Mitgliedstaaten.

8. Was versteht die Bundesregierung unter „technologischer Abhängigkeit“, z. B. in kritischen Bereichen der Informationstechnologie (ebd., S. 17)?

Technologische Abhängigkeit umfasst insbesondere die Abhängigkeit von technologischen Kompetenzen und Kapazitäten sowie Abhängigkeiten in Lieferketten und bei Bezugsquellen für neue Technologien.

9. Wie ist die Ankündigung der Bundesregierung, mehr in Forschung, Entwicklung und Innovation zur Stärkung der technologischen Souveränität zu investieren, vor dem Hintergrund zu verstehen, dass der Haushaltsentwurf der Bundesregierung für das Jahr 2024 für das Bundesministerium für Bildung und Forschung Kürzungen von über 1 Mrd. Euro vorsieht (ebd., S. 17)?

Der Haushaltsentwurf des Jahres 2024 befindet sich noch in der Aufstellung, insofern kann hierzu keine abschließende Aussage getroffen werden.

Zur Beantwortung wird im Übrigen auf die China-Strategie der Bundesregierung (S. 9) verwiesen.

10. Konnte die angekündigte Fortentwicklung der Güterlisten in den internationalen Exportkontrollregimen sowie die Überprüfung der nationalen Güterlisten in den Bereichen Cybersicherheit und Überwachungstechnik bereits umgesetzt werden, wenn nein, warum nicht, und wann soll dies erfolgen, und wenn ja, zu welchen Ergebnissen haben diese Arbeiten geführt (ebd., S. 20)?

Mit der neuen Dual-Use Verordnung, auf die sich der Rat der Europäischen Union am 9. November 2020 unter deutschem Vorsitz mit dem Europäischen Parlament geeinigt hat, ist es gelungen, neue, striktere Kontrollvorschriften für Ausfuhren bestimmter Abhör- und Überwachungstechnik einzuführen. Damit konnte auf die deutsche Initiative aufgesetzt werden, Ausfuhren bestimmter Überwachungstechnologien im Wassenaar-Abkommen international zu kontrollieren. Darüber hinaus hatte Deutschland bereits Mitte des Jahres 2015 zusätzliche nationale Kontrollen für den Export von Monitoringsystemen für Telefonie und entsprechender Vorratsdatenspeicherung eingeführt. Die Bundesregierung setzt sich dafür ein, dass verbleibende Kontrolllücken bei Überwachungstechnologie auch auf internationaler Ebene geschlossen werden. Auf Initiative Deutschlands wurden im Jahr 2019 im Wassenaar-Abkommen neue Kontrollen für Ausfuhren von Software zur Telefonüberwachung vereinbart. Damit konnten die seit dem Jahr 2015 in Deutschland bereits auf nationaler Ebene bestehenden Kontrollen für die Monitoringsysteme erfolgreich auch auf internationaler Ebene verankert werden.

Die Bundesregierung setzt sich weiterhin dauerhaft dafür ein, die Güterlisten auf internationaler Ebene fortzuentwickeln und an neue technische Entwicklungen anzupassen. Dazu engagiert sie sich aktiv in den multilateralen Exportkontrollregimen, die ein wichtiger Baustein der internationalen Sicherheitsarchitektur sind.

11. Gibt es innerhalb der Bundesregierung unterschiedliche Auffassungen, wie mit den Ergebnissen der in der Strategie angesprochenen Prüfung von Huawei-Komponenten gemäß § 9b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) umgegangen werden soll (ebd., S. 21)?

Gibt es innerhalb der Bundesregierung einzelne Ressorts, die einen stärkeren sicherheitspolitischen Fokus haben, und andere Ressorts, die einen stärkeren wirtschaftspolitischen Fokus haben, und wie ist die Position der Auswärtigen Ämter?

Zu den konkreten laufenden Abstimmungsprozessen innerhalb der Bundesregierung kann keine Auskunft erteilt werden, da dies den Kernbereich exekutiver Eigenverantwortung betrifft. Hierzu gehört die Willensbildung der Bundes-

regierung, die sich - wie im konkreten Fall - vornehmlich in ressortübergreifenden und ressortinternen Abstimmungsprozessen vollzieht.

12. Welche öffentlichen Beschaffungen im Bereich kritischer Infrastrukturen (KRITIS) wurden seit dem Jahr 2021 intensiv auf mögliche Sicherheitsrisiken geprüft (ebd., S. 21), auf welcher Gesetzesgrundlage erfolgte dies, welche Maßnahmen wurden dazu ergriffen, und zu welchen Ergebnissen und Konsequenzen haben die Prüfungen geführt?

Öffentliche Beschaffungen speziell im Bereich kritischer Infrastrukturen (KRITIS) gibt es in der Regel nicht, da KRITIS-Betreiber mit wenigen Ausnahmen Unternehmen der Privatwirtschaft sind.

13. Seit wann sind der Bundesregierung die gegen Deutschland gerichteten, immer weiter zunehmenden Spionageaktivitäten insbesondere im Cyberraum bekannt, und kann die Bundesregierung diese Zunahme qualitativ und quantitativ beschreiben (bitte ausführen, ebd., S. 21)?

Im Rahmen der durch die Nachrichtendienste des Bundes analysierten Angriffskampagnen können chinesische Cyberspionageaktivitäten gegen deutsche Ziele gesichert bis ins Jahr 2015 zurückverfolgt werden. Im Fokus chinesischer Cyberakteure stehen insbesondere Wirtschaftsspionage gegen deutsche Unternehmen bzw. der Diebstahl geistigen Eigentums sowie Cyberangriffe gegen Regierungsinstitutionen. Dabei ist über den gesamten Zeitraum ein deutlicher Anstieg des Niveaus technischer Fähigkeiten staatlicher chinesischer Cyberakteure zu beobachten. So werden neben Spear-Phishing-Kampagnen unter anderem Supply-Chain-Angriffe sowie die gezielte Ausnutzung von Schwachstellen in Hard- und Software beobachtet. Diese mit wachsender technischer Expertise ausgeführten Cyberangriffe werden von der Bundesregierung mit hoher Priorität bearbeitet.

14. Wird der Verfassungsschutzbericht auch Hinweise auf Kenntnisse zu chinesischer Cyberspionage enthalten, um das öffentliche Problembewusstsein zu stärken, so wie es auch bezüglich chinesischer Einflussnahme angekündigt wird (ebd., S. 21)?

Das Bundesministerium des Innern und für Heimat (BMI) informiert die Öffentlichkeit mindestens einmal jährlich in einem zusammenfassenden Bericht über Bestrebungen und Tätigkeiten nach § 3 Absatz 1 des Bundesverfassungsschutzgesetzes (BVerfSchG). Dieser Bericht informiert insbesondere auch zu aktuellen Entwicklungen. So enthält der Verfassungsschutzbericht des Jahres 2022 Ausführungen über verschiedene Aspekte chinesischer Cyberspionage und trägt somit zum entsprechenden öffentlichen Problembewusstsein bei. Der Verfassungsschutzbericht des Jahres 2023 wird – wie üblich – im Laufe des auf das Berichtsjahr folgenden Jahres veröffentlicht.

15. In welchem Umfang und welcher Qualität haben nach Kenntnis der Bundesregierung chinesische Desinformationskampagnen im Zusammenhang mit Chinas Politik zu Hongkong und Taiwan seit dem Jahr 2017 zugenommen, und welche Bedeutung haben digitale Instrumente dafür (ebd., S. 22)?

Verschiedene Studien legen die Mechanismen und Instrumente der chinesischen Kommunikationsstrategie, einschließlich Desinformationskampagnen,

detailliert dar. Die Kommunikationsstrategie der Kommunistischen Partei Chinas zielt in den letzten Jahren verstärkt darauf ab, die Wahrnehmung Chinas weltweit in ihrem Sinne zu lenken und Kritik zu unterbinden. Neben der Nutzung von regulären Instrumenten der Öffentlichkeitsarbeit versucht die chinesische Regierung auch, ihren Einfluss auf und über traditionelle und soziale Medien zu vergrößern.

Für diese Einflusstategie spielen auch digitale Plattformen eine zentrale Rolle. So hatten beispielsweise im Zusammenhang mit den Protesten in Hongkong im Jahr 2019 Twitter und Facebook Konten gesperrt, weil Hinweise auf „koordinierte, staatlich unterstützte Operationen“ vorgelegen hätten. Nach Kenntnis der Bundesregierung nutzte die chinesische Regierung im Kontext der Proteste in Hongkong sogenannte „Bots“, um in Sozialen Medien die Protestbewegung zu diffamieren und das eigene Narrativ zu verbreiten.

16. Zu welchen Maßnahmen hat die Ankündigung der Bundesregierung, mit der dienstlichen Verwendung internetbasierter Dienstleistungen, Apps und sozialer Medien aus China restriktiv umzugehen, bereits geführt (ebd., S. 22)?

Wie bereits vor Veröffentlichung der Strategie erfolgt für jeden Einsatz von Apps usw. im Rahmen der Informationssicherheit eine Einzelfallbetrachtung bei entsprechender Risikobewertung durch den Informationssicherheitsbeauftragten in eigener Zuständigkeit der jeweiligen Behörde.

17. Betrachtet die Bundesregierung „maximale Transparenz und Öffentlichkeit, insbesondere, wenn öffentliche Mittel für die Zusammenarbeit mit China eingesetzt werden“ als angemessen, ausreichend und dem nationalen deutschen Interesse dienend, wenn es bei dieser Zusammenarbeit um digitale Technologien geht, die auch militärisch genutzt werden können oder von wesentlicher wirtschaftlicher Bedeutung für den Standort Deutschland sind (ebd., S. 22)?

Die chinesische Politik der zivil-militärischen Fusion setzt der Zusammenarbeit Grenzen. Der Bundesregierung ist bewusst, dass auch zivile Forschungsprojekte, einschließlich Grundlagenforschung, von China strategisch auf ihre militärische Verwendbarkeit hin betrachtet werden können.

Die Bundesregierung sieht es daher als wichtig und richtig an, die Wissenschaftsbeziehungen werte- und interessengetrieben weiterzuentwickeln. Dies schließt – auch im Kontext der Zusammenarbeit bei digitalen Technologien – die Achtung des verfassungsrechtlich verbürgten Grundsatzes der Freiheit der Wissenschaft und der damit verbundenen Verantwortung ein. Risiken für die Freiheit von Forschung und Lehre, illegitime Einflussnahme und einseitiger Wissens- bzw. Technologietransfer müssen dabei minimiert, Transparenz und Öffentlichkeit maximiert werden.

18. Welche neuen klaren Vorgaben wurden von der Bundesregierung seit dem Jahr 2021 bei der Beschaffung von IT des Bundes bislang gemacht, um zu mehr Sicherheit im Cyberraum und insbesondere zur Wahrung der Informationssicherheit zu gelangen, und welche Beschaffungen, die auch Technologie chinesischer Herkunft beinhalteten, waren davon betroffen (ebd., S. 22)?

Mit der Novellierung des BSI-Gesetzes im Jahr 2009 konnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Bundesbehörden verbindli-

che Sicherheitsstandards für die Beschaffung und den Einsatz von IT entwickeln. Auf Grund der sehr unterschiedlichen Beschaffungsgegenstände kommen unterschiedliche Instrumente in den jeweiligen Beschaffungen zum Tragen. Unter anderem stellt das BSI im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 10 BSIG technische Richtlinien bereit, die von den Stellen des Bundes als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmerinnen und Auftragnehmer (Eignung) und IT-Produkte (Spezifikation) für die Durchführung von Vergabeverfahren berücksichtigt werden. Die jeweils individuellen Anforderungen an die Beschaffung von IT ist der jeweiligen Ausschreibung zu entnehmen. Zentrale Beschaffungsvorgaben, welche einzelne Länder besonders behandeln, existieren nicht und sind nicht geplant.

19. Welche Aspekte des Entwurfs eines Gesetzes zur Umsetzung der CER (Critical Entities Resilience)-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen („KRITIS-Dachgesetz“) sind derzeit noch in der Ressortabstimmung, welche unterschiedlichen Positionen werden dazu ggf. noch eingenommen, und zu welchen Aspekten des Entwurfes herrscht in der Bundesregierung bereits Einigkeit (ebd., S. 22)?

Wann soll der Gesetzentwurf in das parlamentarische Verfahren eingestellt werden?

Die Umsetzung der EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie) in Form eines KRITIS-Dachgesetzes befindet sich derzeit in der Bundesregierung in der Abstimmung. Es handelt sich um einen laufenden, nicht finalisierten Vorgang. Zum Schutz des Kernbereichs exekutiver Eigenverantwortung kann über die Abstimmung bzw. Positionierung innerhalb und zwischen den Ressorts keine Auskunft erteilt werden.

20. Sieht die Bundesregierung angesichts der nach Ansicht der Fragesteller offensichtlichen und gravierenden Verfahrensfehler (<https://www.tagesschau.de/inland/regional/hamburg/ndr-china-investition-in-hamburg-falsche-einstufung-durch-hhla-100.html>) die Voraussetzungen der §§ 48, 49 des Verwaltungsverfahrensgesetzes als erfüllt an (vgl. die Einschätzung der Bundesregierung in ihrer Antwort auf die Kleine Anfrage auf Bundestagsdrucksache 20/8548, S. 12), um ggf. die Beteiligung des chinesischen Staatskonzerns Cosco am Hamburger Hafen rückgängig zu machen, und wie begründet die Bundesregierung ihre Einschätzung?

Die Bundesregierung bleibt dabei, dem chinesischen Staatsunternehmen COSCO den Erwerb eines Anteils an der HHLA CTT GmbH in Teilen zu untersagen. Wie im Herbst 2022 im Bundeskabinett entschieden, darf COSCO lediglich Anteile von weniger als 25 Prozent an dem Terminal im Hamburger Hafen erwerben. Die HHLA CTT GmbH gilt inzwischen als Betreiber Kritischer Infrastruktur gemäß den gesetzlichen Vorgaben. Eine Abänderung der Kabinettsentscheidung vom 31. Oktober 2022, die die Veräußerung auf unter 25 Prozent begrenzte, erfolgt nicht. Die Teiluntersagung von Herbst 2022 bleibt damit rechtsgültig. Die Bundesregierung hat den Erwerbsparteien bestätigt, dass die überarbeiteten Kaufverträge im Einklang mit den Bedingungen der Teiluntersagung stehen.

21. Mit welchen finanziellen, personellen oder organisatorischen Ressourcen unterstützt die Bundesregierung die Initiative Wirtschaftsschutz (Bundestagsdrucksache 20/7770, S. 22)?

Die Bundesregierung ist wesentlicher Teil der Initiative Wirtschaftsschutz. Die Koordination der Initiative Wirtschaftsschutz erfolgt durch das Bundesministerium des Innern und für Heimat. Die Mitglieder der Initiative treffen sich regelmäßig auf Arbeits- und Steuerungsebene. Aus dem Haushalt des Bundesministeriums des Innern und für Heimat werden auch Vorhaben der Initiative finanziert.

22. Welche inhaltlichen Positionen wird die Bundesregierung bei der Überarbeitung der EU Cyber Diplomacy Toolbox einbringen (ebd., S. 22)?

Die Bundesregierung wird sich für eine noch wirksamere Ausgestaltung der EU Cyber Diplomacy Toolbox einschließlich des damit verbundenen EU-Cybersanktionsregimes einsetzen.

23. Welche eigens errichteten chinesischen und anderen ausländischen Zertifizierungsregime im Bereich der Cybersicherheit lehnt die Bundesregierung aufgrund sachfremder Auflagen und intransparenter Überprüfungsmethoden ab (bitte einzeln auflisten), wie wird die jeweilige Ablehnung der Bundesregierung umgesetzt, und ab wann wird die jeweilige Ablehnung wirksam werden (ebd., S. 22)?

China hat mit der Ausweitung des Zertifizierungsregimes „Chinese Compulsory Certification“ (CCC) auf IT-Produkte einen eigenen Zertifizierungsrahmen jenseits der international anerkannten Schemata (Common Criteria etc.) geschaffen. Die Bundesregierung lehnt das CCC jedoch ab. Es beinhaltet sachfremde Auflagen und intransparente Überprüfungsmethoden, die einen unerwünschten Abfluss von geistigem Eigentum (Intellectual Property, IP) begünstigen können.

24. Wenn die multilaterale Stärkung der internationalen Cybersicherheit auf Basis des Völkerrechts für die Bundesregierung zur Sicherheit im Cyberraum „eine Priorität“ ist, ist dann die unilaterale Stärkung der nationalen kritischen Infrastrukturen, der nationalen Sicherheitsgesetzgebung und der deutschen IT-Sicherheitsbehörden eine andere Priorität, und wenn ja, welche Priorität priorisiert die Bundesregierung, und wie begründet die Bundesregierung ihre Priorisierungen (ebd., S. 22)?

Beide Bereiche sind für die Bundesregierung prioritär.

- a) An welche konkreten Maßnahmen zur multilateralen Stärkung der internationalen Cybersicherheit auf Basis des Völkerrechts hat die Bundesregierung bei der Formulierung ihrer China-Strategie gedacht?

Die Bundesregierung strebt Einigkeit auf VN-Ebene zur umfassenden Geltung des Völkerrechts im Cyberraum an und unterstützt beispielsweise Staaten darin, ihre nationalen völkerrechtlichen Positionen zur Anwendung des Völkerrechts im Cyberraum zu erarbeiten, um sich verstärkt in multilaterale Prozesse einbringen zu können.

- b) Welche Erfolge im Bereich der Sicherheit im Cyberraum konnten auf Basis des Völkerrechts bereits erzielt werden?

Ein Erfolg ist die Verabschiedung der auf das Völkerrecht im Cyberraum verweisenden VN-Cybernormen durch die Gruppe der Regierungsexpertinnen und -experten der Vereinten Nationen sowie deren Indossierung durch die VN-Generalversammlung.

- c) In welchen Gremien beabsichtigt die Bundesregierung, die multilaterale Stärkung der internationalen Cybersicherheit auf Basis des Völkerrechts voranzutreiben (bitte im Einzelnen erläutern)?

Auf multilateralem Wege wird sich die Bundesregierung vor allem innerhalb der mit Cybersicherheit befassten Gremien der EU, der OSZE, der NATO und der VN für die Stärkung internationaler Cybersicherheit einsetzen.

25. Aus welchen Gründen wird das Thema Produktpiraterie, das insbesondere auch elektronische Konsumgüter betrifft, die weltweit vor allem von China aus über das Internet vermarktet werden und nach Auffassung der Fragesteller nicht nur aus wirtschaftlicher, sondern auch aus Verbrauchersicht hinsichtlich Gesundheits- und Umweltverträglichkeit von hoher Bedeutung sind, in dem 32-seitigen Strategiepapier nur in einem kurzen Halbsatz erwähnt, und welche konkreten Maßnahmen beabsichtigt die Bundesregierung in den nächsten zwei Jahren dagegen zu ergreifen (ebd., S. 11)?

Die Bekämpfung der Produktpiraterie ist der Bundesregierung ein wichtiges Anliegen; deshalb wird diese auch in der umfassenden China-Strategie der Bundesregierung explizit erwähnt. Die Bundesregierung wirkt international und national konstruktiv daran mit, dass die politischen, rechtlichen und gesellschaftlichen Rahmenbedingungen für eine Bekämpfung der Produktpiraterie stetig verbessert werden. So setzt sie sich auf internationaler Ebene sowohl im Rahmen der G7/G20 als auch in den entsprechenden Gremien der Welthandelsorganisation für einen besseren Schutz Geistigen Eigentums ein. Zum Beispiel findet im Dezember 2023 das jährliche Treffen der Präsidentinnen und Präsidenten der Ämter für geistiges Eigentum der G7-Staaten statt, bei dem unter anderem über die Zusammenarbeit der Staaten beim Schutz geistiger Eigentumsrechte gegen neuartige Gefährdungen für geistige Eigentumsrechte durch digitale Technologien wie zum Beispiel künstliche Intelligenz sowie im Metaverse gesprochen werden soll. Die Bundesregierung und die deutschen Auslandsvertretungen in China unterstützen deutsche Unternehmen auch direkt politisch bei der Durchsetzung ihrer geistigen Eigentumsrechte, sei es durch hochrangige politische Ansprache gegenüber der chinesischen Regierung oder durch die in der deutschen Botschaft in Peking eingerichtete Stelle eines IP-Attachés. Die Europäische Kommission hat nach Kenntnis der Bundesregierung Fragen der Produktpiraterie zuletzt Mitte November 2023 im Rahmen der EU-China-IP Working Group angesprochen.

Ebenfalls große Bedeutung kommt der Zusammenarbeit auf europäischer Ebene zu. Die Bundesregierung arbeitet eng mit der Europäischen Kommission sowie mit dem Europäischen Amt für geistiges Eigentum (EUIPO) zusammen und unterstützt die vom EUIPO eingerichtete Europäische Beobachtungsstelle für Verletzungen von Rechten des geistigen Eigentums. Auf nationaler Ebene wurde der Aufgabenbereich des Deutschen Patent- und Markenamts (DPMA) durch den im Jahr 2021 neu eingefügten § 26a des Patentgesetzes um die Information der Öffentlichkeit, insbesondere auch von kleinen und mittleren Unternehmen, über Rechte des geistigen Eigentums einschließlich der Wahrnehmung

und Durchsetzung dieser Rechte erweitert. Dies schließt die Weitergabe von Informationen über Risiken im Zusammenhang mit Piraterieware mit ein.

Zur Verhinderung von Einfuhren von Piraterieware arbeitet die Zentralstelle Gewerblicher Rechtsschutz der deutschen Zollverwaltung sowohl national als auch EU-weit eng mit dem DPMA, dem EUIPO, den Europäischen Zollbehörden und der Europäischen Kommission zusammen. Auch mit den betroffenen Unternehmen besteht eine enge Zusammenarbeit. Stellen die deutschen Zollbehörden Waren fest, die im Verdacht stehen, ein Recht geistigen Eigentums zu verletzen, das Gegenstand eines von der Zentralstelle Gewerblicher Rechtsschutz bewilligten Grenzbeschlagnahmeantrags der Rechteinhaber ist, so setzen sie die Überlassung der Waren aus oder halten diese zurück. Sind die Voraussetzungen nach Artikel 23 VO (EU) 608/2013 erfüllt, werden die Waren vernichtet, damit sie nicht in den Wirtschaftskreislauf gelangen.

26. Ist die Evaluierung der deutsch-chinesischen Kooperation im Bereich Industrie 4.0 mittlerweile abgeschlossen, wenn ja, mit welchem Ergebnis, und wenn nein warum nicht, und wann soll dies erfolgen (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 20/4441)?
- a) Bis wann werden sämtliche Projekte der zweiten Förderbekanntmachung „Chinesische Kooperation zur intelligenten Fertigung (Industrie 4.0) und Smart Services“ abgeschlossen sein, in Form der Einreichung der Verwendungsnachweise durch die Fördernehmer?

Die Fragen 26 und 26a werden gemeinsam beantwortet.

Die Frist für die Einreichung der Unterlagen endet am 30. September 2024.

- b) Ist die finale Entscheidung über die dritte Förderbekanntmachung „Chinesische Kooperation zur intelligenten Fertigung (Industrie 4.0) und Smart Services“ mittlerweile gefallen, wenn ja, wie lautet diese, und wenn nein, warum nicht, und wann soll dies erfolgen (vgl. Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 20/4441)?
- Wurden dabei Evaluierungen vorangegangener Förderrunden berücksichtigt, wenn ja welche, und wenn nein warum nicht?
- c) Wurde bei der Entwicklung der dritten Förderbekanntmachung „Chinesische Kooperation zur intelligenten Fertigung (Industrie 4.0) und Smart Services“ auch die Absicht der Bundesregierung, im Rahmen der Forschungs- und Innovationsförderung Vorgaben zu machen, damit Projekte mit China, in denen Wissensabfluss wahrscheinlich ist, nicht oder nur unter geeigneten Auflagen gefördert werden, berücksichtigt, und wenn ja, wie (ebd., S. 17)?

Die Fragen 26b und 26c werden zusammen beantwortet.

Aufgrund der politischen Schwerpunktsetzung wurde auf eine Förderung im Rahmen der dritten Bekanntmachungsrunde verzichtet.

27. An welche konkreten „ergänzenden Vereinbarungen im Digitalbereich“ denkt die Bundesregierung im Einzelnen hinsichtlich ihrer Absicht, bestehende Abkommen im Bereich der Handelspolitik „noch“ effektiver zu nutzen (Bundestagsdrucksache 20/7770, S. 24)?

Die Bundesregierung unterstützt die Europäische Kommission in ihren Bestrebungen, ein plurilaterales Abkommen zu E-Commerce in der Welthandelsorga-

nisation zu verhandeln und darüber hinaus im Rahmen bilateraler Verhandlungen mit wichtigen Partnerländern, wie etwa Japan, Korea und Singapur, eigenständige Digitalbestimmungen in bestehenden und neuen Handelsabkommen zu verankern. Mit diesen Vereinbarungen soll unter anderem der grenzüberschreitende digitale Handel erleichtert, ein hohes Verbraucherschutzniveau in der digitalen Welt sichergestellt und ungerechtfertigte Datenlokalisierungsaufgaben oder Datenzugriffsmöglichkeiten für staatliche Stellen in Drittstaaten zurückgedrängt werden.