Deutschlands wirtschaftliche Sicherheit und Technologie: Exportkontrollen, Investitionsprüfung und Marktzugangsinstrumente optimieren

Barker, Tyson; Hagebölling, David

Veröffentlichungsversion / Published Version
Sammelwerksbeitrag / collection article

Deutsche Gesellschaft für Auswärtige Politik e. V.

November 2022

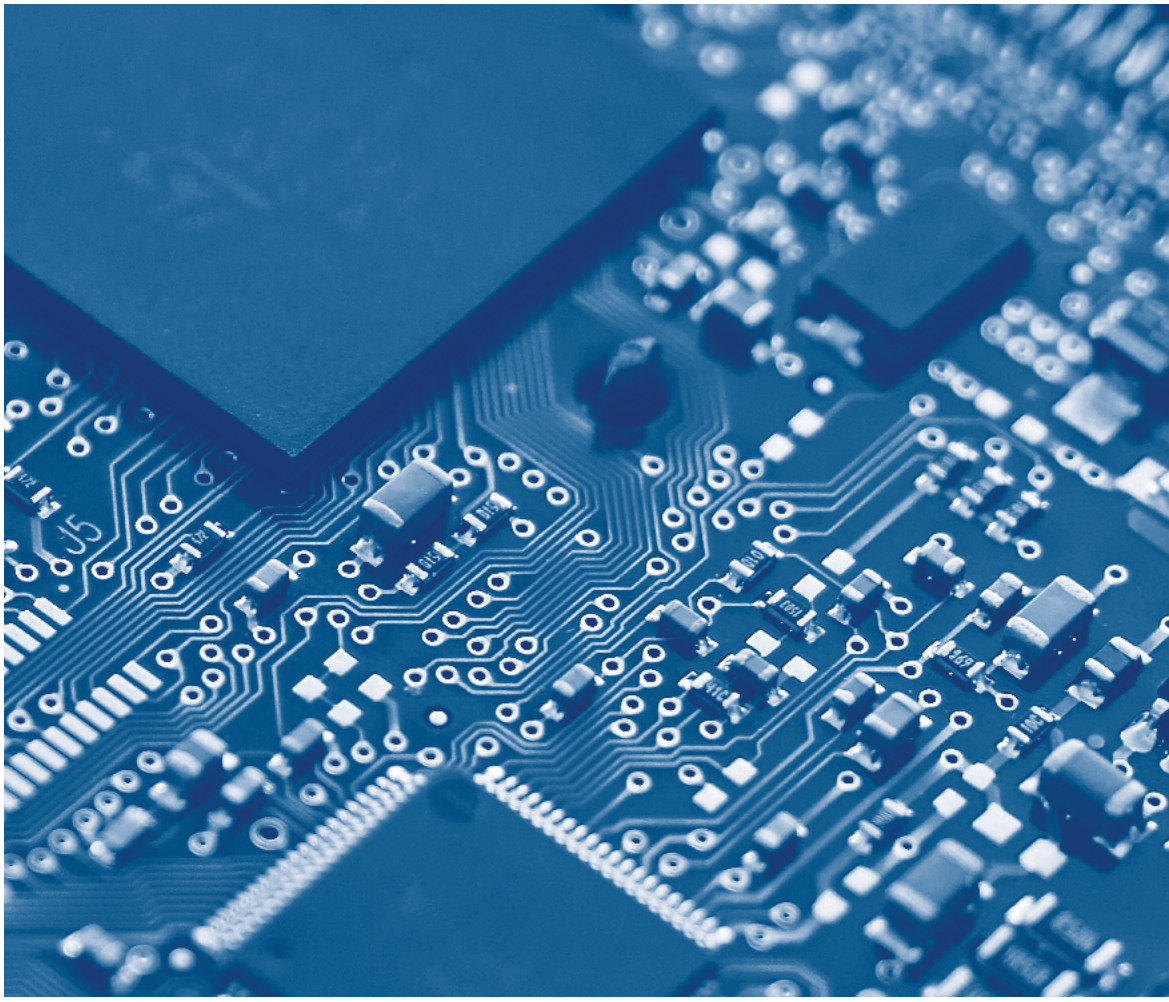
DGAP BERICHT

Deutschlands wirtschaftliche Sicherheit und Technologie

Exportkontrollen, Investitionsprüfung und Marktzugangsinstrumente optimieren

Tyson Barker
Leiter, Programm Technologie und Außenpolitik

Dr. David Hagebölling
Associate Fellow, Programm Technologie und Außenpolitik



KAPITELÜBERSICHT

Zentrale Erkenntnisse

1 Die technologische Entwicklung und der Wettstreit zwischen den USA und China haben geopolitische Konsequenzen für den Zugang zu Technologien. Die Erosion von multilateralen Ausfuhrkontrollregimen für Technologien mit doppeltem Verwendungszweck (Dual-Use), etwa vom Wassenaar-Abkommen, sowie von Investitions- und anderen Kontrollregelungen aus der Zeit nach dem Kalten Krieg, hat zu nationalen, EU- und Ad-hoc-Maßnahmen geführt, wie der Beschränkung von Russlands Zugang zu Halbleitern nach dem Angriff auf die Ukraine.

2 Die Bundesregierung muss Instrumente für die Steuerung von Technologiezugang und -kontrolle in Deutschlands Digital- und Nationale Sicherheitsstrategie integrieren – dazu gehören Ausfuhrkontrollen, die Prüfung bestimmter ausländischer Direktinvestitionen, der Zugang zu kritischen Infrastrukturen, der Schutz von Forschungsergebnissen und Auslandsinvestitionen. Da sich die Digitalstrategie nicht mit dem Zugang zu kritischen Technologien und deren Kontrolle befasst, sollte sich die Nationale Sicherheitsstrategie umfassend mit diesen Themen auseinandersetzen.

3 Die Regeln für die Ausfuhr von Dual-Use-Gütern und die Überprüfung ausländischer Direktinvestitionen wurden sowohl auf nationaler als auch auf EU-Ebene angepasst und sind bereits in Kraft getreten. Dem Ausbau entsprechender Kapazitäten und der Abstimmung mit Bündnispartnern in der EU und der NATO sollte nun mehr Aufmerksamkeit zukommen. Weitere Maßnahmen könnten einen robusteren, institutionalisierten Informationsaustausch umfassen, ebenso wie Konsultationen über Ausfuhr-, Einfuhr-, Investitions- und Forschungskontrollen im Bereich der Dual-Use-Technologien in einem Multilateralen Ausschuss für Technologiekontrolle, welcher aus der G7 oder dem Handels- und Technologierat EU-USA (TTC) hervorgeht. Der Ausschuss sollte zudem in der Lage sein, den Endnutzerzugriff auf deutsche Technologien gemäß eigener Regeln für ausländische Direktprodukte und einer „Entity List“ zu verwehren.

Einleitung

Die Anzahl an Technologien mit doppeltem Verwendungszweck (Dual-Use), sprich Technologien, die sowohl zivil als auch militärisch verwendbar sind, wächst.[1] Die Einstufung als Technologie mit doppeltem Verwendungszweck beschränkte sich früher hauptsächlich auf kapitalintensive Technologien in Bereichen wie Nukleartechnik, Chemie, Präzisionslenkung und Aufklärung. Heutzutage fällt eine viel breitere Palette von Informations- und Kommunikationstechnologien (IKT) unter diese Kategorie, deren Nutzung und Entwicklung vielfältige Formen annehmen können.

Technologien und ihre Komponenten haben nicht nur an strategischer Bedeutung gewonnen, sondern können die sich digitalisierende Gesellschaft, Wirtschaft und sogar die politischen Prozesse Deutschlands mittlerweile empfindlich stören. Hierzulande und in der EU hergestellte oder entwickelte Technologien können das Ziel ausländischer Einflussnahme, Spionage und Übernahme durch Akteure mit unlauteren Absichten werden. Doch auch Technologien, die im Ausland hergestellt, aber im Inland für kritische Infrastrukturen erforderlich sind – etwa Halbleiter und 5G-Technologie – bieten ausländischen Akteuren Möglichkeiten für politische und wirtschaftliche Manipulation.

Für die Wahrung des sozialen Zusammenhalts, der wirtschaftlichen Wettbewerbsfähigkeit und letztlich der nationalen Sicherheit werden der Einsatz von Technologie und die Steuerung des Marktzugangs daher von entscheidender Bedeutung sein. Der Einsatz von Governance-Instrumenten, sei es die Kontrolle des Technologiezugangs, der Schutz geistigen Eigentums, die Reduzierung von Abhängigkeiten in bestimmten Lieferketten oder ausländische Direktinvestitionen, sollte eine zentrale Rolle in der deutschen Digitalpolitik und nationalen Sicherheit spielen.

Einschränkungen des Zugangs zu Technologien sind nie lückenlos. Seit der Entwicklung der Atombombe durch die Sowjetunion zu Beginn des Kalten Krieges haben Industriespionage, illegaler Technologietransfer, die Verbreitung von geistigem Eigentum sowie von Ergebnissen aus Forschung und Entwicklung (FuE) dazu geführt, dass Konkurrenten die

1 SPIRI, Dual-use export controls, (o.D.): https://www.sipri.org/research/armament-and-disarmament/dual-use-and-arms-trade-control/dual-use-export-controls (abgerufen am 20. Oktober 2022).

Technologieführer einholen konnten. Kontrollen über den Zugang zu kritischen Technologien sind daher nur für eine begrenzte Zeit wirksam. Wie lange, hängt von mehreren Faktoren ab: von staatlichen Kapazitäten (China, Iran, Saudi-Arabien, Russland und andere Staaten haben unterschiedliche Innovationskapazitäten, auf die sie zurückgreifen können) und von der technologischen Komplexität (kapital- und Know-how-intensive Produktionsprozesse können zu langfristigen Beschränkungen führen; im Gegensatz dazu ist es bei bestimmten Technologien, wie KI und Cyber-Überwachungssoftware, einfacher, Beschränkungen zu umgehen und so unrechtmäßig auf sie zuzugreifen oder sie zu replizieren).

Status quo

Die Verbreitung digitaler Technologien hat den Wohlstand in Deutschland und weltweit angekurbelt – durch bessere IKT-Konnektivität, eine Verkleinerung der digitalen Kluft und mehr Möglichkeiten für grenzüberschreitende Forschung. Diese Fortschritte bleiben jedoch nicht ohne geopolitische Folgen. Der Zugang und die Kontrolle in Bezug auf moderne Halbleiter, Online-Plattformen, Cloud-Dienste, Datenpools, hochmoderne KI-Lösungen und Quantentechnologie bilden heute den Kern wirtschaftlicher und militärischer Vormachtstellung. Darüber hinaus hat die Verlagerung von Innovationen im Bereich der kritischen Technologien von konkreten zu allgemeinen Anwendungen und vom militärischen zum privaten Sektor die Rahmenbedingungen von Technologie-Ausfuhr, Investition, Forschung und Beschaffung grundlegend verändert. Dies hat Auswirkungen auf die nationale Sicherheit und wirtschaftliche Abhängigkeiten.

DER MULTILATERALE ANSATZ FÜR TECHNOLOGIEZUGANG UND -KONTROLLE

Vor dem Hintergrund der Rivalität zwischen den USA und China, der militärischen Aggression Russlands und dem immer stärkeren Bestreben von Staaten, Technologien nach ihren eigenen ideologischen Vorstellungen zu nutzen, ist die globale Technologie-Governance unter Druck geraten. Deutschland ist Mitglied in zahlreichen multilateralen Exportkontrollregimen wie dem Wassenaar-Abkommen, der Gruppe der Kernmaterial-Lieferländer (Nuclear Suppliers Group, NSG), der Australia Group, dem Trägertechnologie-Kontrollregime (Missile Technology Control Regime, MTCR) und dem kleineren Zangger-Komitee. Unter ihnen ist das nicht bindende Wassenaar-Abkommen von besonderer Bedeutung: Es regelt die Ausfuhrkontrolle von konventionellen Waffen und einigen Dua-Use-Technologien. Dabei haben sich aber auch die Grenzen von multilateralen Abkommen offenbart, die neben demokratischen auch zunehmend autoritäre Regime miteinschließen.

Die derzeitigen multilateralen Regelungen zur Koordinierung von Ausfuhrkontrollen entsprechen jedoch nicht mehr den heutigen geopolitischen Herausforderungen. Das Wassenaar-Abkommen, in dem derzeit 42 Länder vertreten sind, bietet eine normative Grundlage für einige Aspekte von Dual-Use-Technologien, ist jedoch nicht so wirksam wie sein Vorgänger aus dem Kalten Krieg, der Koordinierungsausschuss für multilaterale Ausfuhrkontrollen (Coordinating Committee for Multilateral Export Controls, COCOM).[2] Es gewährt bei geplanten Ausfuhrgenehmigungen kein Vetorecht. Der Informationsaustausch zwischen den Vertragsstaaten ist freiwillig. Ferner enthält es keine klaren Angaben zu den Ländern, denen Schlüsseltechnologien verwehrt werden sollen, sondern verweist lediglich auf „bedenkliche Staaten", ohne nähere Bestimmung. Aufgrund seiner großen Mitgliederzahl – einschließlich Russlands – mangelt es an Kohäsion. Zudem steht das Verständnis vom Umfang von Dual-Use-Technologien in einem Missverhältnis zu dem immer größeren Bereich von Software, Computing-Kapazitäten und geistigen Eigentum, etwa bei der Fertigung von Chips, der zur Repression und Überwachung im Inland und für militärische Zwecke eingesetzt werden kann.

REFORMEN DER DEUTSCHEN REGELUNGEN ZUR TECHNOLOGIEKONTROLLE

In Anbetracht der begrenzten Möglichkeiten der multilateralen Governance kritischer Technologien erfolgt die Regulierung größtenteils auf nationaler

2 COCOM ist als ein Produkt der damaligen technologischen Entwicklung zu betrachten. Der Zusammenhalt des Westens im Hinblick auf eine eindeutige Bedrohung trug zu seiner Wirksamkeit bei, ebenso wie die Vormachtstellung der USA, die konsequente Anwendung einer Liste zentraler Technologien und die relativ geringe Anzahl relevanter Technologien, deren Herstellung, Verwendung und Weitergabe somit leichter zu identifizieren und zu überwachen war. John H. Henshaw, The Origins of Cocom: Lessons for Contemporary Proliferation Control Regimes, in: The Henry L. Stimson Center Report Nr. 7, Mai 1993: https://www.stimson.org/wp-content/files/file-attachments/Report7_1.pdf (abgerufen am 20. Oktober 2022).

DIREKTE U. INDIREKTE ANWENDBARKEIT SPEZIFISCHER EXPORT-KONTROLLREGELUNGEN FÜR AUKOMMENDE TECHNOLOGIE-BEREICHE

TECHNOLOGIEBEREICHE	KI	QC	LR	CS	HL	BT	KT	ET	AT	R
AUSTRALISCHE GRUPPE	○	○	○	○	○	●	○	○	○	○
DT. AUSSENWIRTSCHAFTSVERORDNUNG	●	●	●	●	●	○	●	○	●	●
CHEMIEWAFFENKONVENTION (CWC)	○	○	○	○	○	○	○	○	○	○
TRÄGERTECHNOLOGIE-KONTROLLREGIME (MTCR)	○	○	●	○	○	○	◐	○	○	○
GRUPPE DER KERNMATERIAL-LIEFERLÄNDER (NSG)	○	○	○	○	○	○	○	○	○	◐
WASSENAAR-ABKOMMEN	◐	◐	◐	◐	◐	◐	●	○	◐	◐
ZANGEN CONVENTION	○	○	○	○	○	○	○	◐	○	○

● DIREKT ANWENDBAR ◐ TEILWEISE ANWENDBAR

KI = Künstliche Intelligenz | **QC** = Quantum Computing | **LR** = Luft- und Raumfahrttechnologie | **CS** = Cybersicherheit | **HL** = Halbleiterprodukte | **BT** = Biotechnologie | **KT** = Kommunikationstechnologie (inkl. 5G) | **ET** = Energietechnologie | **AT** = Autonomie | **R** = Robotik

Quelle: Darstellung der Autoren

und EU-Ebene oder durch Ad-hoc-Vereinbarungen. Der deutsche Rechtsrahmen für Ausfuhrkontrollen trägt dem Umstand Rechnung, dass sich der Umfang der Lizenzierung von Dual-Use-Technologien vergrößert hat. Doch aufgrund von lückenhaften Regelungen konnten in der Vergangenheit deutsche Technologien von Akteuren, die als nicht vertrauenswürdig einzustufen sind, gekauft und vertrieben werden.[3] Der Fall des Münchner Unternehmens FinFisher ist ein bekanntes Beispiel hierfür. Das Unternehmen entwickelte eine der weltweit fortschrittlichsten Formen von Spionagesoftware, die auch von den deutschen Strafverfolgungsbehörden eingesetzt wurde. Es nutzte jedoch die laxen Kontrollen aus, um sein Produkt auch an autoritäre Regierungen in Ägypten, Uganda, Äthiopien, Bahrain und der Türkei zu verkaufen. Diese setzten sie wiederum ein, um gegen oppositionelle Aktivistinnen und Aktivisten vorzugehen.[4] Deutschland hat seine Ausfuhrkontrollen nach 2015 verschärft, was zur Insolvenz von FinFisher im Jahr 2022 geführt hat.[5] Doch bleiben Bürokratie und ein Mangel an systemischer Vorausschau ernst zu nehmende Hürden für eine rechtzeitige Regulierung nationaler Technologien und ihrer Nutzung.

Deutschland verfügt auch in anderen Bereichen über einzigartige Stärken in den internationalen Lieferketten für kritische Technologien, die einer genauen Prüfung unterzogen werden sollten. Drei der fünf größten Chiplieferanten von ASML, dem niederländischen Hersteller von UV-Lithografiesystemen, gehören zu Deutschlands „Mittelstand“ (Zeiss, der Werkzeugmaschinen- und Laserhersteller Trumpf und das integrierte Photonik-Unternehmen Jenoptik). Insgesamt ist Deutschland der drittgrößte Exporteur von geistigem Eigentum nach China. Auf das Land entfallen zehn Prozent des externen Ursprungs von technologischem geistigem Eigentum – nur die USA (31 Prozent) und Japan (21 Prozent) liefern mehr.[6]

Auch die Investitionsprüfung wurde im Zuge des zunehmenden technologischen Wettstreits zwischen den USA und China überarbeitet. Auf nationaler Ebene hat Deutschland das Außenwirtschaftsgesetz (AWG)[7]

3 Hans-Martin Tillack, Philipp Grüll, Deutsche Technik in Kriegsschiffen Chinas, in: Tagesschau, 6. November 2021: https://www.tagesschau.de/investigativ/report-muenchen/china-kriegsschiffe-motoren-deutschland-101.html (abgerufen am 9. September 2022).

4 Andre Meister, German Made State Malware Company FinFisher Raided, in: Netzpolitik, 14. Oktober 2020: https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided (abgerufen am 12. September 2022).

5 Chaos Computer Club, Stage win: FinFisher is bankrupt, 28. März 2022).: https://www.ccc.de/en/updates/2022/etappensieg-finfisher-ist-pleite (abgerufen am 12. September 2022).

6 McKinsey Global Institute, China and the world. Inside the dynamics of a changing relationship, Juli 2019: https://www.mckinsey.com/~/media/mckinsey/featured%20insights/china/china%20and%20the%20world%20inside%20the%20dynamics%20of%20a%20changing%20relationship/mgi-china-and-the-world-full-report-june-2019-vf.ashx (abgerufen am 23. September 2022).

7 Bundesministerium für Wirtschaft und Klimaschutz (BMWK), Außenwirtschaftsgesetz, 7. Juli 2020: https://www.bmwk.de/Redaktion/DE/Gesetze/Aussenwirtschaft/AWG.html (abgerufen am 9. September 2022).

und die Außenwirtschaftsverordnung (AWV)[8] reformiert, um die Kontrolle ausländischer Direktinvestitionen zu stärken und zu modernisieren.[9] Beschleunigt wurde diese Restrukturierung der Prüfung ausländischer Direktinvestitionen durch die COVID-19-Pandemie, den Schock über die Übernahme des nationalen Robotik-Champions Kuka im Jahr 2016 und den verstärkten Wettstreit zwischen den USA und China.

Die neue Verordnung wirkt sich auf 16 Wirtschaftssektoren aus, von denen die meisten kritische Technologien betreffen: KI, Robotik, Chipfertigung, Luft- und Raumfahrt, Quantentechnologie, Dateninfrastruktur und 3D-Druck sowie kritische Infrastrukturbereiche wie Telekommunikation.[10] Gemäß den aktualisierten Vorschriften müssen die für Investitionsprüfung zuständigen deutschen Behörden bei der Akquisition von mehr als 20 Prozent der Stimmrechte in einem Unternehmen benachrichtigt werden. Dieser Schwellenwert ist bei Verbündeten niedriger. Japan reduzierte diesen im Rahmen seiner verschärften Wirtschaftssicherheits-Politik in bestimmten Branchen beispielsweise von zehn auf ein Prozent.[11]

Eine Vielzahl von deutschen Behörden und Ministerien prüft Investitionen, jedoch nicht immer in enger Zusammenarbeit. Dazu gehören das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA), das Auswärtige Amt (AA), das Bundesministerium für Wirtschaft und Klimaschutz (BMWK), das Bundesministerium der Verteidigung (BMVg) und das Bundesministerium des Innern und für Heimat (BMI). Die Zahl der zu prüfenden Fälle hat sich seit der Reform im Jahr 2020 mehr als verdreifacht, was die Kapazitäten der Behörden auslastet. Die Reform des Prüfverfahrens im Zusammenhang mit ausländischen Direktinvestitionen hat das BMWK, das BMVg und weitere Behörden dazu veranlasst, vermehrt bilaterale Konsultationen mit Verbündeten, einschließlich des US-Finanzministeriums, durchzuführen.

REFORMEN DER EU-REGELUNGEN ZUR TECHNOLOGIEKONTROLLE

Die EU-Kommission ist eine treibende Kraft hinter nationalen Bemühungen, die Regelungen über den Zugang zu und der Kontrolle von Technologien zu aktualisieren und eine kohärentere europäische Technologie-Governance zu entwickeln. Die neue EU-Ausfuhrkontrollregelung trat im September 2021 in Kraft und wertet die Rolle von Ausfuhrkontrollen kritischer Technologien erheblich auf. Sie konzentriert sich insbesondere auf Cyber-Überwachungstechnologien und ihre „Dimension der menschlichen Sicherheit“,[12] ein für nicht gelistete Güter verwendeter Sammelbegriff. Ziel ist es, die Technologie Deutschlands und anderer Mitgliedstaaten von den internationalen Märkten fernzuhalten, um Missbrauch oder Nachbildung zu verhindern.[13]

Das Kontrollregime umfasst mehrere Neuerungen. Erstens werden der Austausch und die Berichterstattung zwischen den Mitgliedstaaten und der Kommission verstärkt. Zweitens sorgt es für eine bessere Koordinierung und Transparenz zwischen den zuständigen Behörden. Und drittens wird die elektronische Genehmigungsplattform der EU ausgebaut, welche Mitgliedstaaten einen Einblick in die Maßnahmen der anderen EU-Staaten gibt. Diese war bisher jedoch nur begrenzt erfolgreich. Nur drei Staaten und eine Region der Union verwenden sie: Italien, Lettland, Rumänien und die Wallonische Region Belgiens.

DEUTSCHE UND EU-REGELUNGEN IM KONTEXT DER MASSNAHMEN VON PARTNERSTAATEN

Die Maßnahmen von Partnerstaaten, insbesondere der USA, haben die Modernisierung der europäischen Regelungen zur Ausfuhrkontrolle und des Verfahrens zur Überprüfung von ausländischen Direktinvestitionen beeinflusst. Der US-Kongress hat 2018 damit

8 Ebd.

9 BMWK, Außenwirtschaftsrecht – Investitionsprüfung, 2022: https://www.bmwk.de/Redaktion/DE/Artikel/Aussenwirtschaft/investitionspruefung.html (abgerufen am 9. September 2022).

10 United Nations Conference on Trade and Development, World Investment Report 2020. International Production beyond the Pandemic – Chapter III: Recent Policy Developments and Key Issues, Vereinte Nationen, 2020: https://unctad.org/system/files/official-document/WIR2020_CH3.pdf (abgerufen am 9. September 2022).

11 Didi Kirsten Tatlow, Afra Herr, Japan's "Economic Security" Measures – A Model for Managing China's Rise, DGAP Policy Brief, Deutsche Gesellschaft für Auswärtige Politik, 7. Februar 2022: https://dgap.org/en/research/publications/japans-economic-security-measures (abgerufen am 9. September 2022).

12 Verordnung des Europäischen Parlaments und des Rates, Über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck, L 206/1, 11. Juni 2021: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021R0821 (abgerufen am 9. September 2022).

13 IHK Düsseldorf, Leitfaden zur Exportkontrolle, Oktober 2021: https://www.ihk.de/duesseldorf/aussenwirtschaft/zoll-und-aussenwirtschaftsrecht/exportkontrolle-2594636 (abgerufen am 9. September 2022).

begonnen, die Prüfverfahren im Zusammenhang mit kritischen Technologien, Daten, Software und geistigem Eigentum zu überarbeiten, um sicherzustellen, dass das Land mit der rasanten Entwicklung von Allzwecktechnologien Schritt halten kann. Mit zwei Reformen – dem Foreign Investment Risk Review Modernization Act (FIRRMA) und dem Export Control Reform Act (ECRA) – hat der Kongress den Umfang, die Geschwindigkeit und Durchsetzbarkeit von potenziellen Beschränkungen in den Bereichen Export, Lizenzierung geistigen Eigentums und ausländische Direktinvestitionen erheblich erweitert.[14] Angesichts des verschärften geopolitischen Wettstreits mit China sowie Russlands Krieg gegen die Ukraine haben die Trump- und anschließend die Biden-Regierung diese neuen Befugnisse genutzt, um den Zugang Chinas und Russlands zu Halbleitern und entsprechendem geistigen Eigentum zu beschränken. Die USA haben außerdem den Zugang Chinas zu den amerikanischen Märkten für Drohnen, Smart-City-, KI-, Bio- und Mobilfunktechnologie begrenzt.

Jüngst hat die US-Regierung zudem ihre Beschränkungen für China im Bereich der Halbleitertechnologie erweitert und geht nun über ihr bisheriges Ziel hinaus, Peking stets zwei Generationen voraus zu bleiben.[15] Die USA verfolgen nun einen maximalistischen Ansatz und beschränken den Zugang Chinas zu „kräftemultiplizierender" Chiptechnologie. Dazu gehören Beschränkungen beim Design von Chips, die im KI-Bereich und in Hochleistungsrechnern eingesetzt werden, sowie das Verbot für US-Staatsangehörige, an der Produktion, dem Vertrieb und der Wartung von Chip-Produktionsanlagen für den chinesischen Markt mitzuwirken.[16] Dieser veränderte US-Ansatz wirkt sich auf die globalen technologischen Wertschöpfungsketten aus und stellt deutsche und europäische Unternehmen, die tief in diese integriert sind, vor Herausforderungen. Außerdem signalisiert dieser Ansatz die Entschlossenheit der USA, ihre Vormachtstellung in den globalen Technologiemärkten zu nutzen, um die Macht Chinas einzudämmen, und zwar notfalls auch im Alleingang.

Diese Verschiebung im US-amerikanischen Ansatz sowie die sich rapide verschlechternde geopolitische Situation, insbesondere Russlands Invasion der Ukraine, befördern weiter die Bedeutung von Kooperationsformaten zwischen der EU und Partnerstaaten. In Abstimmung mit den USA im Rahmen des TTC hat Deutschland umgehend Beschränkungen für die Ausfuhr von Gütern und den Zugang zu geistigem Eigentum in Bezug auf hochwertige Halbleitertechnologie, die für Russland bestimmt war, eingeführt.[17] Die Auswirkungen dieser Kooperation – die wohl wichtigsten im Zusammenhang mit den Sanktionen gegen Russland – werden die militärischen Fähigkeiten Russlands in den Bereichen Luftfahrt, Drohnentechnologie und Präzisionslenkwaffen schwächen. Des Weiteren wird diese Kooperation auch zu einem allmählichen Zerfall der Automobil-, zivilen Luft- und Raumfahrt-, Geräte- und IKT-Ausrüstungsindustrie in Russland führen.

Für chinesische Unternehmen mit engen Verbindungen zur Kommunistischen Partei und der Volksbefreiungsarmee bestehen dennoch weiterhin spürbare Unterschiede in Bezug auf den Zugang zu Technologien in Deutschland und der EU einerseits und deren Verbündeten andererseits. Im Gegensatz zu einigen seiner Partner hat Deutschland keine sogenannte Entity List für die Bestimmung von Endnutzern, denen der Zugang zu kritischer Technologie und geistigem Eigentum verweigert werden sollte.[18] Die deutschen Regelungen unterscheiden sich – wie der Rest Europas – auch dadurch von denjenigen der USA, dass sie dem Import von Technologien, auch aus autoritären Staaten, offener gegenüberstehen. Der Einsatz von nicht vertrauenswürdigen Technologien als Komponenten kritischer Infrastrukturen ist, angesichts der Nutzung von 5G-Mobilfunknetzausrüstung von chinesischen staatsnahen Unternehmen (Huawei und ZTE), russischer Cybersicherheitssoftware (Kaspersky Labs) und US-amerikanischer Hyperscaler-Cloud-Dienste (Amazon Web Services und Microsoft Azure Cloud) in Deutschland und anderen Mitgliedstaaten, in der

14 Stormy-Annika Mildner, Claudia Schmucker, Investment screening: protectionism and industrial policy? Or justified policy tool to protect national security?, in: Task Force 3 Trade Investment and Growth, September 2021: https://www.t20italy.org/wp-content/uploads/2021/09/TF3_PB08_LM04 (abgerufen am 20. Oktober 2022).

15 Reva Goujon, Running Target: Next-Level US Tech Controls on China, Rhodium Group, 28. September 2022: https://rhg.com/research/running-target (abgerufen am 20. Oktober 2022).

16 Max A. Cherney, The Biden administration issues sweeping new rules on chip-tech exports to China, in: protocol, 7. Oktober 2022 https://www.protocol.com/enterprise/chip-export-restrictions-tsmc-intel (abgerufen am 20. Oktober 2022).

17 U.S. Department of Commerce Bureau of Industry and Security, § 734.9 Foreign-Direct Product (FDP) Rules, (o.D.): https://www.bis.doc.gov/index.php/licensing/reexports-and-offshore-transactions/direct-public-guidelines#:~:text=Foreign%2Dproduced%20items%20located%20outside,a%20foreign%2Dproduced%20item%20is (abgerufen am 19. September 2022); U.S.-EU Trade and Technology Council, U.S.-EU Joint Statement of the Trade and Technology Council, 16. Mai 2022: https://www.whitehouse.gov/wp-content/uploads/2022/05/TTC-US-text-Final-May-14.pdf (abgerufen am 19. September 2022).

18 Dies unterscheidet sich deutlich von der Verwendung von Entity Lists und der Foreign-Direct Product Rule durch die USA, um bestimmten Endnutzerinnen und -nutzern unter anderem über Sekundärmärkte den Zugang zu verweigern. Dies gilt nicht nur für Unternehmen, sondern – nach dem Einmarsch Russlands in der Ukraine – auch für ein ganzes Land.

politischen Debatte der EU zu einem wichtigeren Thema geworden. Trotz dieses wachsenden europäischen Bewusstseins für technologiebezogene Risiken zeigt die 2020 EU Toolbox für 5G-Sicherheit die Schwierigkeiten bei der Beschränkung von Technologie- und Softwareimporten auf, da diese weiterhin in den Zuständigkeitsbereich der Mitgliedstaaten fällt.

Aktueller politischer Ansatz

In der Digitalstrategie 2022 der Bundesregierung finden Instrumente für Technologiezugang und -kontrolle keine Erwähnung. Dies ist ein auffälliger blinder Fleck, wenn man bedenkt, wie wichtig der Zugang zu kritischen Technologien und deren Kontrolle für die technologische Modernisierung Deutschlands sind. Dennoch haben Deutschland und Europa in den letzten fünf Jahren nationale, multilaterale und normative Mechanismen, die kritische Technologien und Marktzugang mit geopolitischem Einfluss verbinden, rapide reformiert. Diese Bemühungen haben dazu geführt, dass Themen wie Demokratie, Menschenrechte und wirtschaftliche Sicherheit bei Marktzugangsinstrumenten wie Investitionsprüfung, Ausfuhrkontrollen und Sanktionen, Lizenzierung von geistigem Eigentum sowie Forschung und Entwicklung stärkere Berücksichtigung finden. Deutschland und die EU haben außerdem schnell gehandelt, um Lieferketten zu diversifizieren und resilienter zu machen, verlässliche „Friendshoring"-Partnerschaften aufzubauen und neue Instrumente zu entwickeln, die bevorzugten Zugang zu kritischen Technologien garantieren, wenn Engpässe die europäische Sicherheit bedrohen.[19]

Deutschland und die EU nutzen ihre Marktmacht und ihre technologischen Stärken zunehmend gemeinsam mit den USA, dem Vereinigten Königreich, Japan und anderen Partnerstaaten. Die Bundesregierung baut weiterhin Kapazitäten für die Durchsetzung der Reformen in den Bereichen Technologieexport und Überwachung von ausländischen Direktinvestitionen aus. Die Folgen des Abschneidens Russlands vom Zugang zu grundlegender Chiptechnologie verdeutlichen konkret die Wirksamkeit dieser Form technologiebasierter Macht und zeigen das Potenzial von Technologiezugang als geopolitisches Instrument für die EU und die NATO.

Deutschland priorisiert ebenfalls, im Rahmen der EU, die Sicherheit der Lieferketten für kritische Technologien, um sich vor externen technologischen Schwachstellen zu schützen. Infolge pandemiebedingter Engpässe bei Lieferketten hat das Land bereits staatliche Anreize eingeführt, um das Onshoring, die Diversifizierung und die Resilienz von Lieferketten für kritische Technologien und deren Komponenten zu fördern. Im Vorfeld der Veröffentlichung der deutschen China-Strategie wurden kontroverse Diskussionen über Politikänderungen geführt, die staatliche Investitionen und Exportgarantien für Unternehmensexpansionen in China einschränken oder gar unterbinden würden. Ziel ist es, die Handels-, Beschaffungs- und Investitionsbeziehungen gemeinsam mit anderen ostasiatischen Staaten zu diversifizieren.[20] Deutschland hat auch die Sorgfaltspflichten für Lieferketten in Bezug auf Menschenrechte aktualisiert, einschließlich der Nutzung von Zwangsarbeit.[21]

Die Europäische Kommission hat sich ihrerseits für ein stärkeres Onshoring und Friendshoring von Technologie und strategisch wichtigen Komponenten eingesetzt, auch mittels ihrer Industriepolitik.[22] Das Europäische Chip-Gesetz ist neben den wichtigen Vorhaben von gemeinsamem europäischem Interesse (Important Projects of Common European Interest, IPCEI) der ehrgeizigste Versuch, einen Rahmen für den Zugang zu kritischen Technologien und deren Resilienz zu schaffen. Gemäß dem Gesetz soll die

19 Europäische Kommission, European Chips Act, 2022: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en (abgerufen am 19. September 2022).

20 Andreas Rinke, Sarah Marsh, Exclusive: German economy ministry reviews measures to curb China business, in: Reuters, 8. September 2022: https://www.reuters.com/markets/exclusive-german-economy-ministry-reviews-measures-curb-china-business-2022-09-08 (abgerufen am 19. September 2022).

21 Bundesministerium für Arbeit und Soziales, Act on Corporate Due Diligence in Supply Chains, 8. August 2021: https://www.bmas.de/EN/Services/Press/recent-publications/2021/act-on-corporate-due-diligence-in-supply-chains.html (abgerufen am 23. September 2022).

22 Europäische Kommission, Commission presents an updated in-depth review of Europe's strategic dependencies, 23. Februar 2022: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1124 (abgerufen am 24. Oktober 2022).

Sicherheit der europäischen Halbleiterversorgung durch eine Kombination aus gezielter staatlicher Unterstützung, verstärkter Zusammenarbeit mit Partnerstaaten und verbesserten Handlungsmöglichkeiten in Krisenzeiten gestärkt werden. Die Kommission hat die Mitgliedstaaten und ihre Industrien aufgefordert, Engpässe und Schwachstellen in Halbleiter-Lieferketten zu erfassen. Für die deutsche Automobilindustrie, das industrielle Internet der Dinge (IoT), die Robotikbranche und das verarbeitende Gewerbe ist dies ein besonders sensibles Thema. Ferner zielt die Kommission darauf ab, staatliche Beihilfen für „Erstproduktionen" zu gewähren, um die Subventionierung kritischer Technologien, für die auf den Märkten bereits Nachfrage besteht, zu begrenzen. All dies geschieht zu einer Zeit, in der in Deutschland lebhaft über die Effizienz eines stärker staatskapitalistisch ausgerichteten Modells zur Erhaltung des Zugangs zu kritischen Technologien debattiert wird. Einige argumentieren, dass der zusätzliche Nutzen die Kosten nicht rechtfertige. In China, den ostasiatischen Demokratien und zunehmend auch in den USA geht der Trend jedoch dahin, dass der Abbau von Abhängigkeiten und die Sicherstellung des Zugangs zu und der Entwicklung von Technologie gegenüber diesen marktwirtschaftlichen Bedenken überwiegen.

Auch über die Grenzen der EU hinaus arbeitet die Kommission verstärkt mit Partnern zusammen, insbesondere mit den USA. In den Jahren 2021 und 2022 hat sie beispielsweise ein Ersuchen der USA an die deutsche Bundesregierung und die deutsche Industrie unterstützt, sich an einem Kartierungs- und Frühwarnverfahren zur Sicherheit der Halbleiterversorgung zu beteiligen. Der Nationalismus im Kontext der COVID-19-Impfung Anfang 2021, insbesondere in den USA und im Vereinigten Königreich, hat jedoch zu einer Neubewertung sicherer Versorgungswege für kritische Technologien geführt, selbst unter Verbündeten. Die Kommission hat eine Debatte zu Monitoring und Krisenreaktion angestoßen, auch in Bezug auf Beschränkungen der Technologieausfuhr. Diese wurde auch durch die Entscheidung der US-Regierung befördert, COVID-19-Impfstoffhersteller mit dem Defense Production Act dazu zu zwingen, amerikanischen Aufträgen Vorrang zu geben.[23]

Was die Sorgfaltspflicht bezüglich Cybersicherheit bei der Beschaffung und in Lieferketten betrifft, so hat die Bundesregierung neue Anforderungen an ihre kritischen Technologieinfrastrukturen vorgegeben (wie in der NIS-2-Richtlinie beschrieben). Sie hat den Betreibern kritischer Infrastrukturen strengere IT-Sicherheitsanforderungen auferlegt und beruft sich zum ersten Mal auf die IT-Sicherheit als Grund für die Regulierung bestimmter Unternehmen und die Einstufung bestimmter Infrastrukturen als kritisch.[24] Komponenten, die in kritischen Infrastrukturen verwendet werden, dürfen nur noch mit einer Erklärung über die Vertrauenswürdigkeit des Anbieters verwendet werden, wobei die Erklärung die Mindestanforderungen des Bundesministeriums des Innern und für Heimat (BMI) erfüllen muss, die allerdings noch nicht festgelegt sind.

Die Bundesregierung hat damit wichtige Schritte unternommen, um die Verwendung von kritischen Komponenten, die den Sicherheitsinteressen Deutschlands, der EU und der NATO entgegenstehen, zu unterbinden. Diese Schritte zielen implizit auf die 5G-/6G-Netzwerkausrüster Huawei und ZTE ab. Doch der Prozess der technischen und politischen Konsensfindung, an dessen Spitze der Bundeskanzler steht, ist bewusst komplex und das Ergebnis schwer zu vereinbarender Differenzen, die auf die unterschiedlichen Interessen und Standpunkte der Ministerien zurückzuführen sind. Auch die Entscheidungsfindung verläuft schleppend, da das Bundesamt für Sicherheit in der Informationstechnik (BSI) sein Zertifizierungsprogramm für vertrauenswürdige Komponenten gerade erst aufgelegt hat.[25] Unterdessen ist der politische Druck für einen schnellen Ausbau von 5G-Netzen hoch, während Huawei auf dem Weg ist, mehr als die Hälfte der 5G-Netztechnik in Deutschland zu stellen, vor allem in der Funkzugangsnetz-Infrastruktur (Radio Access Network, RAN).[26] Einige der EU- und NATO-Partner Deutschlands sind der Ansicht, dass die Nutzung von Huawei-Komponenten ein inakzeptables Risiko darstelle, und viele schließen diese sowohl aus ihrer 5G-Kern- als auch aus RAN-Infrastruktur aus. Das BSI deutet auch in anderen Bereichen neue Beschränkungen an. So hat es beispielsweise öffentlich vor Sicherheitsrisiken im Zusammenhang

23 Generaldirektion Handel der Europäischen Kommission, Defense Production Act (DPA) during COVID-19, 27. März 2022: https://trade.ec.europa.eu/access-to-markets/de/barriers/details?isSps=false&barrier_id=15818 (abgerufen am 12. September 2022).

24 Deutscher Bundestag, Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, Drucksache 19/26106, 25. Januar 2021: https://dserver.bundestag.de/btd/19/261/1926106.pdf (abgerufen am 12. September 2022).

25 Stefan Krempl, Huawei-Klausel: BSI startet Zertifizierungsprogramm für 5G-Komponenten, in: Heise Online, 5. Juli 2022: https://www.heise.de/news/Huawei-Klausel-BSI-startet-Zertifizierungsprogramm-fuer-5G-Komponenten-7163182.html (abgerufen am 20. Oktober 2022).

26 Philipp Alvares de Souza Soares, Moritz Koch, Dietmar Neuerer, Bundesregierung droht Huawei mit Rauswurf, 25. Juli 2022: https://www.handelsblatt.com/technik/cybersecurity/it-sicherheit-bundesregierung-droht-huawei-mit-rauswurf/28541284.html?utm_campaign=hb-update&utm_content=25072022&utm_medium=email&utm_source=nl (abgerufen am 20. Oktober 2022).

mit der IT-Sicherheitssoftware Kaspersky gewarnt und hat der deutschen Privatwirtschaft empfohlen, diese nicht mehr einzusetzen.[27]

Und schließlich unternimmt Deutschland erste zaghafte Schritte, um die Bedenken seiner Verbündeten hinsichtlich des Forschungsschutzes zu berücksichtigen. Das Bundesministerium für Bildung und Forschung (BMBF) hat diskret begonnen, über Mittel und Wege nachzudenken, um die Integrität und Offenheit von Grundlagenforschungsprogrammen an Universitäten und in Netzwerken wie der Max-Planck-Gesellschaft, der Fraunhofer-Gesellschaft und der Helmholtz-Gemeinschaft zu schützen. Diese Bemühungen stehen auch im Einklang mit der gesteigerten Aufmerksamkeit der Europäischen Kommission bezüglich illegaler chinesischer Forschungstransfers.[28] Deutschlands ausgezeichnete Forschung in den Bereichen Quantenphysik, künstliche Intelligenz und Robotik hat besondere Aufmerksamkeit hinsichtlich ihrer Attraktivität für chinesische Forschende an akademischen Einrichtungen, die der Volksbefreiungsarmee nahestehen, erregt.[29] China entsendet gezielt Mitarbeiterinnen und Mitarbeiter, die in seinen militärisch-akademisch-industriellen Komplex eingebettet sind, an ausländische Universitäten und setzt zurückkehrende Wissenschaftlerinnen und Wissenschaftler unter Druck, damit sie Einblicke in ihre Arbeit im Ausland gewähren.[30] Fälle von Infiltrationen im des Wissenschaftsbereichs von durch autoritäre Regierungen beauftragten Personen geben der EU Anlass zur Sorge.[31] Während viele deutsche Hochschulen die Zusammenarbeit mit dem Militär und Verteidigungssektor ihres eigenen Landes meiden, ist man sich paradoxerweise der Risiken einer akademischen Zusammenarbeit mit Personen und Forschungseinrichtungen, die in das chinesische Militärsystem eingebunden sind, kaum bewusst.

Die deutsche Forschungsgemeinschaft muss daher ein Gleichgewicht finden zwischen Achtsamkeit in Bezug auf Infiltrationsrisiken und ihrer Offenheit gegenüber Forschenden aus aller Welt, einschließlich China und Russland. In den USA hat das harte Vorgehen gegen chinesische Forschende dem Ruf und der Attraktivität des Landes als Forschungs- und Innovationszentrum strategischen Schaden zugefügt.[32] Während Deutschland, und im weiteren Sinne die EU, die internationale Beteiligung an ihrer Forschung neu bewertet, müssen deutsche akademische Einrichtungen und das BMBF weiterhin auf die Einhaltung der Sorgfaltspflicht, die Achtung der Menschenrechte sowie auf Rechtsstaatlichkeit, Verhältnismäßigkeit und ein offenes deutsches Forschungsklima achten.

Handlungs-empfehlungen

Wie auch der Rest Europas ist Deutschland dabei, den Zugang zu kritischen Technologien und ihre Kontrolle angesichts der angespannten geopolitischen Lage und der sich weiter beschleunigenden technologischen Entwicklung neu zu justieren. Die erste deutsche Nationale Sicherheitsstrategie sollte einen kohärenteren und am geopolitischen Umfeld ausgerichteten Ansatz für Technologie-Governance und den Marktzugang zu kritischen Technologien ermöglichen und gleichzeitig einen möglichst offenen Zugang zu technologischen Innovationen gewährleisten. Dazu muss die Bundesregierung ein Gleichgewicht zwischen offenen Märkten und anderen wirtschaftlichen Anforderungen sowie nationaler und europäischer Sicherheit und Resilienz finden. Um dies zu erreichen, sollte sie:

Gemeinsam mit Verbündeten einen multilateralen Ausschuss für Technologiekontrolle im 21. Jahrhundert schaffen. Dieser neue Ausschuss würde den Informationsaustausch und die Koordinierung

27 Bundesamt für Sicherheit in der Informationstechnik, BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten, 15. März 2022: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html (abgerufen am 12. September 2022).

28 Ursula von der Leyen, 2022 State of the Union Address, 14. September 2022: https://ec.europa.eu/commission/presscorner/detail/ov/speech_22_5493 (abgerufen am 19. September 2022).

29 Naomi Conrad, Esther Felden and Sandra Petersmann, Are European academics helping China's military?, in: Deutsche Welle, 19. Mai 2022: https://www.dw.com/en/are-european-academics-helping-chinas-military/a-61834716 (abgerufen am 19. September 2022).

30 Alex Joske, The China Defence Universities Tracker, in: Australian Strategic Policy Institute, 25. November 2019: https://www.aspi.org.au/report/china-defence-universities-tracker (abgerufen am 12. September 2022).

31 Ursula von der Leyen, 2022 State of the Union Address, 14. September 2022: https://ec.europa.eu/commission/presscorner/detail/ov/speech_22_5493 (abgerufen am 20. Oktober 2022).

32 Nidhi Subbaraman, Scientists' fears of racial bias surge amid US crackdown on China ties, in: nature, 29. Oktober 2021: https://www.nature.com/articles/d41586-021-02976-8 (abgerufen am 20. Oktober 2022).

von Zugangsbeschränkungen bezüglich strategischer Technologien für autoritäre Staaten wie Russland und China systematisieren. Er könnte im Rahmen des TTC oder der G7 eingerichtet werden, mit potenziellen Andock-Mechanismen für andere konsolidierte Demokratien wie Australien und Neuseeland. Zu seinen Funktionen sollte das Erstellen von Dashboards für den Informationsaustausch, das Formulieren von Empfehlungen für Einfuhr- und Ausfuhrkontrollen für kritische Technologien mit doppeltem Verwendungszweck, Investitionsprüfung, die Ermittlung vertrauenswürdiger Anbieter und Forschungsschutz gehören. Bei Einfuhren sollte ein besonderes Augenmerk auf KI-gestützte Überwachungstechnologie für Smart Cities, digitale Dienstleistungen und Hardware gelegt werden. Ferner könnte sich der Ausschuss dafür einsetzen, dass in den Bereichen Ausfuhr, Investitionen und geistiges Eigentum dieselben Beschränkungen auch für Cyber-Akteure gelten, die ihre Produkte an autoritäre Regime vertreiben, die wiederum ihre Bürgerinnen und Bürger überwachen und die Menschenrechte verletzen. Zu diesen Akteuren gehören das israelische Unternehmen NSO, das die berüchtigte Spionagesoftware Pegasus entwickelt hat, und das nordmazedonische Unternehmen Cytrox, das die Spionagesoftware Predator vertrieben hat.[33]

Instrumente wie die „Foreign-Direct Product Rule“ und die „Entity List“ in Deutschland einführen. Die Foreign-Direct Product Rule der USA ermöglicht es, den Export von Technologien zu beschränken, wenn diese in den USA hergestellt wurden oder amerikanische Ausrüstung, Tools, Software oder geschütztes geistiges Eigentum umfassen. Die meisten europäisch kontrollierten Engpässe für Technologien liegen zwar in anderen Bereichen, aber Deutschland verfügt über viele wichtige, versteckte Hebel in High-Tech-Wertschöpfungsketten. Darüber hinaus würden solche Instrumente Deutschland helfen, sich auf künftige potenzielle Engpässe in der Quanten- und Biotechnologie vorzubereiten – Bereiche, in denen Deutschland über wichtige Nischenfähigkeiten in der Lieferkette verfügen könnte.

Eine handlungsorientierte politische Debatte über die Governance von Forschung und abfließenden Investitionen anstoßen. Das BMWK hat begonnen, geeignete Überprüfungsmechanismen zu evaluieren und erwägt, Anreize für Investitionen in Produktion, FuE oder Joint Ventures in autoritären Staaten, die zu einem illegalen Technologietransfer führen könnten, abzubauen. Die Bundesregierung sollte mit ihren EU- und NATO-Partnern evaluieren, wie Investitionen von autokratischen Staaten besser geprüft werden können, ohne offene Märkte zu gefährden.[34] Das BMBF sollte sich auf EU-Maßnahmen in diesen Bereichen vorbereiten, indem es Leitlinien erstellt und diese öffentlich zugänglich macht.

Die Bewertung der Vertrauenswürdigkeit über 5G-Netzwerkausrüstung hinaus ausweiten. Die Nationale Sicherheitsstrategie Deutschlands sollte eine stärkere Entwicklung nationaler Instrumente ermöglichen, die politische und sicherheitspolitische Faktoren bei der Beschaffung von Technologie heranziehen. Diese Instrumente sollten über die Bestimmungen des IT-Sicherheitsgesetzes 2.0 und der EU-Toolbox für 5G-Sicherheit hinausgehen und auch für Bereiche wie Smart Citys, intelligente Netze und Satellitentechnologie gelten. Die Integration dieser Bereiche ist in US-amerikanischen Regelungen bereits Standard, findet sich aber auch in der Integrated Review of Foreign Policy, Defence, Security and International Development[35] des Vereinigten Königreichs aus dem Jahr 2021 und in der japanischen Wirtschaftssicherheits-Politik. Die Bundesregierung sollte Mittel zur Verfügung stellen, um verdeckte wirtschaftliche und sicherheitsrelevante Externalitäten der Nutzung nicht vertrauenswürdiger Anbieter zu bewerten. Dies schließt auch Externalitäten eines möglichen „Rip and Replace“ wichtiger Technologie in kritischer 5G-/6G- und Smart-City-Infrastruktur sowie in der Screening- und Überwachungstechnologie von Städten und Bundesländern ein.[36]

Die europäische Beteiligung an neu entstehenden Vereinbarungen über den Zugang zu Technologien und deren Kontrolle im indopazifischen Raum fördern. Eine stärkere strategische Konvergenz

33 Ryan Gallagher, Spyware Vendor FinFisher Claims Insolvency Amid Investigation, in: Bloomberg, 28. März 2022: https://www.bloomberg.com/news/articles/2022-03-28/spyware-vendor-finfisher-claims-insolvency-amid-investigation (abgerufen am19. September 2022).

34 Inu Manak, Outbound Investment Screening Waits in the Wings, Deutsche Gesellschaft für Auswärtige Politik, 15. August 2022: https://www.cfr.org/blog/outbound-investment-screening-waits-wings (abgerufen am 20. Oktober 2022).

35 Bundeskabinett, The Integrated Review 2021, 16. März 2021: https://www.gov.uk/government/collections/the-integrated-review-2021 (abgerufen am 12. September 2022).

36 Johannes Rieckmann, Tim H. Stuchtey, The Hidden Cost of Untrusted Vendors in 5G Networks – State of Discussion and Estimations for Germany, Brandenburgisches Institut für Gesellschaft und Sicherheit, März 2021: https://www.bigs-potsdam.org/publikationen/the-hidden-cost-of-untrusted-vendors-in-5g-networks-state-of-discussion-and-estimations-for-germany (abgerufen am 19. September 2022).

zwischen Europa und anderen demokratischen Akteuren ist der Schlüssel zur Schaffung eines robusten, zuverlässigen Marktes für kritische Technologien. Die Bundesregierung sollte sich im Rahmen der EU dafür einsetzen, dass Europa sich auf geoökonomischer und technologischer Ebene verstärkt im indopazifischen Raum engagiert. Die EU könnte sich an der wachsenden Zusammenarbeit zwischen demokratischen Halbleiterproduzenten wie den USA, Taiwan, Japan und Südkorea (siehe die im Entstehen begriffene Chip 4 Alliance) beteiligen. In diesem Forum könnte die EU dazu beitragen, den freien Austausch von Chipdesign, geistigem Eigentum und Produktionsmitteln zu gewährleisten und Zugangsregeln festzulegen, die den illegalen Transfer von Technologie und geistigem Eigentum verhindern.[37]

37 Arjun Gargeyas, The Chip 4 Alliance Might Work on Paper, But Problems Will Persist, in: The Diplomat, 25. August 2022: https://thediplomat.com/2022/08/the-chip4-alliance-might-work-on-paper-but-problems-will-persist (abgerufen am 12. September 2022).

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

Die Deutsche Gesellschaft für Auswärtige Politik e.V. (DGAP) forscht und berät zu aktuellen Themen der deutschen und europäischen Außenpolitik. Dieser Text spiegelt die Meinung der Autorinnen und Autoren wider, nicht die der DGAP.

Die DGAP ist gefördert vom Auswärtigen Amt aufgrund eines Beschlusses des Deutschen Bundestages.

Herausgeber
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Übersetzung executive english

Redaktion Jana Idris

Layout Lara Bührer

Design Konzept WeDo

Fotos Autorinnen und Autoren © DGAP