Eine digitale Grand Strategy für Deutschland: Digitale Technologien, wirtschaftliche Wettbewerbsfähigkeit und nationale Sicherheit in Zeiten geopolitischen Wandels

Barker, Tyson (Ed.); Hagebölling, David (Ed.)

Veröffentlichungsversion / Published Version
Sammelwerk / collection

Empfohlene Zitierung / Suggested Citation:
Barker, T., & Hagebölling, D. (Hrsg.). (2022). *Eine digitale Grand Strategy für Deutschland: Digitale Technologien, wirtschaftliche Wettbewerbsfähigkeit und nationale Sicherheit in Zeiten geopolitischen Wandels* (DGAP-Bericht, 8). Berlin: Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-85179-8

Deutsche Gesellschaft für Auswärtige Politik e. V.

Nr. 8
November 2022

DGAP BERICHT

Eine digitale Grand Strategy für Deutschland

Digitale Technologien, wirtschaftliche Wettbewerbsfähigkeit und nationale Sicherheit in Zeiten geopolitischen Wandels

Tyson Barker
Leiter, Programm Technologie und Außenpolitik

Dr. David Hagebölling
Associate Fellow, Programm Technologie und Außenpolitik

BIOGRAPHIE DER AUTOREN

Tyson Barker ist seit Oktober 2020 bei der Deutschen Gesellschaft für Auswärtige Politik (DGAP) als Leiter des Programms „Technologie und globale Angelegenheiten" tätig. Zuvor war er bei Aspen Deutschland tätig, wo er als stellvertretender Geschäftsführer und Fellow für die digitalen und transatlantischen Programme des Instituts verantwortlich war. Davor war Barker in zahlreichen Positionen tätig, unter anderem als Senior Advisor im Büro für europäische und eurasische Angelegenheiten des US-Außenministeriums und als Direktor für transatlantische Beziehungen bei der Bertelsmann-Stiftung. Er hat für zahlreiche Publikationen auf beiden Seiten des Atlantiks geschrieben, darunter Foreign Affairs, Foreign Policy, Politico, The Atlantic, The National Interest und Der Spiegel.

Dr. David Hagebölling ist Associate Fellow im Programm Technologie und Außenpolitik der DGAP. Zudem ist er Senior Scientist am Fachgebiet Internet-Technologien und Systeme des Hasso-Plattner-Instituts (HPI). Von Mai 2021 bis Juni 2022 war Hagebölling Research Fellow bei der DGAP. Zuvor war er Gastforscher am Wissenschaftszentrum Berlin für Sozialforschung sowie der Technischen Universität München. Hagebölling sammelte außerdem professionelle Erfahrung beim Auswärtigen Amt, dem Bundesministerium für Wirtschaft und Energie sowie der Deutschen Investitions- und Entwicklungsgesellschaft. Er forscht und berät schwerpunktmäßig zu Fragen deutscher und europäischer Digital-Außenpolitik, Internet- und Cyber-Governance sowie internationaler Technologiekooperation.

DANKSAGUNG

Dieser Bericht ist das Ergebnis von einem Jahr Recherche, Diskussionen, Beratungen und Debatten mit einem breiten Spektrum von Expertinnen und Experten aus Politik, Privatwirtschaft, Think Tanks, Wissenschaft und IT in Deutschland und Europa. Wir möchten uns bei allen Personen und Institutionen bedanken, die diesen Bericht möglich gemacht haben. Unser besonderer Dank gilt den 38 Mitgliedern der Arbeitsgruppe, die sich mehrfach getroffen und uns bei der Erarbeitung der in diesem Bericht enthaltenen Aussagen und Empfehlungen beraten haben. Wir danken auch den 15 Impulsreferenten, die die Fragen, die wir in unserer Arbeit behandelt haben, umrissen haben.

Unser großer Dank gilt auch der hausinternen Unterstützung, die wir von unseren Kolleginnen und Kollegen der DGAP erhalten haben. Ihre Beiträge waren von unschätzbarem Wert für diesen Bericht. Wir schätzen die Führung und Anleitung von Dr. Guntram Wolff und Dr. Roderick Parkes in jedem Schritt dieses Prozesses. Wir möchten dem Team des Programms Technologie und Außenpolitik, bestehend aus Anke Schlieker, Anthon Klerck, Dr. Valentin Weber, Dr. Katja Muñoz und Dr. Tim Rühlig, sowie den ehemaligen Teammitgliedern Brittany Demogenes, Isabeau Höhn, Martin Kümmel, Julian Heiss, Afra Herr, Louisa Biffar, Christoph Mayer, Diego von Lieres, Jonas Winkel und insbesondere Richard Skalt für ihre Unterstützung, Recherchen und Überarbeitungen danken.

Wir danken auch Andrew Cohen, der diesen Text redigiert hat, dem DGAP-Kommunikationsteam, Wiebke Ewering, Lara Bührer, Luise Rombach und Jana Idris, für die Gestaltung dieses Berichts, und dem DGAP-Veranstaltungsteam, insbesondere Yulia Loeva, für ihre Unterstützung bei der Organisation der Workshops und der Veranstaltung anlässlich der Veröffentlichung des Berichts.

Schließlich möchten wir der Open Society Initiative for Europe für ihre Unterstützung danken, die es uns ermöglicht hat, dieses umfangreiche Projekt zu verwirklichen. Wir möchten auch dem Hasso-Plattner-Institut und seinem Direktor, Christoph Meinel, für ihre wissenschaftliche Unterstützung und Partnerschaft während dieses Projekts danken, ohne die dieser Bericht nicht möglich gewesen wäre.

EXECUTIVE SUMMARY

Deutschland erlebt eine beispiellose Phase des technologischen und geopolitischen Wettbewerbs. Inmitten des russischen Krieges gegen die Ukraine, steigender Energiepreise, von Inflation, Klimawandel und einem dringenden Bedarf an wirtschaftlichem Aufschwung und Haushaltskonsolidierung, stößt die rasante Entwicklung von Allzwecktechnologien auf einen zunehmend unerbittlichen Wettbewerb zwischen den USA und China.

Die Bundesregierung muss sich den Folgen dieser Entwicklung stellen. Um die wirtschaftlichen und technologischen Wettbewerbsvorteile des Landes zu sichern, muss sie Kapazitäten und politische Zielsetzungen im Bereich der digitalen Technologien auf nationaler und internationaler Ebene bündeln. Dafür muss Deutschland seine Doktrin der digitalen Souveränität in sechs Bausteinen verankern, die das Prinzip der „Wahlfreiheit" berücksichtigen: die Unterstützung des nationalen Innovationsumfeldes; die Förderung des offenen Wettbewerbs von Ideen und Technologien; die Festlegung eindeutiger Regeln zwecks Schaffung einer demokratischen, menschenzentrierten Ordnung; die Wiederherstellung der informationellen Selbstbestimmung der Nutzerinnen und Nutzer in Europa und weltweit; die Reduzierung von CO_2-Emissionen und Sicherung von technologischer Nachhaltigkeit sowie die Durchsetzung von angemessenen Sanktionen im Falle einer Verletzung dieser Grundsätze. Ein Ansatz des „dritten Weges" im Bereich der Digitaltechnologien – eine Äquidistanz zu den USA und China – ist für Deutschland keine Option. Deutschland und die EU sollten mit anderen gleichgesinnten Staaten, insbesondere den USA, zusammenarbeiten, um ihr kollektives Gewicht in Bezug auf Marktgröße, Marktzugang und Innovationsbasis zu nutzen. Eine solche Zusammenarbeit könnte dazu beitragen, Regeln, Werte, Wechselseitigkeit und Zugangsmöglichkeiten miteinander zu verknüpfen, die in einer demokratischen Technologie-Governance als sich gegenseitig verstärkende Instrumente wirken. Gleichzeitig muss die Bundesregierung Maßnahmen zur Stabilisierung von Deutschlands innovationsorientierter industrieller Basis ergreifen, um sich selbst – und Europa – vor Verwundbarkeit durch einen immer härteren Wettbewerb zwischen den beiden weltweit führenden Technologiemächten zu schützen.

Deutschlands Erfolg bei der Gestaltung einer digitalen Grand Strategy wird davon abhängen, ob es dem Land gelingt, eine „vernetzte Mentalität" zu schaffen, die zu einem Konsens innerhalb der Bundesregierung, zwischen politischen Entscheidungsträgerinnen und -trägern von Bund, Ländern und Kommunen sowie zwischen dem öffentlichen und privaten Sektor führt. Die Digitalstrategie von August 2022 ist zwar ein geeigneter erster Schritt hin zu konkreten, messbaren Zielen im Bereich der digitalen Modernisierung. Allerdings konzentriert sich die Bundesregierung dabei zu sehr auf innenpolitische Belange und schafft keine Grundlage, um auf kurzfristige Trends zu reagieren („der Sprint") und gleichzeitig eine strategische Weitsicht zu entwickeln, das heißt für mittelfristige Trends und deren nationale und internationale Auswirkungen zu planen („der Marathon"). Der bisherige Schritt-für-Schritt-Ansatz in der deutschen Digitalpolitik hat vier strategische Lücken zur Folge: in den Bereichen Daten, Anpassung, Investitionen und Kommerzialisierung sowie Cybersicherheit. Der deutsche Ansatz ist außerdem nach wie vor zu sehr auf die „vier Bs" bedacht: Bund-Land (Föderalismus in Deutschland), Bürokratie (IT-Konsolidierung und Digitalisierung in der Verwaltung), Breitband (Breitband- und sonstige Konnektivitätsinfrastruktur) und Bildung (digitale Bildung). Maßnahmen in all diesen Bereichen sind zwar notwendig, aber unzureichend.

Der vorliegende Bericht bietet einen systematischen Überblick über den Status quo im Bereich der Digitalpolitik und den aktuellen politischen Ansatz der Bundesregierung. Er enthält Empfehlungen, wie sich Deutschland noch stärker um den erfolgreichen Aufbau einer soliden und leistungsfähigen europäischen Digitalwirtschaft bemühen kann, die in eine offene, demokratische und regelbasierte digitale Ordnung eingebettet ist. Der Bericht unterbreitet 48 Empfehlungen in sieben aufeinander aufbauenden Politikfeldern, die ein schlüssiges Ganzes, eine Art „Technologiepolitik-Stack" darstellen. Die Empfehlungen bilden die Grundlage für einen integrierten Ansatz im Bereich der internationalen Digitalpolitik, der sich auf die sieben Ebenen dieses „Technologiepolitik-Stack" stützt. Die Empfehlungen in den folgenden Kapiteln beinhalten:

Kapitel 1

Digitale Souveränität als Deutschlands Leitmotiv im globalen Kontext

Eine klar definierte „regelbasierte" Doktrin der digitalen Souveränität unterstützen, die im Prinzip der Wahlfreiheit, offenen Märkten und Menschenrechte verankert ist. Bei der Umsetzung strategischer Technologieprojekte und Vorschriften zu Cloud-Computing, Halbleitern, 5/6G-Mobilfunknetzen muss sich die deutsche Regierung von der zunehmend kontraproduktiven Mehrdeutigkeit digitaler Souveränität lösen.

Geopolitisches Denken bei Mitarbeitenden des Ministeriums und der Referate für Digitalpolitik (insbesondere im erweiterten BMDV) verankern. Das Ministerium sollte ressortübergreifende Tagungen einführen, um geopolitische Auswirkungen zu bewerten und die geostrategischen Implikationen von digitaler und technologischer Regulierung sowie Politik zu bestimmen. Hierfür müssen auch die Rollen des Auswärtigen Amts (AA) und des Bundesministeriums der Verteidigung (BMVg) in der Technologiepolitik gestärkt werden.

Einen umfassenden Aktionsplan im Bereich Technologie und Außenpolitik vorlegen, der einen Zusammenhang zwischen der Digitalstrategie und der geplanten Nationalen Sicherheitsstrategie herstellt. Im Anschluss an die Digitalstrategie sollten das BMDV, das AA und das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) einen Aktionsplan entwerfen, der innenpolitische und europäische Fragen der Industriepolitik und der Regulierung des Technologiesektors mit außenpolitischen Fragen verknüpft, die in Bezug auf Techno-Autoritarismus, die Festlegung internationaler Standards, Internet Governance und Technologieallianzen relevant sind.

Das Amt eines Sonderbeauftragen für Technologie mit drei Stellvertreterinnen bzw. Stellvertretern einführen, die die deutsche Digital-Außenpolitik koordinieren können. Das AA sollte das Amt eines Sonderbeauftragten im Rang eines Staatssekretärs einführen, der insbesondere die Umsetzung des Aktionsplans überschaut. Dem Sonderbeauftragten sollten Stellvertreterinnen bzw. Stellvertreter für Cybersicherheit, Digitalwirtschaft und digitale Rechte zur Seite stehen, um die technologiepolitischen Ziele Deutschlands auf internationaler Ebene erfolgreich und kohärent zu vermitteln.

Den digitalen Föderalismus flexibler gestalten. Die Bundesregierung muss die Interoperabilität, die Komplementarität von Innovationen und die Bewertung der Sicherheit von Technologien zwischen Bund und Ländern stärken, um skalierbare Technologien auf europäischer und letztlich globaler Ebene aufzubauen. Entsprechende Bemühungen auf nationaler Ebene sind somit zugleich auch außenpolitisch relevant. Deutschland könnte beispielsweise einen „App Store" für digitale Instrumente in den Bereichen Bildung, Gesundheitswesen und Polizeiarbeit einrichten. Die Bundesregierung könnte auch die Auflagen bei ihren Finanzierungsanreizen für die Technologiebeschaffung durch Cyber- und Anbieterrichtlinien verstärken, die mit nationalen, EU- und NATO-Sicherheitsinteressen in Einklang stehen.

Einen ressortübergreifenden Bundestagsausschuss „Technologie- und Außenpolitik" einrichten. Ein solcher Ausschuss würde die Kohärenz der Ansätze in Politikfeldern wie Föderalismus und demokratische Technologieallianzen gewährleisten.

Kapitel 2

Stärken und Schwächen von Deutschlands digitalem Innovationsökosystem

Anreize für die Koordination zwischen innovationsfördernden Einrichtungen schaffen. Die deutschen Innovationsagenturen sollten einen nationalen strategischen Technologierat und einen offiziellen behördenübergreifenden Koordinationsprozess schaffen, um strategische Zielsetzungen zu vergleichen, potenzielle Kooperationen zu testen, Hindernisse zu ermitteln und die Erforschung von Technologien mit doppeltem Verwendungszweck und deren Anwendung zu prüfen.

Die Wechselwirkung zwischen Deutschlands sicherheitspolitischer Zeitenwende und Innovation in Dual-Use-Technologien betonen. Das im Rahmen der „Zeitenwende" angekündigte 100-Milliarden-Euro-Sondervermögen muss die Modernisierung des Verteidigungssektors mit grundlegenden Forschungs- und Entwicklungskapazitäten für Innovationen in Dual-Use-Technologien verbinden,

EXECUTIVE SUMMARY

einschließlich Verteidigungssoftware. Als Teil des Mentalitätswandels müssen Länder und Universitäten mit der Bundesregierung und dem Privatsektor an einer vernünftigen Nutzung der sogenannten Zivilklausel arbeiten.

Anreize für verlässliche Kapitalinvestitionen mit Schwerpunkt auf industriellen Plattformen, IoT (Internet der Dinge) sowie Deep Technology und umweltfreundlichen digitalen Technologien schaffen. Deutschland sollte eine Bündelung des Zukunftsfonds mit institutionellen Investitionen in einem deutschen Staatsfonds in Erwägung ziehen, wobei ein Teil der Mittel speziell strategisch wichtigen Risikokapitalvorhaben vorbehalten sein sollte.

Sandboxes, sprich geschützte Forschungsräume in öffentlich finanzierten Forschungseinrichtungen und Agenturen schaffen, die freier von Vorschriften, Bürokratie und öffentlichen Beschaffungsanforderungen sind. Forschungseinrichtungen und Innovationsagenturen würden von entsprechend angepassten Finanzierungsanforderungen des öffentlichen Sektors für die Auftragsvergabe und Ausschreibungen sowie für die Evaluierung und langfristige Planung profitieren, die mit der raschen globalen Innovation Schritt halten können.

Das Engagement des Privatsektors in „Expeditionsinvestitionen" und Übernahmen von Technologieführern und Start-ups außerhalb Europas fördern. Deutschlands führende, von der Regierung unterstützte Unternehmen müssen das Instrumentarium im Bereich der ausländischen Direktinvestitionen nutzen, um Zugang zu bahnbrechenden Innovationen, unterschiedlichen Organisations- und Managementphilosophien sowie wichtigen geistigen Eigentumsrechten zu erhalten.

Den Zugang zu Spitzenforschung und -entwicklung unter geostrategischen Gesichtspunkten betrachten. Die Bundesregierung sollte mögliche defensive Instrumente prüfen, mit denen sich die unerwünschte Weitergabe von geistigem Eigentum verhindern lässt, insbesondere im Bereich der Deep Technology. Diese Instrumente sollten allerdings weiterhin den zentralen Status Deutschlands als offener globaler Forschungsraum sicherstellen.

Den digitalen Binnenmarkt zu einer geopolitischen Priorität machen. Die Bundesregierung sollte eine führende Rolle bei der Verwirklichung des digitalen Binnenmarkts spielen, einschließlich der Bemühungen, den freien Datenfluss und sektorspezifische Datenräume in der EU zu fördern. Dies sollte auch eine vereinfachte Registrierung von Start-ups und den Aufbau eines einheitlichen Kapitalmarkts beinhalten, der grenzüberschreitende Investitionen fördert.

Die Förderung von Fachkräften in der Informations- und Kommunikationstechnologie (IKT) als kritische Infrastruktur betrachten. Forschungsinstitute müssen für die Ausstattung, Ressourcen, Forschungsinfrastruktur sowie für wettbewerbsfähige Gehälter und die nötige Flexibilität bei der Einstellung sorgen, die ihre US-amerikanische, britische und chinesische Konkurrenz bereits anbietet.

Kapitel 3

Bewahrung von Deutschlands technologischen Fähigkeiten und industrieller Stärke

Nationale Stärken und Schwächen im Bereich kritischer Technologien behördenübergreifend erfassen. Die Bundesregierung sollte in Anlehnung an die Bemühungen ihrer Partner eine behördenübergreifende Initiative starten, um drei industriepolitische Ziele auszuarbeiten: technologische Führung, Ebenbürtigkeit mit der Konkurrenz und Risikoreduzierung bei Abhängigkeiten.

Die Kohärenz der strategischen Industriepolitik zwischen Bund und Ländern sowie zwischen den Ländern selbst verbessern. Die Bundesregierung sollte sich darauf konzentrieren, dass die Industriepolitik der Länder mit den nationalen Technologiezielen im Einklang steht. Hochrangige Beamtinnen und -beamte, Forschungskonsortien und die Industrie könnten ein entsprechendes Dashboard nutzen, um Synergien zwischen Initiativen in einzelnen Forschungsbereichen und branchenübergreifend zu ermitteln und zu nutzen.

Transnationale Industriekonsortien ausbauen – in Europa und mit gleichgesinnten Partnern. Die Bundesregierung sollte grenzüberschreitende Konsortien für Innovationen fördern, indem sie sich für ein verschlanktes Verfahren zur Notifizierung bei IPCEIs (Important Projects of Common European Interest) sowie für Andock-Programme für ausländische Lieferanten aus gleichgesinnten Staaten einsetzt, um positive Spillover-Effekte zu verstärken.

Den Schwerpunkt auf nationale – und europäische – Wettbewerbsvorteile sowie strategische Interdependenzen innerhalb einer größeren Gemeinschaft gleichgesinnter Partner legen. Die Bundesregierung sollte ihre Industriepolitik so gestalten, dass sie eine größere Gemeinschaft gleichgesinnter Partner unterstützt, in deren Mittelpunkt die EU steht, die aber ebenfalls wichtige Partner wie die USA, Japan und Südkorea einschließt. Diese Gemeinschaft sollte drei Ziele verfolgen: IT-Sicherheit, die Widerstandsfähigkeit von Lieferketten und industrielle Wettbewerbsfähigkeit.

Das öffentliche Beschaffungswesen darauf ausrichten, Schwachstellen in der IT-Sicherheit und in Lieferketten zu verringern. Die Bundesregierung ist der größte Abnehmer von IT-Systemen in Deutschland und kann ihre Kaufkraft nutzen, um strategische Verwundbarkeiten zu reduzieren, insbesondere in den sicherheitskritischen Bereichen ihres Technologie-Stacks.

Kapitel 4

Gestaltung eines globalen Technologie-Regelwerks im Sinne Europas

Politische Abwägungen im Zusammenhang mit digitalpolitischen Entscheidungen adressieren. Bei den schwierigsten Aspekten der Digital-Regulierung stehen wichtige deutsche Prioritäten wie Datenschutz und Sicherheit oft im Widerspruch zueinander. Politische Entscheidungsträgerinnen und -träger müssen diese Ziele klar gegeneinander abwägen und in die Regulierung einfließen lassen.

Musterklauseln und -module erarbeiten, die in Regularien von Partnerländern integriert werden können. Es könnte ein Verzeichnis von Open-Source-Regeln geschaffen werden, das den Prozess für außereuropäische Partner beschleunigt, wenn es darum geht, Angemessenheit mit der EU in Bezug auf den Fluss personenbezogener und industrieller Daten, die IoT-Sicherheit und die Moderation von Inhalten zu erreichen und die oben erwähnten Herausforderungen mit der DSGVO zu bewältigen.

Geopolitische Folgenabschätzungen für Entwürfe deutscher und europäischer Digital-Regulierung durchführen. Maßnahmen Deutschlands und der EU können unbeabsichtigt digitalem Autoritarismus Vorschub leisten oder unerwünschte globale Trends wie Datenlokalisierung, Zensur, Schwächung von Cybersicherheit oder Internetfragmentierung begünstigen. Eine aufmerksame Bewertung der Auswirkungen der deutschen und der EU-Technologiepolitik außerhalb Europas könnte solchem Missbrauch entgegenwirken.

Dem zunehmenden Staatszentrismus bei der europäischen technischen Standardsetzung entgegentreten. Die technische Standardsetzung darf nicht allein dem Privatsektor überlassen werden. Dennoch sollte Deutschland ein akutes Interesse daran haben, ein Gleichgewicht zwischen nationalen und europäischen Interessen und der Führungsrolle des Privatsektors zu bewahren.

Die Kapazitäten des privaten Sektors in der technischen Standardsetzung stärken. Die Bundesregierung sollte steuerliche Anreize und einen Mechanismus für staatliche Förderung deutscher Unternehmen, Start-ups und Verbände schaffen, damit sie in Normungsgremien mitwirken, Vorsitze übernehmen, neue einschlägige Normen entwickeln und mit gleichgesinnten Staaten zusammenarbeiten können.

Die europäische Cloud-Zertifizierung und die GaiaX-Architektur in die globalen Cloud-Governance-Bemühungen einbetten. Da Industriedaten zu einer neuen Front in der globalen Technologieregulierung werden könnten, sollte die Bundesregierung nach Wegen suchen, das Datenraummodell Gaia-X zu internationalisieren und außereuropäische Partner, insbesondere die Vereinigten Staaten, einzubeziehen. Darüber hinaus könnte Deutschland den Aufbau von Kapazitäten in den Global Gateway-Partnerländern zur Nutzung europäischer Cloud Computing-Architekturen unterstützen, um die Interoperabilität zu erhöhen und die Menschenrechte zu wahren.

Digital-Regulierung und technische Standardsetzung in die Zeitenwende und die Nationale Sicherheitsstrategie integrieren. Die Bundesregierung muss sich intensiver mit den Auswirkungen der Regulierung digitaler Technologien auf die nationale Sicherheit und die Verteidigungsindustrie befassen. Sie muss sicherstellen, dass Deutschland in der Lage ist, Technologien mit doppeltem Verwendungszweck in vergleichbarer Weise zu übernehmen und einzusetzen wie andere Länder, etwa Frankreich, Kanada, Japan und das Vereinigte Königreich.

EXECUTIVE SUMMARY

Das Engagement der deutschen außen- und sicherheitspolitischen Gemeinschaft bei der Gestaltung und Durchsetzung von Regulierungsvereinbarungen erhöhen. Die deutschen Nachrichtendienste, die Außenpolitik, die Strafverfolgungs- und die Verteidigungsbehörden haben alle Anteil an der Durchsetzung der nationalen Technologievorschriften. Es ist an der Zeit, dass diese Behörden auch im Rahmen des post-Privacy Shield Data Privacy Framework mehr Gewicht kommen.

Multistakeholder-Ansatz unter Einbeziehung von Zivilgesellschaft, Unternehmen und anderen nichtstaatlichen Akteuren ermöglichen. Deutschland und Europa haben begonnen, neue Modelle für die Regulierung von Technologien und deren Durchsetzung zu entwickeln. Diese flexiblen Strukturen sollten weiterentwickelt werden, da sie eine ständige und kompromissfähige Aufsicht ermöglichen.

Evaluierungen und Auslaufklauseln in der digitalen Regulierung ausweiten, um Flexibilität zu fördern. Evaluierungen und Auslaufklauseln würden die Regulierungsbehörden dazu zwingen, die Wirksamkeit und Relevanz von Vorschriften zu prüfen. Solche Klauseln würden auch die Kohärenz mit der Regulierung in anderen Demokratien fördern.

Kapitel 5

Exportkontrollen, Investitionsüberwachung und Marktzugangsinstrumente optimieren

Gemeinsam mit Verbündeten einen multilateralen Ausschuss für Technologiekontrolle im 21. Jahrhundert schaffen. Dieses neue Organ, das aus dem EU-USA-Handels- und Technologierat (Trade and Technology Council, TTC) oder der G7 hervorgehen könnte, würde den Informationsaustausch und die Koordinierung von Zugangsbeschränkungen zu strategischer Technologie durch autoritäre Staaten wie Russland und China systematisieren. Zu seinen Funktionen könnte 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.

Instrumente wie die „Foreign-Direct Product Rule" und die „Entity List" in Deutschland einführen. Deutschland verfügt über zahlreiche wichtige, versteckte Hebel in Hightech-Wertschöpfungsketten. Solche Instrumente könnten Deutschland helfen, sich auf künftige potenzielle Engpässe in der Quanten- und Biotechnologie vorzubereiten – Bereiche, in denen Deutschland über wichtige Nischenfähigkeiten in der Lieferkette verfügt.

Eine handlungsorientierte politische Debatte über die Governance und Forschung von abfließenden Investitionen anstoßen. Die Bundesregierung sollte mit ihren EU- und NATO-Partnern prüfen, wie Investitionen in autokratischen Staaten besser geprüft werden können, ohne offene Märkte zu gefährden. 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 (u. a. Smart Cities, KI, Satellitentechnologie) heranziehen. Diese sollten zwischen NATO- und EU-Verbündeten, Verbündeten im Rahmen bilateraler Abkommen und konsolidierten Demokratien einerseits sowie Nicht-EU/NATO und autoritären Staaten andererseits differenzieren.

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

Kapitel 6

Internationale Allianzen, Partnerschaften und Normen im Technologiebereich stärken

Die Idee einer demokratischen Vertrauenszone („trust zone") im Bereich der digitalen Technologien vorantreiben. Diese Vertrauenszone würde den Austausch von Wissen, Kapital und Daten regeln, um die Wettbewerbsfähigkeit und die Vertrauenswürdigkeit von strategisch wichtigen IKT-Infrastrukturen wie Netzausrüstung, Cloud-/Edge-Diensten und Smart-City-Anwendungen zu steigern.

Eine globale Konnektivitätsdoktrin mit offenem Internetzugang als Grundrecht einführen. Deutschland sollte mit der EU und anderen gleichgesinnten Demokratien zusammenarbeiten, um gemeinsam finanzierte „Konnektivitätspakete" zu entwickeln, die die Entwicklung der digitalen Infrastruktur mit dem Aufbau von Cyber-Kapazitäten verbinden. Auf dem Wege der Zusammenarbeit muss zudem dafür gesorgt werden, die digitale Kluft im Globalen Süden zu verringern sowie offene Informationsflüsse während Internetsperren durch autoritäre Regime und in Konfliktgebieten aufrechtzuerhalten.

Eine deutsche Open-Tech-Stiftung gründen. Der neu eingerichtete Sovereign Tech Fund sollte durch eine deutsche Open-Tech-Stiftung ergänzt werden, um Mittel für die Entwicklung von Technologien bereitzustellen, welche die Demokratie und Privatsphäre stärken und im Einklang mit dem Verständnis von digitaler Souveränität der Bundesregierung stehen. Diese Mittel sollten vor allem Gemeinschaften im Globalen Süden zugutekommen.

Der Politisierung von Standardsetzung im Bereich kritischer und neuer Technologien entgegenwirken. Da der Anteil von Nichtmarktwirtschaftsländern in den Gremien für technische Standardisierung zunimmt, sollte Deutschland eine internationale Studiengruppe initiieren, die ermittelt, ob und welche politischen Instrumente eingesetzt werden, um die Standardsetzung im Bereich kritischer und neu entstehender Technologien zu beeinflussen. Dies sollte die Grundlage für ein koordiniertes Engagement mit den internationalen Standardsetzungs-Gremien bilden, um den Vorrang technischer Kriterien zu gewährleisten und ihren Ruf als unparteiische Institutionen zu wahren.

Das Entstehen einer digitalen „Bewegung der Blockfreien Staaten" verhindern. Die Bundesregierung hat ihren Digitaldialog mit Indien bereits 2022 wieder aufgenommen und das Land zum diesjährigen G7-Gipfel eingeladen. Mit Blick auf die G20-Präsidentschaft Indiens im Jahr 2023 sollte Deutschland nun auf seinem Engagement aufbauen und Indiens demokratische Verantwortung betonen, eine integrative digitale Agenda zu fördern, in deren Mittelpunkt klimafreundliche Technologien sowie offene und freie Konnektivität stehen.

Kooperatives Engagement im EU-US-Technologiedialog zeigen, insbesondere im TTC. Deutschland sollte einen bilateralen Digitaldialog mit den Vereinigten Staaten institutionalisieren, der die politischen Ergebnisse des TTC aufnehmen und verstärken kann.

Asymmetrische Technologieallianzen mit subnationalen Verwaltungseinheiten bilden. Städte und Bundesstaaten übernehmen zunehmend Aufgaben der digitalen Governance, die nationale Regierungen nicht übernehmen wollen oder können. Im Einklang mit den neuen Schlussfolgerungen des Europäischen Rates zur digitalen Diplomatie sollte Deutschland mit Entscheidungsträgerinnen und -trägern auf dieser Ebene zusammenarbeiten, um Technologieallianzen zu bilden, die die deutschen und EU-Werte im Bereich der Regulierung widerspiegeln und die subnationale Übernahme von Normen für die Internet- und Cyber-Governance unterstützen.

Kapitel 7

Aufkommende und disruptive Technologien, die Bundeswehr und die Zeitenwende

2 Prozent des 100-Milliarden-Euro-Sondervermögens für die Förderung disruptiver Verteidigungstechnologien bereitstellen. Die Bundesregierung sollte mindestens 2 Prozent des Sondervermögens für die Förderung disruptiver Verteidigungstechnologien bereitstellen, um Anreize für den Zufluss von Risikokapital in neue Start-ups im Verteidigungssektor und höhere FuE-Ausgaben etablierter deutscher Verteidigungsunternehmen zu setzen.

Die ethische Debatte über militärische Anwendungen von EDTs mit Einsatzrealitäten verbinden. In Deutschland werden Diskussionen rund um das

EXECUTIVE SUMMARY

Thema Ethik häufig stark abstrahiert von der Realität militärischer Einsätze geführt. Dabei sollten sich Diskussionen auf die Bestimmung eines angemessenen Maßes an maschineller Autonomie und die Festlegung von vertretbaren Zwecken für den Einsatz von EDTs konzentrieren.

Dual-Use Implikationen von EDTs mit innovationsorientierter Industriepolitik verknüpfen. Deutschlands neue Nationale Sicherheitsstrategie sollte einen Abschnitt enthalten, der die technologie- und innovationsbezogene Industriepolitik, einschließlich ihrer für die Verteidigung relevanten Aspekte, zusammenführt – und zwar im Rahmen einer regierungsübergreifenden Bewertung zentraler Bedrohungen für die nationale Sicherheit.

Wissenstransfer zwischen militärischer und ziviler FuE verbessern. Die Bundesregierung sollte das Münchner Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw) stärker mit den bayerischen Hightech-Start-ups vernetzen. Zudem sollte sie eine separate Track-II-Plattform einrichten, die Innovatoren bei der Entdeckung von Dual-Use-Anwendungen von EDTs unterstützt, welche mit der Förderung von Innovationsagenturen wie SPRIND und dem Cyber Innovation Hub entwickelt wurden. Außerdem sollte sie Anreize für deutsche und europäische Risikokapitalinvestitionen in Start-ups im Bereich der Verteidigungstechnologie setzen, etwa durch Ko-Finanzierungen.

Die Beschaffung von Verteidigungsgütern an technologische Innovationszyklen anpassen. Schwankungen im Verteidigungshaushalt erschweren die Unterstützung längerer EDT-Innovationszyklen. Die Regierung sollte einen bis 2030 laufenden SpezialFonds für disruptive Verteidigungstechnologien mit jährlichen Mindestbudgetgarantien einrichten.

Die Interoperabilität mit Verbündeten durch gemeinsame Grundsätze und militärische Formationen aufrechterhalten. Die Bundesregierung muss sicherstellen, dass die EDT-bezogene Transformation der Bundeswehr nicht die Interoperabilität mit verbündeten Streitkräften untergräbt. Sie sollte die Entwicklung gemeinsamer ethischer Grundsätze und Verhaltenskodexe fördern, wie etwa in der KI-Strategie der NATO geschehen.

KAPITELÜBERSICHT

Sprint und Marathon

Der geopolitische Wettbewerb zwischen etablierten und aufstrebenden Mächten, Demokratien und autoritären Systemen – und auch zwischen regelorientierten Multilateralisten und machtbasierten Unilateralisten – hat zu einer deutlichen Zunahme der Instrumentalisierung von Abhängigkeiten geführt.[1] Deutschland und Europa sind mit einer neuen Realität konfrontiert: Der Zugang zu und die Kontrolle über Knotenpunkte und Engpässe in den Bereichen Handel, Finanzen, Energie, Rohstoffe, oligarchische Netzwerke und sogar Nahrungsmittel werden als Instrumente eines globalen Konflikts niedriger Intensität eingesetzt.

Dies trifft insbesondere auf technologische Konnektivität zu. Die USA, China und ihre Big-Tech-Partner, unter anderem in den Bereichen KI, Cloud-, Plattform- oder Chip-Technologie, haben die Kontrollhoheit über wichtige Knotenpunkte. Der zunehmend universelle Charakter bestimmter grundlegender Technologien im Hinblick auf die wirtschaftliche, politische und militärische Wettbewerbsfähigkeit macht diese Situation für Deutschland und Europa noch gefährlicher.

Vor diesem Hintergrund bemüht sich Deutschland seit einiger Zeit um einen ressortübergreifenden Ansatz im Bereich der digitalen Technologie. Im August 2022 hat sich das Bundeskabinett auf eine erste deutsche Digitalstrategie verständigt. Das vom BMDV erarbeitete Dokument konzentriert sich auf drei Aktionsbereiche: eine vernetzte und digital souveräne Gesellschaft; innovative Wirtschaft, Arbeitswelt, Wissenschaft und Forschung; und den digitale Staat. Die Strategie beinhaltet auch einige „Hebelprojekte", insbesondere in puncto Normen und Standards, Datenverfügbarkeit und digitale Identitäten.[2]

Doch auch wenn sich die Bundesregierung mit ihrer Digitalstrategie der Notwendigkeit stellt, das ministerielle Silodenken zu überwinden und die Privatwirtschaft in einen politischen Ansatz für digitale Technologien einzubinden, scheinen ihr die geopolitischen Bedrohungen, denen sich Deutschland bereits heute stellen muss, zu sehr aus dem Blickfeld geraten zu sein.[3] Zudem gelingt es der Regierung in ihrer Digitalstrategie noch nicht, technologische Trends zu erkennen und sich im Einklang mit ihren politischen Zielen auf diese vorzubereiten (siehe Abbildung 1). Die zurückhaltenden digitalpolitischen Strategien der letzten deutschen Regierungen konzentrierten sich vor allem auf kurzfristige Anliegen im Digitalbereich. Sie erwiesen sich als ungeeignet, Herausforderungen wie die Auswirkungen neuer Technologien auf die Innovationslandschaft, die industrielle Basis und ein durch Technologie, wirtschaftlichen Wettbewerb, Ideologie und Sicherheit eng verwobenes internationales System zu bewältigen. Als solche haben diese Maßnahmen erschwert, dass Deutschland mittelfristig wichtige technologische Trends erkennen und mitgestalten kann.

Darüber hinaus zeichnete sich die deutsche Digitalpolitik bisher häufig durch geografische Kurzsichtigkeit aus, da sie stark auf das Inland ausgerichtet war. Digitalstrategie 2022 muss dabei zugutegehalten werden, dass sie eine ausschließliche Fixierung auf die Infrastruktur, die die Digitalisierung ermöglicht, überwinden will und die folgenden Bereiche, die vier „Bs", in den Vordergrund stellt:

Bund-Land (Föderalismus): Ausarbeitung einer Vereinbarung zwischen Bund und Ländern über interoperable Genehmigungsverfahren, die Standardisierung von IT-Schnittstellen und die Multi-Cloud-Strategie in der Verwaltung

Bürokratie (IT-Konsolidierung und Digitalisierung in der Verwaltung): Behördenportale für eingereichte Unterlagen, die bis 2025 mit EU-Systemen kompatibel sein werden; Ausarbeitung einer Deutschen Verwaltungscloud-Strategie (DVS) und Festlegung von Kriterien für nachhaltige Rechenzentren auf der Grundlage sicherer und idealerweise Open-Source-Software sowie von Standards für die Beschaffung von Datenspeichern; e-ID-Standards; öffentlich zugängliche Daten und Umsetzung des Online-Zugangsgesetzes (OZG)

1 Henry Farrell and Abraham L. Newman, „Weaponized Interdependence: How Global Economic Networks Shape State Coercion", in: International Security, 44, no. 1 (Juli 2019), S. 42-79: https://direct.mit.edu/isec/article-abstract/44/1/42/12237/Weaponized-Interdependence-How-Global-Economic?redirectedFrom=fulltext (abgerufen am 5. Oktober 2022).

2 Bezeichnenderweise wurde kein eigener Haushalt für die Umsetzung der Strategie vorgesehen.

3 Beispielsweise wird China in dem 52 Seiten langen Dokument nur ein einziges Mal erwähnt. Bundesministerium für Digitales und Verkehr, „Digitalstrategie. Gemeinsam digitale Werte schöpfen", (2022): https://digitalstrategie-deutschland.de/static/1a7bee26afd1570d3f0e5950b215abac/220830_Digitalstrategie_fin-barrierefrei.pdf (abgerufen am 5. Oktober 2022).

Breitband (Breitband- und sonstige Konnektivitätsinfrastruktur): Ausweitung der 7,5 Millionen Glasfaseranschlüsse in Deutschland auf ländliche Regionen im Rahmen des Weiße-Flecken-Förderprogramms; lückenloses Mobilfunknetz im ländlichen Raum und entlang der Bahnstrecken; erweiterte Frequenzlizenzen; ein Gigabit-Grundbuch (Gigabit-Register mit Informationen zur Erweiterung der digitalen Infrastruktur) mit klaren Vorgaben für den Ausbau der IKT-Infrastruktur

Bildung (digitale Bildung): Digitalpakt 2.0 bis 2030 mit Cloud- und Software-Tools in einer sogenannten Nationalen Bildungsplattform, die auf Gaia-X und Hardware-Wartung basiert, aufbauend auf den digitalen Tools der einzelnen Bundesländer

Auch wenn all diese Maßnahmen notwendig sind, muss klar werden, dass ein auf diesen vier Bs basierender Ansatz unzureichend ist. Die Bundesregierung muss – in Zusammenarbeit mit der Privatwirtschaft, den Forscherinnen und Forschern im Land sowie der Zivilgesellschaft – ihre Fähigkeit stärken, kurzfristige technologische Entwicklungen zu erkennen und schnell auf diese zu reagieren. Stichwort: „Sprint". Gleichzeitig muss sie eine strategische Weitsicht entwickeln, um für mittelfristige Trends und deren Auswirkungen zu planen. Stichwort: „Marathon". Beides miteinander in Einklang zu bringen, stellt die Politik zweifellos vor Herausforderungen. Wenn sie die kurzfristigen Probleme in den Vordergrund stellt, könnte das zu einer unzureichenden Planung im Digitalbereich führen. Schenkt sie jedoch den mittelfristigen Risiken mehr Aufmerksamkeit, besteht die Gefahr, dass sie die erforderlichen Schritte übersieht, um unverzüglich zu reagieren.

Das Spannungsverhältnis zwischen kurzfristiger und langfristiger technologischer Entwicklung wird auch in den Strategien der deutschen Privatwirtschaft im Digitalbereich deutlich. Dadurch liegt Deutschland in vier Bereichen hinter seinen internationalen Partnern zurück und muss dringend aktiv werden:

Datenlücke: Studien zu den direkten Auswirkungen der DSGVO und anderer Datenschutzvorschriften auf die Innovation in Europa lassen keine eindeutigen Schlüsse zu. In einigen Fällen hat die Verordnung eine Minderung der Verfügbarkeit von Daten und ihrer Verarbeitung zur Folge. In anderen Fällen eröffnet sie neues Innovationspotenzial.[4] Allerdings ist der Umfang der Datenmärkte in Europa im Vergleich zu anderen demokratischen Staaten wie den USA begrenzt. Diese Tendenz könnte sich zudem durch die Bemühungen um mehr Datenlokalisierung – innerhalb der EU und weltweit – weiter verschärfen. Als vielversprechend können das Streben nach mehr Datenaltruismus auf europäischer Ebene (im Rahmen des Datengesetzes und des Daten-Governance-Gesetzes), die Freigabe öffentlicher Daten für kommerzielle Zwecke und die Förderung von Datenräumen in Bereichen wie Gesundheit und Mobilität gewertet werden. Doch bisher bleibt es nur bei derartigen Plänen. Zudem stößt der Datenaustausch auf kulturell bedingte Hindernisse.

Anpassungslücke: In der deutschen Industrie, insbesondere im Mittelstand und bei kleinen Unternehmen, kommt es weiterhin zu Verzögerungen bei der Einführung von Cloud-Services, die zunehmend den Zugang zur industriellen Digitalisierung und zu Plattformen sicherstellen, auf denen weitere digitale Dienstleistungen in den Bereichen KI, Cybersicherheit und Datenanalysen angeboten werden.[5] Bei der Cloud-Einführung rangiert Deutschland auf Platz 20 aller 27 EU-Mitgliedstaaten.[6] Dass die deutsche Industrie keine größeren Nachteile durch die verzögerte Einführung der ursprünglichen Software- und Internetrevolution zu spüren bekam, war darauf zurückzuführen, dass sie ihre weltweite Wettbewerbsfähigkeit durch ihre Nischenfähigkeiten bewahren konnte. Und doch sind mit den potenziellen Auswirkungen neuer Technologien, die sich in den einzelnen Branchen langsam bemerkbar machen, grundlegende – wenn nicht sogar existenzielle – Gefahren für einige Geschäftsmodelle verbunden.

Investitions- und Kommerzialisierungslücke: Die Bundesregierung plant FuE-Investitionen in Höhe von 3,5 Prozent des BIP. Außerhalb Europas kommen die meisten Mittel für FuE im Bereich neuer Technologien aus der Privatwirtschaft. Die Hälfte der wichtigsten privaten Investoren im Bereich Quantencomputing stammen aus den USA, 40 Prozent aus China, kein einziger dagegen aus Europa. In Europa werden lediglich 12 Prozent, in den USA 40 Prozent und in

4 Crispin Niebel, „The impact of the general data protection regulation on innovation and the global political economy", in: Computer Law & Security Review, (April 2021), S. 1-15: https://www.sciencedirect.com/science/article/abs/pii/S026736492030128X (abgerufen am 5. Oktober 2022).

5 Tyson Barker, „Into the clouds: European SMEs and the Digital Age", Atlantic Council, (Oktober 2016): https://www.atlanticcouncil.org/wp-content/uploads/2016/10/Into_the_Clouds_web_1011.pdf (abgerufen am 5. Oktober 2022).

6 European Commission, „Digital Economy and Society Index (DESI) 2021 Integration of digital technology", SCRIBD: 3_DESI_2021_Thematic_chapters__Integration_of_digital_technology_umQXbSLQ9FpmtmS8rGgaTi7AKcg_80555.pdf (abgerufen am 5. Oktober 2022).

1 – ENTWICKLUNG DIGITALER TECHNOLOGIEN: DEUTSCHLAND MUSS SOWOHL KURZ- ALS AUCH MITTELFRISTIG PLANEN

„DER SPRINT“ (AKTUELL UND KURZFRISTIG)	„DER MARATHON“ (MITTEL- BIS LANGFRISTIG)
Begrenzte KI: Einsatz von KI, die sich auf einzelne, klar definierte Aufgabenbereiche beschränkt	Breite Anwendung hochpräziser KI-Algorithmen auf dem Weg zu Allgemeiner Künstlicher Intelligenz – der Fähigkeit, die gleichen Aufgaben auszuführen, die auch ein Mensch ausführen kann
Internet der Dinge (IoT): Kommunikation von Maschine zu Maschine (M2M), Mensch zu Maschine; umfangreichere Nutzung von industriellen Daten	Biometrische Verfahren: größere Verschmelzung von personenbezogenen und nicht-personenbezogenen Daten; Verbindung von Mensch und Maschine mit der digitalen Welt
5G: fortgeschrittenes IoT; Smart City, Smart Factory und Smart Home; führerloses Fahren, Krisenmanagement und prädiktive Analyse	6G: Immersive Augmented Reality/Virtual Reality (Metaversum) und Nutzung von Hologrammen
Vormachtstellung von US-amerikanischen Big-Tech-Unternehmen in Europa	Die Präsenz von chinesischen und US-amerikanischen Big-Tech-Unternehmen in Europa
Oligopolistische, datengesteuerte Plattformmodelle: gezielte Werbung und Data Mining; potenzielle Content-Atomisierung auf Social-Media-Plattformen / geschlossene Messaging-Dienste und Gruppen	Diversifizierung von Plattformmodellen: weniger vom Westen dominierte Plattformen; vom E-Commerce angetriebene digitale Währung (Möglichkeit für staatliche Überwachung)
Hyperscaler-Cloud-Computing	Fusion von Cloud- und Edge-Computing mit der Telekommunikationsinfrastruktur
Brüssel-Effekt: Größe des EU-Marktes als Grundlage für regulatorischen Einfluss (BIP der USA im Verhältnis zum globalen BIP: 23 Prozent im Jahr 2010, 25 Prozent im Jahr 2020; BIP der EU im Verhältnis zum globalen BIP: 21,5 Prozent im Jahr 2010 und 17,1 Prozent im Jahr 2020)	Beschränkte ordnungspolitische Vorherrschaft der EU aufgrund des Rückgangs des relativen BIP
Unterseekabel; LEO-Satelliten-Netzwerke (Low Earth Orbit) und VSAT-Empfänger (Very Small Aperture Terminal; ein kleiner Satellitenempfänger und -sender)	Dezentralisierte Distributed-Ledger-Technologie (Web3); Quanteninternet
High-Performance-Computing	Exascale-Computing: Digital Twin; hyperkomplexe synthetische Realität
Globales Internet (Anwendungs- und Protokollschichten): Domainnamen-System; Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN)	Splinternet: Chinas 6G-Internet-Neugestaltung, um dem Internet „inhärente Sicherheit“ zu verleihen; Internet Governance Forum + (IGF+) 2025; Weltgipfel zur Informationsgesellschaft (WSIS+20)

Quelle: Darstellung der Autoren

Asien 32 Prozent der weltweiten privaten Investitionen in KI getätigt.[7] Das Missverhältnis im Bereich der Kommerzialisierung liegt auf der Hand: Europa ist bei Patenten nur in zwei von zehn Schlüsseltechnologien führend.[8] Und dies, obwohl sich die Grundlagenforschung in Europa, mit Deutschland an der Spitze, auf Augenhöhe mit den USA und China bewegt.[9]

Cyber-Lücke: Die Zahl der Sicherheitsvorfälle in deutschen IT-Systemen – darunter IP-Diebstahl, Angriffe mit Schadprogrammen auf Kommunen und Krankenhäuser, politische motivierte Hackerangriffe wie 2021 auf den Deutschen Bundestag[10] und unbeabsichtigte Kollateralschäden[11] – haben seit der Pandemie zugenommen. Die Angriffe durch staatliche Akteure wie China und Russland und durch staatsnahe und nicht-staatliche Akteure werden immer zahlreicher und ausgefeilter. Deutschland hat sich an vorderster Front um die Erarbeitung von Cyber-Kontrollen und -Standards bemüht, um Vorkehrungen für die sich verändernde Bedrohungslandschaft zu treffen.[12] Im Rahmen der EU verweist Deutschland auf die möglichen Folgen – von Sanktionen bis hin zu Attribuierung – derartiger Angriffe gemäß der Cyber Diplomacy Toolbox. Außerhalb der EU hat der norwegische Staatsfonds festgestellt, dass Cybergefahren eine wichtige Ursache für systemische wirtschaftliche Risiken darstellen.[13]

In jedem dieser vier Bereiche hat sich bisherige Herangehensweise („Schritt-für-Schritt") als ungeeignet erwiesen, Herausforderungen wie die Auswirkungen neuer Technologien auf die Innovationslandschaft und Industrie des Landes zu bewältigen, ebenso wenig wie die Auswirkungen eines internationalen Systems, in dem Technologie, wirtschaftliche Wettbewerbsfähigkeit, nationale Sicherheit, und zunehmend auch ideologische Belange, untrennbar miteinander verwoben sind. Hier kann Deutschland nur erfolgreich sein, wenn es endlich eine solide, leistungsfähige europäische Digitalwirtschaft aufbaut, die in eine offene, demokratische und regelbasierte digitale Ordnung eingebettet ist. Dies ist besonders wichtig, weil sich die Risiken einer Fragmentierung des Internets, von Datenlokalisierung und einer zunehmenden Rolle von Technologien beim Export von Governance-Modellen erhöhen. Zudem ist es wichtig, da digitale Abhängigkeit zunehmend als Schwachstelle für geopolitische Ziele genutzt wird.

7 Sven Smit et. al, „Securing Europe's competitiveness: Addressing its technology gap", McKinsey Global Institute Report, (22. September 2022): https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/securing-europes-competitiveness-addressing-its-technology-gap (abgerufen am 5. Oktober 2022).

8 Jan C. Breitinger, Benjamin Dierks und Thomas Rausch, „World class patents in cutting-edge technologies: The innovation power of East Asia, North America, and Europe", Bertelsmann Stiftung, (3. Juni 2020): https://www.bertelsmann-stiftung.de/en/publications/publication/did/world-class-patents-in-cutting-edge-technologies (abgerufen am 26. Oktober 2022).

9 Insgesamt 18 Prozent der weltweiten KI-Forschenden arbeiten in der EU. Sie haben etwa 15.000 wissenschaftliche Artikel zu diesem Thema publiziert; in den USA sind 20 Prozent der weltweiten KI-Forschungsgemeinschaft ansässig. Kaan Sahin und Tyson Barker, „Europe's Capacity to Act in the Global Tech Race Charting a Path for Europe in Times of Major Technological Disruption", DGAP Bericht Nr. 6, Deutsche Gesellschaft für Auswärtige Politik (April 2021): https://dgap.org/sites/default/files/article_pdfs/210422_report-2021-6-en-tech.pdf (abgerufen am 5. Oktober 2022).

10 Der Spiegel, „EU wirft Russland vor Bundestagswahl gezielte Cyberangriffe vor" (24. September 2021): https://www.spiegel.de/netzwelt/netzpolitik/eu-wirft-russland-vor-bundestagswahl-gezielte-cyberangriffe-vor-a-9ee768d4-007a-418c-9bdc-f99e4cd590b0 (abgerufen am 5. Oktober 2022).

11 Maria Sheahan, Christoph Steitz and Andreas Rinke, „Satellite outage knocks out thousands of Enercon's wind turbines", Reuters, (28. Februar 2022): https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/ (abgerufen am 5. Oktober 2022).

12 Dies gilt in vielen Bereichen, vom IdD über Router bis hin zu den jüngsten Cyber-Leitlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) für LEO-Satelliten. Catherine Stupp, „Germany Offers Model for Space-Industry Cybersecurity Standards", The Wall Street Journal, (17. August 2022): https://www.wsj.com/articles/germany-offers-model-for-space-industry-cybersecurity-standards-11660728604 (abgerufen am 5. Oktober 2022).

13 Adrienne Klasa und Robin Wigglesworth, „Norway's oil fund warns cyber security is top concern", Financial Times, (22. August 2022): https://www.ft.com/content/1aa6f92a-078b-4e1a-81ca-65298b8310b2 (abgerufen am 26. Oktober 2022).

Digitale Souveränität als Leitmotiv im globalen Kontext

Um die vier Lücken zu schließen und die kurz- und mittelfristige technologische Entwicklung zu bewältigen, muss Deutschland in einem integrierten Ansatz seine Kapazitäten und Zielsetzungen auf nationaler und internationaler Ebene in einem technologiepolitischen Rahmen bündeln. Eine solche integrierte Strategie erfordert die Aufmerksamkeit und Unterstützung von Vertreterinnen und Vertretern aller politischen Institutionen, einschließlich des Bundestages, der Ministerien, der EU, der Länder, von etablierten Unternehmen sowie Start-ups des Privatsektors und anderen Partnern in Europa und über den Kontinent hinaus. Nur so lassen sich gemeinsame Ziele und Strategien entwickeln.[14]

Deutschland muss seinen Partnern wie auch seinen Gegnern ein klares Verständnis von seiner internationalen Digitalpolitik als umfassendes Ganzes vermitteln. Diese Politik sollte auf die Rolle als führender EU-Mitgliedstaat ausgerichtet sein und sich auf sechs Bausteinen stütze, die auf dem Prinzip der **„Wahlfreiheit“** basieren:[15]

Unterstützung eines starken Innovationsumfelds. Im Rahmen der Strategie sollten stärkere Verbindungen geschaffen werden zwischen staatlich geförderter FuE, Kommerzialisierung und Industriepolitik in neu entstehenden Technologiebereichen wie KI, Quantencomputing, fortschrittliche Chips und Cloud Computing.

Förderung des offenen Wettbewerbs von Ideen und Technologien. Digitalpolitik sollte Lock-in-Effekte vermeiden und gleichzeitig eine Diversifizierung der Anbieter unterstützen, um die Versorgungssicherheit bei kritischen Technologien und der Beschaffung von Rohstoffen zu erhöhen. Sie sollte strategische Interdependenzen mit gleichgesinnten Staaten schaffen, den pragmatischen Einsatz von Open-Source-Software fördern, die Interoperabilität proprietärer Systeme fordern und einen Bottom-up-und Multistakeholder-Ansatz mit mehreren Interessengruppen bei der Festlegung von Standards priorisieren.

Festlegung eindeutiger Regeln, die eine demokratische, menschenzentrierte Ordnung schaffen. Digitalpolitik sollte die Inhaltsmoderation, die Marktmacht von Online-Plattformen, von Industriedaten, Cybersicherheit, Cloud-Regeln und KI regeln, um das digitale Vertrauen der Europäerinnen und Europäer zu stärken und ein globales Modell zu schaffen. Sie muss die Fähigkeiten Deutschlands und Europas erneuern, technische Standards zu setzen.

Wiederherstellung der informationellen Selbstbestimmung der Userinnen und User in Europa und weltweit. Digitalpolitik sollte den Datenschutz, die Ende-zu-Ende-Verschlüsselung und die Inhaltsmoderation fördern, ohne die Meinungsfreiheit wesentlich einzuschränken. Sie muss Wahlfreiheit als Leitprinzip der IKT-Infrastrukturzusammenarbeit mit den westlichen Balkanstaaten, den Ländern der Östlichen Partnerschaft und des Globalen Südens unterstützen.

Reduzierung von CO_2-Emissionen und Gewährleistung von technologischer Nachhaltigkeit. Digitalpolitik sollte den Einsatz neuer Technologien fördern, die „Green by Design“ sind und bei denen die CO_2-Reduzierung im Mittelpunkt steht. Derartige Technologien umfassen modernste Chips und Edge-Computing, energieeffiziente Algorithmen, KI-gestützte Energieoptimierung im IoT sowie Quantentechnologie für eine nachhaltige Landwirtschaft.

Durchsetzung von angemessenen Sanktionen im Falle einer Verletzung dieser Regeln. Digitalpolitik sollte angemessene Sanktionen, Investitionsbeschränkungen, Exportkontrollen und den Verlust des Zugangs zu geistigem Eigentum, Daten und Märkten gegenüber Staaten und Technologieunternehmen, einschließlich Gatekeeper-Plattformen, Telekommunikations- und Internetdienstleistern und Hardware-Anbietern und Messenger-Diensten vorsehen, wenn diese gegen Regeln verstoßen.

14 Katrin Suder, „Staat-up“, TAE Advisory & Sparring GmbH, (22. Juli 2021): https://www.linkedin.com/pulse/staat-up-katrin-suder/?trk=articles_directory&originalSubdomain=de (abgerufen am 21. Februar 2022).

15 Henning Kagermann, Karl-Heinz Streibich und Katrin Suder, „Digitale Souveränität: Status quo und Handlungsfelder“ acatech IMPULSE, (25. März 2021), S. 9: https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder (abgerufen am 12. April 2022).

Ein solches Vorgehen ist weniger naheliegend, als es scheint. In den letzten Jahren hat die EU zwischen zwei Konzepten der digitalen Souveränität einen Ausgleich gesucht und mitunter tiefe innere Spannungen zwischen den Mitgliedstaaten über die strategische Ausrichtung in diesem Bereich überspielt. Der regelzentrierte Ansatz[16] baut auf der ordoliberalen Tradition auf und beruht auf einer starken Unterstützung des Wettbewerbs, einer klar definierten Regulierung, Grundrechten und offenen Märkten. Er lehnt die auf Netzwerkeffekten basierende Kartellbildung, Lock-in-Effekte und Hindernisse für grenzüberschreitende digitale Dienstleistungen ab.[17] Diese Auffassung beruht auch auf einem mehrdimensionalen Verständnis von Souveränität, das die Selbstbestimmtheit des Staates, von Institutionen und Einzelpersonen wahrt. Einige Partner Deutschlands – insbesondere Frankreich und Teile der Europäischen Kommission – befürworten jedoch einen Ansatz mit einer mehr auf die Marktteilnehmenden ausgerichteten, interventionistischen Vorstellung von digitaler Souveränität, die technologische importsubstituierende Industrialisierung (ISI), protektionistische Maßnahmen und Datenlokalisierung innerhalb Europas hervorhebt.[18]

Beide Vorstellungen von digitaler Souveränität beruhen im Kern darauf, den europäischen digitalen Binnenmarkt zu verwirklichen und die Skalierbarkeit in ganz Europa zu gewährleisten. Beide sehen die Stärkung der inländischen Innovationskapazitäten und die Verringerung externer Schwachstellen als strategisches Ziel an. Außerdem unterstreichen beide die Rolle des Staates bei der Gestaltung der IKT-Umgebung. Doch solange beide Traditionen in Europa bestehen – und zentrale Konflikte und Widersprüche unter den Teppich gekehrt werden – kann es sein, dass wichtige strategische Entscheidungen im Rahmen von Konsensbildung verzögert werden.

EIN „DRITTER WEG" ODER EINE DEMOKRATISCHE TECHNOLOGIE-GOVERNANCE MIT DER EU UND DEN USA IM ZENTRUM?

Die Frage, wie Deutschland und die EU die digitale Souveränität als Rahmen interpretieren, wirkt sich unmittelbar auf die digitale Grand Strategy der EU und ihre strategische Positionierung aus. Politikerinnen und Politiker ordnen den europäischen Ansatz zur digitalen Technologie manchmal als selbständigen geopolitischen „dritten Weg" zwischen einem eher liberalen, „amerikanischen" Ansatz für Technologie-Governance und dem chinesischen Techno-Autoritarismus ein. Doch ein solcher Ansatz in der Digitalpolitik birgt zwei strategische Nachteile.

Erstens stärkt er eine Vorstellung von digitaler Souveränität, die sich auf die inländische Lokalisierung von Daten, sozialen Medien, digitalen Diensten und strategischen Technologien konzentriert, um die Industrialisierung und politische Kontrolle zu fördern. Dieser Ansatz könnte autoritäre Vorstellungen von digitaler Souveränität legitimieren wie sie Russland und China vertreten, die es einem starken, zentralisierten Staat erlauben, alle Lebensbereiche zu durchdringen, um die Ordnung aufrechtzuerhalten. Er könnte auch einen globalen digitalen Merkantilismus begünstigen, der die Welt in Einflusssphären im Bereich digitaler Dienstleistungen und Daten unterteilt, die europäische Regeln und Akteure aus anderen geografischen Regionen ausschließen könnten.

Zweitens kann der Ansatz des sogenannten dritten Weges die Wahlfreiheit einschränken, indem er die Nutzung von Technologien, Daten und digitalen Dienste begrenzt, die sowohl den Nutzerinnen und Nutzern als auch einer innovativen industriellen Basis zugutekommen. Die weltweite Tendenz zu Datenlokalisierung, einem Splinternet und geschlossenen Technologieplattformen, die in regionale oder nationale Einflussbereiche eingeteilt sind, sollte den europäischen politischen Verantwortlichen zu denken

16 Angela Merkel brachte in ihrer Amtszeit als Bundeskanzlerin dieses weithin akzeptierte Verständnis auf dem Internet Governance Forum (IGF) 2019 auf den Punkt, als sie sagte: „Nach meinem Verständnis bedeutet digitale Souveränität nicht Protektionismus oder Vorgabe von staatlichen Stellen, was an Informationen verbreitet werden kann – also Zensur –, sondern beschreibt vielmehr die Fähigkeit, sowohl als Individuum als einzelne Person, als auch als Gesellschaft die digitale Transformation selbstbestimmt gestalten zu können." Die Bundesregierung bekräftigte diesen Gedanken 2021 erneut in einem Brief, der auch von den Staats- und Regierungschefs von Dänemark, Estland und Finnland unterzeichnet wurde.
Angela Merkel et. al, „Joint letter to the EU President on Digital Sovereignty", Politico, (1. März 2021): https://www.politico.eu/wp-content/uploads/2021/03/01/DE-DK-FI-EE-Letter-to-COM-President-on-Digital-Sovereignty_final.pdf (abgerufen am 5. Oktober 2022).

17 Henning Kagermann, Karl-Heinz Streibich und Katrin Suder, „Digitale Souveränität: Status quo und Handlungsfelder" acatech IMPULSE, (25. März 2021), S. 8: https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/ (abgerufen am 12. April 2022).

18 Ministère de l'Europe et des Affaires étrangères, „Building Europe's Digital Sovereignty", (7. Februar 2022): https://www.diplomatie.gouv.fr/en/french-foreign-policy/europe/the-french-presidency-of-the-council-of-the-european-union/article/building-europe-s-digital-sovereignty-7-feb-22 (abgerufen am 22. Februar 2022).

geben. Ihre Amtskollegen in Neu-Delhi reagieren bereits auf diesen Trend und fordern einen „vierten Weg“ für Indien.[19] Andere aufstrebende Digitalmächte könnten diesem Beispiel folgen. Wenn die Welt von einem regional zersplitterten Internet geprägt wäre und dem digitalen Merkantilismus verfiele, würde Europa mit seiner Abhängigkeit von digitalen Diensten aus den USA sowie ostasiatischer Hardware neben anderen Nationen noch weiter als bisher zurückfallen, wenn es darum geht, eigene Kapazitäten in Bereichen wie IoT, dem industriellen Internet der Dinge (IIoT) und neue Technologien wie Quantencomputing, Blockchain und KI auszubauen. Außerdem könnte dies einen digitalen Protektionismus befördern, der weitere offene Märkte ausschließt und durch den Deutschland und die EU möglicherweise Zugangsmöglichkeiten, Innovationspotenzial und Governance-Partner verlieren.

All dies bedroht Deutschlands – und Europas – digitale Souveränität, die auf universellen Prinzipien aufbauen muss, um sich zu behaupten. Digitale Souveränität muss die Emanzipation des Einzelnen in einem globalen, demokratischen Wertesystem in den Mittelpunkt stellen, auch wenn sie darauf abzielt, die deutsche und europäische technologische Wettbewerbs und Widerstandsfähigkeit zu stärken.

Zu diesem Zweck sollten Deutschland und die EU mit anderen gleichgesinnten Staaten – insbesondere den USA – zusammenarbeiten, um ihr kollektives Gewicht in Bezug auf Marktgröße, Technologiezugang und Innovationskapazität zu nutzen. Eine solche Zusammenarbeit könnte auch zur Offenheit beitragen, indem sie Regeln, Werte, Wechselseitigkeit und Zugangsmöglichkeiten miteinander verknüpft, die in einer demokratischen Technologieordnung als sich gegenseitig verstärkende Instrumente wirken.[20]

Zusammenfassend ist ein Paradigma des „dritten Wegs“ im Sinne einer Äquidistanz zwischen den USA und China für Deutschland keine Option. Doch unabhängig von der Zusammenarbeit mit Partnern, in erster Linie den USA, muss Deutschland auch Maßnahmen zur Stabilisierung seiner Technologie-Industrie ergreifen, um sich selbst – und Europa – vor Verwundbarkeit durch einen immer härteren Wettbewerb im Technologiesektor zu schützen, in dem Europa eine führende Rolle übernehmen will. Dazu gehören auch die Entwicklung neuer Instrumente der gegenseitigen Unterstützung, für den Marktzugang, die Bildung von Technologieallianzen und eine Neuausrichtung der Forschung und Entwicklung auf Allzwecktechnologien.

ZWECKGERECHTE POLITISCHE ENTSCHEIDUNGSSTRUKTUREN

Bisher hat die Abgrenzung von Politikfeldern und die breite Verteilung von Zuständigkeiten auf verschiedene Ministerien eine wirksame Koordinierung von Maßnahmen erschwert, die FuE, Industriepolitik, Regulierung und Werte auf kohärente Weise miteinander verbinden, um die wirtschaftliche Wettbewerbsfähigkeit, nationale Sicherheit und demokratische Werte in Deutschland zu fördern. Die Bundesregierung will mit Hilfe ressortübergreifender Reformen bisherige strukturelle Schwächen überwinden, um sowohl die Politik als auch die Haushaltsplanung im Digitalbereich zu optimieren (siehe Abbildung 2). Da es jedoch die Interessen von drei Parteien zu berücksichtigen galt, hat die Ampelkoalition die Zuständigkeiten für Technologie aufgeteilt, sodass sie nun breiter gestreut sind als in früheren Regierungen. Das Ergebnis – so wie es im Koalitionsvertrag steht – dürfte mit erheblichen Hürden für die Entwicklung einer klaren Vision von der digitalen Transformation Deutschlands – und damit von einer starken internationalen Position des Landes im globalen Technologiewettbewerb – verbunden sein.

Das BMWK steuert die digitale Wettbewerbspolitik. Auch das Bundeskartellamt gehört zu seinem Geschäftsbereich. Es überwacht die Einhaltung des Gesetzes über Digitale Märkte (Digital Markets Act, DMA) und verfügt über wichtige Zuständigkeiten in den Bereichen Data Governance, KI und Cloud, einschließlich Gaia-X und SPRIND, Deutschlands Agentur für Sprunginnovation. Es verwaltet die Industriepolitik im Technologiesektor. Dazu gehören auch wichtige Projekte von gemeinsamem europäischem Interesse (Important Projects of Common European Interest, IPCEIs) in Bereichen wie Halbleiter,

19 Justin Sherman, „India's Sudden Reversal on Privacy Will Affect the Global Internet“, Slate, (5. September 2022): https://slate.com/technology/2022/09/india-data-protection-bill-fourth-way.html (abgerufen am 5. Oktober 2022).

20 Der Anteil der OECD-Staaten am weltweiten BIP liegt bei 50 Prozent; allein die EU und die USA machen 42 Prozent des weltweiten BIP und 41 Prozent des Welthandels aus. Deutschland und Europa können neue multilaterale Mechanismen und Zielsetzungen entwickeln, um die gemeinsame technologische Innovationskraft und die Markt- und Regulierungsmacht der EU, der USA, Großbritanniens, Japans und anderer gleichgesinnter Staaten wirksamer zu nutzen.

Cloudcomputing und Wasserstofftechnologien.[21] Außerdem gibt es die Richtung der Außenwirtschaftspolitik vor und kontrolliert die wichtigsten Instrumente zur Steuerung von Technologie, nationaler Sicherheit und Handel. Zu diesen Instrumenten gehören die Kontrolle der Ausfuhr von Gütern mit doppeltem Verwendungszweck und das System für die Überprüfung von ausländischen Direktinvestitionen. All diese Hebel sind entscheidend, um Deutschlands und Europas Fähigkeit zur Gestaltung der Digitalpolitik und der digitalen Souveränität zu stärken.

Das Bundesministerium für Bildung und Forschung (BMBF) wiederum verfügt über wesentliche Entscheidungskompetenzen bezüglich der Vergabe von Fördermitteln und Aufträgen in der Grundlagenforschung bei Instituten wie der Max-Planck-Gesellschaft sowie in der angewandten Forschung bei den 75 Einrichtungen der Fraunhofer-Gesellschaft, der Helmholtz-Gemeinschaft, der Leibniz-Gemeinschaft und der Deutschen Forschungsgemeinschaft (DFG). Das BMBF ist zusammen mit dem BMWK federführend bei der Gestaltung der neuen Agentur für Transfer und Innovation (DATI). Das BMWK verfolgt zugleich aber auch das Ziel, die Ausgaben im Bereich FuE bis 2025 auf 3,5 Prozent des BIP zu erhöhen.[22] Die Verwaltung der IT-Konsolidierung im öffentlichen Sektor, der Cybersicherheit, des Schutzes kritischer Infrastrukturen und der Rechtsmäßigkeit des Datenzugriffs und der Datenspeicherung für Strafverfolgungszwecke verbleibt in der Zuständigkeit des Bundesministeriums des Innern und für Heimat (BMI). Das Bundesfinanzministerium (BMF) behält die Kontrolle über datenbezogene Politik, die für die Dateninfrastruktur von entscheidender Bedeutung ist und sich auf die Datenlokalisierung, die Industrieplanung und die Rahmenbedingungen auswirkt, unter denen amerikanische und chinesische Hyperscaler an den Cloud-Service-Angeboten der öffentlichen Hand teilnehmen können.

Die Entscheidung der Regierung, die gesamte digitale Verantwortung auszulagern und das Koordinationspersonal im Bundeskanzleramt zu dekonzentrieren, wird zumindest teilweise von dem Gefühl getragen, dass die digitale Transformation in der Ära Merkel stagnierte. Damit könnte jedoch ein Rückschritt verbunden sein, denn das Bundeskanzleramt ist für die Durchsetzung von Maßnahmen von allen Regierungsstellen am besten positioniert. Es hat regelmäßig das Digitalkabinett einberufen, um behördenübergreifende Bemühungen zu bündeln, und die Beiträge externer Interessengruppen in die Strategie und die Bemühungen zur Schaffung eines digitalen Staates einfließen lassen.[23]

Es hat gleichzeitig eine Konsolidierung stattgefunden, die dazu führen könnte, dass ein erweitertes BMDV zum Ausgangspunkt eines künftigen umfassenden Digitalministeriums wird. Die Verlagerung der Referate für europäische und internationale Digitalpolitik des BMWK und der zuständigen Führungskräfte in das BMDV könnte es einem solchen neuen „Tech-Zaren" ermöglichen, auf dem Internet Governance Forum (IGF), im EU-Ministerrat für Digitales in Brüssel und bei anderen externen Zusammenkünften auf internationaler Ebene die politische Richtung vorzugeben. Das BMDV ist auch für die Bereiche Telekommunikation, Breitband und das Gesetz über digitale Dienste zuständig und leitet das Digitalkabinett der Regierung, das über ein Budget von 500 Millionen Euro verfügt.

Der Erfolg Deutschlands bei der Gestaltung einer digitalen Strategie wird davon abhängen, ob es dem BMDV gelingt, eine „vernetzte Mentalität" zu schaffen, die zu einem Konsens innerhalb der Bundesregierung, zwischen den politischen Entscheidungsträgerinnen und -trägern von Bund, Ländern und Kommunen sowie zwischen dem öffentlichen und privaten Sektor führt. Die Zusammenarbeit des BMDV und BMWK wird von entscheidender Bedeutung sein, um kohärente nationale und globale Strategien zu entwickeln – für Data Governance, Start-ups, internationale Standards, Gaming, Marktzugang und Marktabschottung durch technoautoritäre Staaten sowie industriepolitische Maßnahmen für den Technologiesektor, einschließlich digitaler Infrastruktur, und Internet Governance.

21 Thierry Breton, „IPCEI on microelectronics – A major step for a more resilient EU chips supply chain", LinkedIn, (20. Dezember 2021): https://www.linkedin.com/pulse/ipcei-microelectronics-major-step-more-resilient-eu-chips-breton/?published=t (abgerufen am 22. Februar 2022).

22 Die Sozialdemokratische Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und die Freien Demokraten (FDP), „Koalitionsvertrag 2021-2025: Mehr Fortschritt wagen" (24. November 2021): https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1 (abgerufen am 12. April 2022).

23 Ryan Budish, Urs Gasser und Melyssa Eigen, „German Digital Council: An 'Inside -Out' Case Study", Berkman Center No. 2021-3, (28. April 2021): https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836185 (abgerufen am 22. Februar 2022).

Handlungs-empfehlungen

Die Fähigkeit Deutschlands, seine strategischen Zielsetzungen zu verfolgen und die globale Technologieordnung zu gestalten, erfordert auf allen Regierungsebenen ein Umdenken und eine stärkere Interdisziplinarität. Dafür bedarf es einer entsprechenden Neuausrichtung seiner operativen Strukturen. Mit den folgenden sieben Maßnahmen könnte Deutschland dies erreichen:

Eine klar definierte „regelbasierte" Doktrin der digitalen Souveränität unterstützen, die im Prinzip der Wahlfreiheit, offenen Märkten und Menschenrechten verankert ist. Die strategische Mehrdeutigkeit mit Blick auf das Konzept der digitalen Souveränität ist überholt. In einer Zeit, in der Europa strategische Technologieprojekte und Vorschriften für KI, Cloud-Computing, Halbleiter, 5/6G- Mobilfunknetze und Quantencomputing auf den Weg bringt, muss sich die Bundesregierung von ihrer inzwischen kontraproduktiven Mehrdeutigkeit verabschieden.

Geopolitisches Denken bei den Mitarbeitenden des Ministeriums und der Referate für Digitalpolitik (insbesondere im erweiterten BMDV) verankern. Das BMDV sollte ressortübergreifende Tagungen einführen, um die geostrategischen Implikationen digitaler und technologischer Regulierung sowie Politik zu bestimmen.[24] Hierfür muss die Rolle des AA und des BMVg in der Technologiepolitik gestärkt werden.[25] Die Bundesregierung sollte die Mandate dieser Ministerien auf Bereiche jenseits des Ausbaus von 5G-Netzwerken, der Cybernormen, der Nichtverbreitung von Massenvernichtungswaffen (weapons of mass destruction, WMD) und der Beschaffung aufkommender Technologien ausweiten. Ihre Zuständigkeiten sollten sich auf technische Forschung und Entwicklung, technische Normen und zivile Anbieter von Infrastrukturen jenseits der Mobilfunkausrüstung erstrecken.

Einen umfassenden Aktionsplan im Bereich Technologie und Außenpolitik vorlegen, der einen Zusammenhang zwischen der Digitalstrategie und der geplanten Nationalen Sicherheitsstrategie herstellt. Das BMDV hat gemeinsam mit dem BMWK, BMBF, BMI, AA und BMVg und in Zusammenarbeit mit anderen Stakeholdern die erste integrierte Digitalstrategie der Bundesregierung erarbeitet. Nun sollten BMDV, AA und BMWK einen Aktionsplan entwerfen, der innenpolitische und europäische Fragen der Industriepolitik und der Regulierung des Technologiesektors mit außenpolitischen Fragen verknüpft, die in Bezug auf Techno-Autoritarismus, die Festlegung internationaler Standards, Internet Governance und Technologieallianzen relevant sind. Der Aktionsplan muss Haushaltsprioritäten setzen, die gewährleisten, dass die Haushaltskonsolidierung nach der Covid-19-Pandemie nicht zu Lasten eines technologischen Wandels geht, der die Herausforderungen der nächsten Welle des globalen geopolitischen und wirtschaftlichen Wettbewerbs bewältigen kann.

Das Amt eines Sonderbeauftragen für Technologie mit drei Stellvertreterinnen bzw. Stellvertretern einführen, die die deutsche Digital-Außenpolitik koordinieren können. Das AA sollte das Amt einer/eines Sonderbeauftragten im Rang einer Staatssekretärin/eines Staatssekretärs einführen, die bzw. der insbesondere die Umsetzung des Aktionsplans übernimmt. Der bzw. dem Sonderbeauftragten sollten Stellvertreterinnen bzw. Stellvertreter für Cybersicherheit, Digitalwirtschaft und digitale Rechte zur Seite stehen, um die technologiepolitischen Ziele Deutschlands auf internationaler Ebene erfolgreich und kohärent zu vermitteln.[26]

Den digitalen Föderalismus flexibler gestalten. Die Bundesregierung muss die Interoperabilität, die Komplementarität von Innovationen und die Bewertung der Sicherheit von Technologien zwischen

24 Politikfelder wie Datenschutz, Forschung und Entwicklung im Bereich kritischer Technologien, Plattformregulierung, Cybersicherheit, öffentliche Beschaffung von Hardware und digitalen Diensten für Bildung, Gesundheit und Steuern auf Bundes-, Landes- und kommunaler Ebene sowie Cloud- und Datenräume haben erhebliche geopolitische Auswirkungen, die in der aktuellen Politik nicht ausreichend berücksichtigt werden.

25 Dabei sollten Bündnisse wie die NATO und die Beziehung zwischen der EU und den USA und die weitreichenden institutionellen Beziehungen in den Vereinten Nationen, der Organisation für Sicherheit und Zusammenarbeit in Europa, der G7, der G20 und dem Europarat sowie die Beziehung zwischen der EU und ASEAN berücksichtigt werden. Dies gilt auch für in Konfliktgebieten feindlich gesonnene Akteure wie Russland und technologisch-strategische Konkurrenten wie China.

26 Das US-Außenministerium hat vor Kurzem beispielsweise das Bureau of Cyberspace and Digital Policy mit drei Zuständigkeitsbereichen eingerichtet: internationale Cybersicherheit, IKT-Politik und digitale Freiheit. Diese Entwicklung basierte weitgehend auf dem Bericht der 2020 Cyberspace Solarium Commission, der Defizite in der technologiebezogenen US-Außenpolitik feststellte: https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/; Office of the Spokesperson, „Establishment of the Bureau of Cyberspace and Digital Policy, US Department of State Media Note", (4. April 2022): https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/ (abgerufen am 5. Oktober 2022).

Bund und Ländern stärken, um skalierbare Technologien auf europäischer und letztlich globaler Ebene aufzubauen. Entsprechende Bemühungen auf nationaler Ebene sind somit zugleich auch außenpolitisch relevant. Deutschland könnte beispielsweise einen „App Store" für digitale Instrumente in den Bereichen Bildung, Gesundheitswesen und Polizeiarbeit einrichten. Die Bundesregierung könnte auch die Auflagen bei ihren Finanzierungsanreizen für die Technologiebeschaffung durch Cyber- und Anbieterrichtlinien verstärken, die mit nationalen, EU- und NATO-Sicherheitsinteressen in Einklang stehen.

Einen ressortübergreifenden Bundestagsausschuss „Technologie- und Außenpolitik" einrichten. Ein solcher Ausschuss würde die Kohärenz der Ansätze in Politikfeldern wie Föderalismus und demokratische Technologieallianzen gewährleisten. Die Gruppe, die sich parteiübergreifend aus Mitgliedern der Bundestagsausschüsse für Digitales, Auswärtige Angelegenheiten, Wirtschaft, Inneres, Finanzen und Verteidigung zusammensetzen würde, sollte sich mit Themen befassen, die für alle vertretenen Ressorts relevant sind.

2 – VERANTWORTLICHKEITEN FÜR DIGITALE THEMEN IN DER DEUTSCHEN REGIERUNG

GROSSE KOALITION 2017 – 2021

BUNDESMINISTERIUM FÜR WIRTSCHAFT UND ENERGIE (BMWI)

WIRD →

BUNDESMINISTERIUM FÜR WIRTSCHAFT UND KLIMASCHUTZ (BMWK)

Behält:
- **Regulierungs**- und **Wettbewerbspolitik**, **Bundeskartellamt**, **DMA-Zuständigkeit**
- Zuständigkeiten der Unterabteilung VI C für Datenpolitik, KI und Cloud, einschließlich Gaia-X und SPRIN-D
- Abteilung IV, zuständig für **Tech-Industriepolitik**, inklusive der IPCEI Bereiche Halbleiter, Edge Computing und Wasserstoffenergie
- Abteilung V, verantwortlich für **Dual-Use-Exportkontrollen** und **FDI-Screening**

BUNDESKANZLERAMT

- Kein weiterer Kompetenzenaufbau in der Digitalpolitik
- Ein kleinerer Teil der IT-Planung geht ins BMI zurück
- Kein/e Staatsminister/in für Digitalisierung

Zuständigkeiten der Gruppe 6.2 für Digitalpolitik

Games-branche

Kompetenzen für den Digitalbereich

Abteilung VI für Digital- und Innovationspolitik
- Ehemaliger Leiter der Abteilung VI wird verbeamteter Staatssekretär im BMDV,
- Teile der Abteilung VI (Unterabteilungen A und B), womöglich auch die Zuständigkeit für **EU-Digitalvorhaben,** wandern ins BMDV,
- Zuständigkeiten für **nationale**, **europäische** und **internationale Digitalpolitik**, **Telekommunikation** und **DSA**.

BUNDESMINISTERIUM DES INNERN UND FÜR HEIMAT (BMI)

Behält:
- Verwaltung der IT-Konsolidierung des öffentlichen Sektors
- Fragen der **Cybersicherheit**, des **Schutzes kritischer Infrastrukturen** und des rechtmäßigen **Zugriffs auf Daten und deren Speicherung** für die Strafverfolgung

"AMPEL"-KOALITION 2021 – HEUTE

BUNDESMINISTERIUM FÜR VERKEHR UND DIGITALE INFRASTRUKTUR (BMVI)

Bislang nur zwei für die Digitalpolitik zuständige Unterabteilungen:

- **DG1 für Digitale Gesellschaft und Infrastruktur**, für Frequenzpolitik, Mobilkommunikation, Infrastrukturgesetze und Breitbandausbau zuständig
- **DG2 für Mobilität 4.0**, für das automatisierte Fahren, Satellitenpolitik und die Digitalisierung des Bauwesens und die Gamesbranche zuständig

WIRD →

BUNDESMINISTERIUM FÜR DIGITALES UND VERKEHR (BMDV)

Behält:
- **Zentrale Koordinierung** der **Digitalpolitik**
- Zwei Abteilungen, zuständig für die Digitalpolitik: Abteilung für **Digital- und Datenpolitik** und Abteilung für **digitale Konnektivität**

BUNDESFINANZ-MINISTERIUM (BMF)

Behält Kontrolle über **Datenzentrenpolitik**

BUNDESMINISTERIUM FÜR ERNÄHRUNG UND LANDWIRTSCHAFT (BMEL)

Zuständigkeit für allgemeine und spezielle **Produktsicherheit** (für die **KI-Regulierung** relevant)

BUNDESUMWELT-MINISTERIUM (BMUV)

Bereich **Verbraucherschutz**

BUNDESJUSTIZ-MINISTERIUM (BMJ)

BUNDESMINISTERIUM FÜR BILDUNG UND FORSCHUNG (BMBF)

Zentrale Anlaufstelle für **3,5% BIP in FuE 2025**

Behält Finanzierungsentscheidungen über die Auftragsvergabe für:
- **Grundlagenforschung**, die von den Instituten der Max-Planck-Gesellschaft durchgeführt wird
- **Angewandte Forschung**, die von den 75 Instituten der Fraunhofer-Gesellschaft und Forschungsnetzen wie der Helmholtz-Gemeinschaft, der Leibniz-Gemeinschaft und der Deutsche Forschungsgemeinschaft durchgeführt wird

Quelle: Darstellung der Autoren

KAPITEL 2

Digitale Innovation im geopolitischen Kontext

Stärken und Schwächen von Deutschlands digitalem Innovationsökosystem

KAPITELÜBERSICHT

Zentrale Erkenntnisse

1 Der Zustrom öffentlicher und privater Fördermittel, der während der Covid-19-Pandemie in die deutsche Forschung und Entwicklung im Bereich digitale Technologien floss, neigt sich dem Ende zu. Dies ist unter anderem auf die Inflation, die Haushaltskonsolidierung und die durch die „Zeitenwende" ausgelöste sicherheitspolitische Neuaufstellung zurückzuführen.

2 Deutschlands Zukunft in einer EU, die zu den weltweit führenden Technologiemächten gehört, erfordert eine grundlegende und schnelle Verlagerung der Forschungs- und Entwicklungskapazitäten – und zwar auf datenintensive und systemzentrierte Bereiche des Internets der Dinge (IoT) und der Deep Technology, die mit der industriellen Basis Deutschlands zusammenspielen. Es bedarf neuer politischer Ansätze in den drei Bereichen *Money*, *Markets*, *Minds*, sprich Fördermitteln, Märkten und Fachkräften.

3 Neue Technologien wie Robotik, künstliche Intelligenz (KI), fortschrittliche Materialwissenschaft sowie Biotechnologie und Quantencomputing sind vielfältig einsetzbar. Doch unkoordinierte Finanzierungsinstrumente, die Zivilklauseln von Uni-versitäten und Hochschulen sowie restriktive Visa- und Einstellungsrichtlinien für ausländische Fachkräfte bremsen die Innovation in diesen Bereichen und schaden der techno-geopolitischen Wettbewerbsfähigkeit Deutschlands.

4 Mittelfristig könnte Deutschland eine Bündelung des Zukunftsfonds mit neuen institutionellen Investitionen in einer Art deutschen Staatsfonds in Erwägung ziehen, wobei ein Teil der Mittel speziell strategisch wichtigen Risikokapitalvorhaben vorbehalten sein sollte.

Einleitung

Das Vertrauen in das deutsche Technologie-Ökosystem war bis vor Kurzem auf einem Allzeithoch. Durch den Aufbau einer soliden Grundlage für Forschung und Entwicklung (FuE), Investitionen und Start-ups war der digitale Sektor auf dem besten Weg, die Fertigungsindustrie bis 2030 bei der DAX-Marktkapitalisierung zu überholen.[27] Die daraus resultierenden Vorteile hätten sich nicht nur in den Portfolios von Aktienhändlerinnen und Aktienhändlern niedergeschlagen. Ein florierender digitaler Sektor hätte einen zentralen Pfeiler der künftigen techno-geopolitischen Stellung Deutschlands dargestellt. Er wäre Ausgangspunkt für Deutschlands Bemühungen um digitale Souveränität in Europa gewesen – einer Souveränität, die auf Entscheidungs- und Wahlfreiheit, erhöhter Widerstandsfähigkeit und der Vermeidung technologischer Abhängigkeiten von geopolitischen Konkurrenten beruht. Inzwischen ist die Lage jedoch deutlich angespannter.

Die Auswirkungen des russischen Angriffskriegs gegen die Ukraine, die steigenden Energiepreise und die Inflation reduzieren das weltweit verfügbare Kapital für den Technologiesektor. Privatanlegerinnen und -anleger ziehen sich in einem alarmierenden Tempo aus dem deutschen Digitalsektor zurück. Die Bundesregierung wendet sich der Haushaltskonsolidierung zu und strebt für 2023 einen ausgeglichenen Haushalt an. Da die Modernisierung der Bundeswehr und die Umstellung auf erneuerbare Energien ganz oben auf der Agenda der Regierung stehen, könnte die Unterstützung für den innovationsorientierten Industriestandort Deutschland deutlich abnehmen, wenn der Forschung und Entwicklung im Bereich der digitalen Technologien nicht genügend Mittel zur Verfügung stehen.

Die deutsche Wirtschaft ist hochgradig differenziert und wird von clusterorientierten Innovationen, politischem Föderalismus, einem von Familienunternehmen geprägten Mittelstand und diffusen nationalen Forschungsnetzwerken angetrieben. Diese dezentralisierte Struktur war in der Vergangenheit stets eine Stärke. Im Industriezeitalter erwiesen sich hochentwickelte Nischenfähigkeiten als weltweit wettbewerbsfähig. Doch dieses Zeitalter ist

27 Ryan Browne, Start-up founder predicts a shakeup in Germany's blue-chip DAX index, with tech taking over by 2030, in: CNBC, 17. November 2021: https://www.cnbc.com/2021/11/17/germanys-dax-index-will-be-taken-over-by-tech-in-2030-says-wefox-ceo.html (abgerufen am 22. April 2022).

weitgehend vorbei. In der heutigen Welt sind Netzwerkeffekte der Schlüssel zur internationalen Wettbewerbsfähigkeit auf dem Markt für datenintensive Plattformen, KI und Cloud Computing. Das bedeutet: Deutschland muss seine komparativen Vorteile im digitalen Sektor besser nutzen, um die Herausforderungen in den drei miteinander verknüpften Bereichen Fördermittel, Märkte und Fachkräfte anzugehen.

Hierbei geht es nicht „nur" um die Stellung Deutschlands in der Welt. Innovation ist auch unerlässlich, um globale geostrategische Ziele zu erreichen. Die Entwicklung des deutschen Innovationsökosystems wird die sich verändernde Rolle Europas mitbestimmen – als Großmacht für strategische Technologien und als Verfechterin einer demokratischen Technologiepolitik.

Status quo

Innovation erfordert ein Ökosystem aus Fördermitteln, Märkten und Fachkräften, das in der Lage ist, die Stärken Deutschlands bei FuE in Vorteile bei datenintensiven, systemzentrierten Gebieten der IoT und Deep Technology zu verwandeln, die den nationalen Fertigungssektor stärken. Die Covid-19-Pandemie hat zu positiven Verschiebungen in der Struktur der deutschen und europäischen Innovationslandschaft geführt, insbesondere bei Fördermitteln. Europaweit stiegen die Start-up-Finanzierungen von rund 40 Milliarden Euro im Jahr 2020 auf 106 Milliarden Euro im Jahr 2021, was zu einer explosionsartigen Zunahme von europäischen Unicorns führte. Insgesamt erreichten 321 mit Risikokapital finanzierte Start-ups einen Unternehmenswert von mindestens einer Milliarde Dollar, von denen sich allein 55 in Deutschland befinden. Außerdem haben hierzulande 26 Decacorns mit einem Wert von mehr als 10 Milliarden Dollar ihren Sitz.[28] Risikokapital-Investitionen in Deutschland erreichten 2021 17,4 Milliarden Euro und haben sich somit im Vergleich zum Vorjahr verdreifacht.[29] In diesem Zeitraum verdoppelte sich auch die Finanzierung von Deep Technology, zu der Robotik, KI, Sensorik, fortschrittliche Materialien, Biotechnologie und Quantencomputing gehören. 2021 flossen in Europa 21 Prozent des gesamten Risikokapitals in diese Bereiche. Der Zustrom von Fördermitteln war so erheblich, dass sich die Quanten- und Post-Quanten-Kryptographie, VR-Gesundheitsversorgung, KI-basierte Arzneimittelforschung, Cognitive Computing und Silizium-Photonik zu Spitzentechnologien entwickelten. Arbeit von Unternehmen wie Q.ANT und Franka Emika ist Deutschland in der Robotik und Sensorik besonders gut aufgestellt.[30] Es entwickelt derzeit seine Fähigkeiten bei Flugzeugen der nächsten Generation (bei Lilium), Biopharma (bei BioNTech) und KI für Verteidigung (bei Helsing.ai).[31]

Obwohl Deutschland in bestimmten Sektoren europäischer Technologie-Innovator ist,[32] fällt es auf anderen Gebieten hinter einige Nationen zurück. US-amerikanische und chinesische Tech-Unternehmen mögen zwar Marktführer sein, aber auch Unternehmen aus dem Vereinigten Königreich, Kanada, Südkorea und Israel wetteifern um die Schaffung, Kontrolle und Kommerzialisierung von Innovationen in einer breiten Spanne von Bereichen - von Social Media-Plattformen bis Deep Technology. Selbst Europas größtes Technologieunternehmen ASML (Marktwert 352 Milliarden Dollar) verblasst neben Microsoft (2,5 Billionen Dollar) oder dem chinesischen Unternehmen Tencent (601 Milliarden Dollar). Europa macht lediglich 7 Prozent der Kapitalisierung im weltweiten Technologiemarkt aus.[33] Und obwohl hier jährlich etwa die gleiche Anzahl von Start-ups wie in den USA gegründet werden, lässt sich in Europa eine stärkere Stagnationsrate beobachten (45 Prozent gegenüber 37 Prozent).[34] Dieser Unterschied – der zum Teil auf

28 Atomico, *State of European Tech 2021*, 9. Dezember 2021, S. 14: https://soet-pdf.s3.eu-west-2.amazonaws.com/State_of_European_Tech_2021.pdf (abgerufen am 22. April 2022).

29 Ernst & Young GmbH, Startup-Barometer Deutschland, Januar 2022: https://assets.ey.com/content/dam/ey-sites/ey-com/de_de/news/2022/01/ey-startup-barometer-2022.pdf (abgerufen am 22. April, 2022).

30 Henning Kagermann, Karl-Heinz Streibich und Katrin Suder, „Digitale Souveränität: Status quo und Handlungsfelder" acatech IMPULSE, (25. März 2021), S. 13: https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/ (abgerufen am 12. April 2022)

31 Deutschland steht hinter dem Vereinigten Königreich an zweiter Stelle der europäischen Standorte für Unicorns mit primären (25) oder sekundären (26) Hubs. Zwei der fünf größten digitalen Hubs befinden sich in Deutschland.

32 Bei den börsennotierten Technologieunternehmen liegt Deutschland mit drei Unternehmen (SAP, Infineon und Delivery Hero) in Europa an der Spitze. Die privatwirtschaftliche Technologielandschaft des Landes ist geprägt von etablierten Unternehmen wie SAP, Deutsche Telekom, Infineon und Bosch sowie von neuen Anbietern digitaler Dienstleistungen wie Delivery Hero, N26, HelloFresh und Zalando. Von den 10 größten Technologie-Deals in Europa im Jahr 2021 betrafen vier deutsche Unternehmen (Celonis, Gorillas, N26 und Trade Republic), gefolgt von jeweils zwei im Vereinigten Königreich und den Niederlanden. Der größte mit Risikokapital finanzierte Exit in Europa war der Börsengang der AUTO1Group im Februar 2021.

33 Oliver Noyan, Europe tech investment to reach $100 billion in 2021 in: *EURACTIV*, 9. Dezember 2021: https://www.euractiv.com/section/digital/news/europe-tech-investment-is-reaching-100-billion-annually (abgerufen am 22. April 2022).

34 Europäische Kommission, Europe's next leaders: the Start-up and Scale-up Initiative COM(2016) 733 final, 22. November 2016: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A733%3AFIN (abgerufen am 22. April 2022).

den leichteren Zugang zu Märkten, Later-Stage-Finanzierungen und Talenten außerhalb Europas zurückzuführen ist – hat zu einer „Scale-up"-Falle geführt, die die EU in den letzten zwei Jahrzehnten etwa eine Million Arbeitsplätze und 2 Billionen Euro an BIP gekostet hat.[35]

Deutschland mangelt es zudem an Finanzierungen. Seine größten Risikokapitalfonds sind im Vergleich zu denen in den USA und China klein.[36] Auch die Investitionsquote der Pensionsfonds ist nach wie vor gering.[37] Dagegen ist mindestens ein US-Investor an 61 Prozent aller europäischen Later-Stage-Investitionen in Unternehmen beteiligt, die kurz vor dem Markterfolg stehen. US-amerikanische oder asiatische Investierende sind insgesamt an 95 Prozent aller europäischen Later-Stage-Finanzierungen von mehr als 250 Millionen Dollar beteiligt.[38] Das US-Kapital macht mehr als die Hälfte der Gesamtinvestitionen in Deutschland aus und spielt besonders bei Late-Stage-Investitionen eine erhebliche Rolle.[39] Bedenklich ist, dass diese Investitionen zunehmend versiegen, da die europäischen Zentralbanken auf die Inflation reagieren und die geopolitischen Risiken, die sich aus dem Einmarsch Russlands in die Ukraine ergeben, die Bereitschaft globaler institutioneller Investoren zur Finanzierung des digitalen Sektors verringern.

35 Ebd.

36 World Fund (406 Millionen Dollar), Bayern Kapital (238 Millionen Dollar), Heal Capital (122 Millionen Dollar), Atlantic Food Labs (117 Millionen Dollar), Earlybird (88 Millionen Dollar), and Visionaries Club (85 Millionen Dollar)

37 In der DACH-Region werden nur 4 Prozent der Gesamtmittel aufgebracht, in Skandinavien sind es 28 Prozent.

38 Atomico, State of European Tech 2021, 9. Dezember 2021, S. 57: https://soet-pdf.s3.eu-west-2.amazonaws.com/State_of_European_Tech_2021.pdf (abgerufen am 22. April 2022)

39 Atomico, State of European Tech 2021, 9. Dezember 2021, S. 253: https://soet-pdf.s3.eu-west-2.amazonaws.com/State_of_European_Tech_2021.pdf (abgerufen am 22. April 2022)

3 – FUE-HUBS FÜR NEUE SCHLÜSSELTECHNOLOGIEN

Quelle: Eigene Darstellung

• **DIE KONSORTIUM-BASIERTE QUANTEN-INITIATIVE BAYERNS** bündelt unter anderem die Forschungsnetzwerke der Fraunhofer-Gesellschaft, der Max-Planck-Gesellschaft und der Technischen Universität München (TUM) in einem Zentrum für Quantencomputing und Quantentechnologien (ZQQ). Das Zentrum ist das Kernstück eines Münchner Technologieparks, zu dem auch privatwirtschaftliche Akteure wie IBM gehören, deren Q System One in Ehningen eingesetzt wird.[40] Der Q System One ist ein Quantencomputer mit 27 Qubits, aber IBM hat sich zum Ziel gesetzt, bis 2023 den ersten Quanten-Chip mit mehr als tausend Qubit fertigzustellen.[41]

• **CYBER VALLEY** ist Europas größtes Forschungskonsortium für künstliche Intelligenz. Es vernetzt das Max-Planck-Institut für Intelligente Systeme, die Universitäten Stuttgart und Tübingen sowie privatwirtschaftliche Akteure wie Amazon, Daimler, Bosch, Amazon und BMW. Cyber Valley baut in Tübingen einen Campus mit einer 180-Millionen-Euro-Finanzierung auf.

• Dank der Kooperation des **FORSCHUNGSZENTRUMS JÜLICH** mit dem kanadischen Unternehmen D-Wave nimmt der fortschrittlichste Quantencomputer Europas die Arbeit auf. Der Rechner mit 5.000 Qubit soll in die Supercomputing-Infrastruktur am Forschungszentrum eingebunden werden und Mitte 2024 online gehen. Das Bundesministerium für Bildung und Forschung (BMBF) unterstützt das Jülicher Verbundprojekt QSolid mit einem Budget von 76,3 Millionen Euro. 25 Unternehmen und Forschungseinrichtungen – darunter das Leibniz-Institut für Photonische Technologien, das Karlsruher Institut für Technologie, die Universität Ulm, die Freie Universität Berlin und die Universität zu Köln – arbeiten gemeinsam daran, einen Quantencomputer auf Basis modernster Technologie zu bauen.

• **DAS DEUTSCHE FORSCHUNGSZENTRUM FÜR KÜNSTLICHE INTELLIGENZ (DFKI)** ist eines der ältesten und größten KI-Forschungszentren der Welt. Es unterhält Standorte in sieben Städten, die auf den Gebieten der Bilderkennung, Simultanübersetzung, Robotik und kognitive Assistenten arbeiten.

40 Max-Planck-Gesellschaft, Das Munich Quantum Valley – ein Sprung für Quantenwissenschaft und -technologie, in: mpg.de, 12. Januar 2021: https://www.mpg.de/16258573/munich-quantum-valley (abgerufen am 27. April 2022).

41 Jay Gambetta, IBM's roadmap for scaling quantum technology, in: IBM [Weblog], 15. September 2020: https://research.ibm.com/blog/ibm-quantum-roadmap (abgerufen am 27. April 2022).

Deutschlands angehende Technologie-Champions sind folglich gezwungen, sich um außereuropäische Finanzmittel zu bemühen, wenn sie sich vom Start-up zum reiferen Marktteilnehmer entwickeln. Sie sehen sich auch mit einem unangenehmen Paradoxon konfrontiert: Je größer ihr Erfolg, desto größer ist der Anteil amerikanischer und chinesischer Risikokapitalgeber und institutioneller Investoren. Gleichzeitig verfolgen deutsche und europäische Kapitalgeber nur eine begrenzte „Auswärtsstrategie" mit ausländischen Direktinvestitionen, um außerhalb der Landesgrenzen oder der EU neue Möglichkeiten zu erkunden. Der Mangel an Kapital und Risikobereitschaft, regulatorische Unterschiede und Abhängigkeiten im Inland behindern die Entwicklung in diesem Bereich. In die USA fließt viel weniger europäisches Risikokapital als umgekehrt. Die Folge ist, dass Europa praktisch nicht an den weltweiten Technologieinvestitionen beteiligt ist und hinter anderen Ländern zurückbleibt.

Ein weiterer Nachteil Deutschlands ist, dass es nur begrenzt in der Lage ist, auf außereuropäische Talente zurückzugreifen, wodurch es im weltweiten Wettbewerb um die besten Fachkräfte ins Hintertreffen geraten ist. Der Anteil der Europäerinnen und Europäer in deutschen Start-ups ist mit 85,9 Prozent sehr hoch, während nur 6,6 Prozent der Beschäftigten aus Asien, 2,2 Prozent aus Nordamerika und 5,4 Prozent aus anderen Ländern stammen.[42] Im Gegensatz dazu wurden zwei Drittel der Silicon-Valley-Beschäftigten aus den Bereichen Ingenieurwesen und Informatik außerhalb der Vereinigten Staaten geboren. Außerdem stammt bei der Hälfte der US-amerikanischen Unicorn-Unternehmen mindestens eine Gründerin oder ein Gründer aus dem Ausland. In Deutschland hat jede fünfte Gründerin oder jeder fünfte Gründer einen Migrationshintergrund;[43] lediglich 15 Prozent sind Frauen. Ebenso auffällig ist, dass nur 1,3 Prozent der europäischen Fördermittel an Gründerinnen und Gründer gingen, die ethnischen Minderheiten angehören.[44]

In den letzten Jahren hat sich die technische Forschung in Deutschland weiterentwickelt, was durch eine liberalisierte Zulassungspolitik für internationale MINT-Studierende (Mathematik, Informatik, Naturwissenschaft und Technik) und eine starke Wirtschaft begünstigt wurde. Hier hat Deutschland von geopolitischem Rückenwind profitiert: von Entwicklungen, die IT-Talente aus den südlichen Ländern der Eurozone, dem Nahen Osten und zuletzt aus der kriegszerrütteten Ukraine und dem autoritären Russland vertrieben haben. Allerdings fehlt es in Deutschland noch an flexiblen Arbeitsbedingungen, angemessenen Gehältern, attraktiven Sozialleistungen und Forschungsressourcen, um Toptalente anzuziehen und zu binden. Die USA, Kanada und das Vereinigte Königreich liegen in diesem Wettlauf weiterhin vorne – in einer Zeit, in der weltweiter IT-Fachkräftemangel herrscht.

Der Fachkräftemangel in der Informations- und Kommunikationstechnologie (IKT) ist eine große Herausforderung für Deutschlands technologische Leistungsfähigkeit und somit auch für die Sicherheit Europas. Die EU hat sich das Ziel gesetzt, bis 2030 20 Millionen IKT-Fachkräfte zu beschäftigen,[45] doch in Deutschland werden jährlich nur 70.000 von ihnen ausgebildet. Im Halbleitersektor von Silicon Saxony fehlt es derzeit an nahezu 30.000 Arbeitskräften.[46] Sachsen-Anhalt, der Standort der künftigen Halbleiterproduktion in Deutschland, steht vor den noch größeren Schwierigkeiten, europäische und globale Talente aus Regionen wie Süd- und Ostasien, dem Nahen Osten und Afrika anzuziehen. In beiden Regionen wird die Situation durch ein politisches und gesellschaftliches Umfeld verschärft, das teilweise noch immer Rechtsextremismus, Rassismus und Fremdenfeindlichkeit duldet.[47] Die unzureichende Mitarbeiterzahl in den deutschen Cyber-Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Cyber Innovation Hub der Bundeswehr und der kürzlich gegründeten Agentur für Innovation in der Cybersicherheit in Halle bleibt

42 Bundesverband Deutsche Startups e.V., *Deutscher Startup Monitor 2021*, Oktober 2021: https://deutschestartups.org/wp-content/uploads/2021/10/Deutscher-Startup-Monitor_2021.pdf (abgerufen am 24. April 2022).

43 Tom Schmidtgen, Jedes fünfte Start-up hat im Schnitt einen Gründenden mit Migrationshintergrund, in: *Startbase*, (28. April 2021): https://www.startbase.com/news/jedes-fuenfte-start-up-hat-gruenderin-oder-gruender-mit-migrationshintergrund/ (abgerufen am 24. April 2022).

44 Atomico, State of European Tech 2021, 9. Dezember 2021, S. 134: https://soet-pdf.s3.eu-west-2.amazonaws.com/State_of_European_Tech_2021.pdf (abgerufen am 22. April 2022)

45 Europäische Kommission, 2030 Digital Compass: the European way for the Digital Decade" COM (2021) 118 final, in: eur-lex.europa.eu, 09. März 2021: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (abgerufen am 24. April 2022).

46 Joe Miller, Silicon Saxony' aims to be EU chipmaking hub, in: *Financial Times*, 16. Dezember 2021: https://www.ft.com/content/75841b94-196e-466f-ad1b-72d3809c33fc (abgerufen am 24. April 2022).

47 Sonderkommission zu institutionellem Antisemitismus, Rassismus und Fremdenfeindlichkeit, *Bericht der Sonderkommission zu institutionellem Antisemitismus, Rassismus und Fremdenfeindlichkeit in der Landespolizei Sachsen-Anhalt*, März 2021: https://mi.sachsenanhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/MI/MI/2._Aktuelles/20210228_Bericht_Sonderkommission_Druckversion.pdf (abgerufen am 24. April 2022).

ein weiteres wichtiges strategisches Hindernis, das zu schwierigen Entscheidungen bei der Festlegung und Verfolgung von Prioritäten führen kann.

Einige der erfolgreichsten digitalen Innovationsökosysteme haben sich in kleinen, offenen Volkswirtschaften entwickelt, die mit einer konstanten Sicherheitsbedrohung durch einen geopolitischen Konkurrenten konfrontiert sind. Diese existenzielle Bedrohung kann ein nationales Bewusstsein schaffen, das einen interdisziplinären Ansatz für staatlich geförderte Forschung und Entwicklung ermöglicht und die mit einem kleinen Binnenmarkt zusammenhängenden Herausforderungen meistert. Dies ist in Taiwan, Estland, Südkorea und Israel der Fall – in Ländern, die alle ein weltweit wettbewerbsfähiges Ökosystem für technologische Innovationen entwickelt haben, das oft eng mit dem Verteidigungssektor verwoben ist. Als eine Mittelmacht, die sich keiner unmittelbaren geostrategischen Gefahr ausgesetzt sieht, stützt sich Deutschland mehr auf den EU-Markt, um seine Ambitionen als Innovationszentrum zu verfolgen. Die Grenzen der regulatorischen Konvergenz innerhalb der EU sind jedoch deutlicher geworden, und Deutschland sollte seine Marktentwicklungsstrategie auf die Nutzung offener Standards und Open-Source-Software verlagern, um die Hürden für FuE bei digitalen Technologien auf der Angebotsseite zu verringern. Entsprechende Skalenvorteile können auch dazu beitragen, die Stärken der Technologiekonkurrenten Deutschlands in Bereichen wie Marktgröße (USA, China) oder geopolitisch bedingter Kohäsion (Israel, Taiwan, Südkorea) auszugleichen.

Aktueller politischer Ansatz

Die deutsche Innovationspolitik konzentriert sich am stärksten auf Grundlagenforschung.[48] Das Land wendet bereits 3,13 Prozent des BIP dafür auf und die Ampelregierung hat sich das ehrgeizige Ziel gesetzt, diesen Anteil auf 3,5 Prozent zu erhöhen. Deutschlands Ausgaben machen derzeit nahezu ein Drittel der gesamten europäischen FuE-Ausgaben aus.[49]

Bei der Kommerzialisierung von Forschung besteht in Deutschland allerdings noch Nachholbedarf. Das Zentrale Innovationsprogramm (ZIM) fördert seit Jahrzehnten die Forschung und Entwicklung im Mittelstand. Das Zentrum ist jedoch unterfinanziert und kann die Nachfrage nach seinen Dienstleistungen nicht bewältigen.[50] Seit Oktober 2021 hat es keine neuen Förderanträge angenommen. Um dieses Problem anzugehen, hat die Regierung 2017 das EXIST-Programm ins Leben gerufen, das die unternehmerische Initiative und die Kommerzialisierung der akademischen Forschung fördert. Eine weitere Maßnahme ist die Einrichtung der Deutschen Agentur für Transfer und Innovation (DATI), um die deutsche Forschung zu kommerzialisieren. Die DATI würde Möglichkeiten bieten, um Anreize für die Kommerzialisierung von Universitätsforschung zu testen, angehende akademische Unternehmerinnen und Unternehmer zu unterstützen und sie mit dem Privatsektor zu verbinden. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) koordiniert im Rahmen seiner Digital Hub Initiative zudem zwölf anerkannte und über Deutschland verteilte Innovationshubs. Jeder dieser Hubs ist auf einen Sektor spezialisiert, um die lokalen Stärken in Forschung und Entwicklung sowie in der kommerziellen Technologie für eine bundesweite Skalierbarkeit zu stärken.[51]

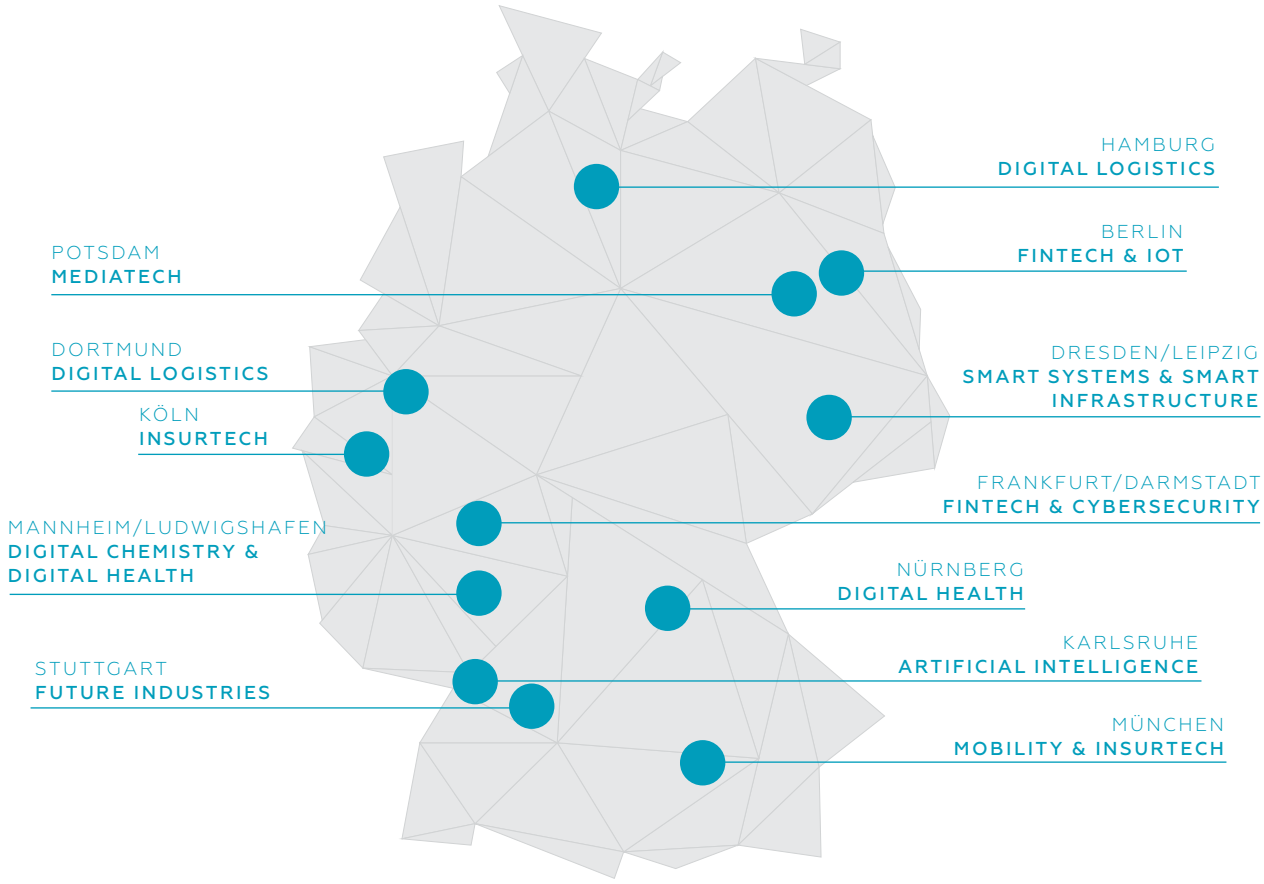
48 Grundlagenforschung und -entwicklung wird definiert als Forschung, die auf ein umfassenderes, theoretisches Verständnis grundlegender Aspekte von Technologien abzielt, im Gegensatz zur angewandten Forschung, die sich in der Regel leichter vermarkten lässt.

49 Bundesministerium für Bildung und Forschung, Forschung und Innovation (2021): https://www.datenportal.bmbf.de/portal/de/research.html (abgerufen am 25. April 2022).

50 Bundesministerium für Wirtschaft und Klimaschutz, Zentrales Innovationsprogramm *Mittelstand*, in: zim.de, 7. Oktober 2021: https://www.zim.de/ZIM/Redaktion/DE/Meldungen/2021/4/2021-10-06-aussetzung-zur-antragsannahme.html (abgerufen am 24 April 2022).

51 Bundesministerium für Wirtschaft und Klimaschutz, Zwölf Hubs, ein digitales Netzwerk, in: de.digital https://www.de.digital/DIGITAL/Redaktion/DE/Dossier/digital-hub-initiative.html (abgerufen am 26. April 2022).

4 – DEUTSCHLANDS ZWÖLF DIGITAL HUBS – EIN STARKES NETZWERK VON TECHNOLOGISCHER EXPERTISE UND INNOVATIONSKRAFT



Quelle: Bundesministerium für Wirtschaft und Klimaschutz

Darüber hinaus stellt das Venture Tech Growth Financing-Programm – eine gemeinsame Prä-Covid-19- Initiative der Regierung und der *Kreditanstalt für Wiederaufbau* (KfW), der Investitions- und Entwicklungsbank Deutschlands – Darlehen in Höhe von 50 Millionen Euro pro Jahr für Start-ups bereit. Bereits in den ersten 100 Tagen ihrer Amtszeit hat die Ampelregierung mit ihrer regierungsweiten Start-up-Strategie einen ehrgeizigen Ansatz vorgestellt, mit einem Zehn-Punkte-Programm zu Themen von Kapital bis Datenzugang.[52] Vor allem aber sieht die Start-up-Strategie vor, dass staatliche und private Pensionsfonds einen Teil ihrer Mittel als Risikokapital investieren. Zusammen mit dem Zukunftsfonds 2021 ist dies eine wichtige Überbrückungsmaßnahme für den Einbruch des Risikokapitals nach dem Ausbruch der Covid-19-Pandemie, insbesondere in Bezug auf risikoreiche Deep Technology.

Paradoxerweise hat die Regierung auch damit begonnen, die Finanzierung von Projekten zurückzustellen, die Technologie-Ökosysteme durch Skalierbarkeit, Interoperabilität und Open Source-Entwicklung fördern. In einem Moment der Leichtfertigkeit – oder vielleicht auch absichtlich – strich die Koalition zunächst die Mittel für die DATI, die Digitalisierung der Bildung, die Gaia-X-Cloud-Architektur für Standards und den Sovereign Tech Fund zur Unterstützung der Entwicklung von Open-Source-Software für Sicherheit,

52 Bundesministerium für Wirtschaft und Klimaschutz, Start-up-Strategie der Bundesregierung, in: bmwk.de, 21. Juni 2022: https://www.bmwk.de/Redaktion/DE/Dossier/Digitalisierung/start-up-strategie.html (abgerufen 19. Juli 2022)

Widerstandsfähigkeit und technologische Vielfalt. Doch diese Maßnahmen zu opfern, um die deutsche Haushaltskonsolidierung nach der Coronakrise umzusetzen, könnte sich als kurzsichtig erweisen und sich negativ auf die deutsche Innovationslandschaft und Cybersicherheit auswirken. Beschränkungen von FuE-Ökosystemen im Bereich der Güter mit doppeltem Verwendungszweck haben traditionell die Innovation im Verteidigungsbereich geschwächt, die eine der größten Quellen für technologische Entdeckungen weltweit ist. Das wirkt sich wiederum auf die wirtschaftliche und geopolitische Wettbewerbsfähigkeit aus.

Dieser Trend ist in Deutschland nichts Neues. Die Universitäten und Hochschulen des Landes, allen voran die Universität Bremen im Jahr 1986, haben sogenannte „Zivilklauseln" eingeführt, um die Forschung auf zivile Zwecke zu beschränken.[53] Mehr als 70 deutsche Einrichtungen des tertiären Bildungsbereichs, darunter die Technische Universität Berlin und die Universität Tübingen, die beide führende KI-Forschung betreiben, haben inzwischen Zivilklauseln.[54] Die strikte Trennung von ziviler und militärischer Forschung erschwert Durchbrüche in kritischen und grundlegenden Technologien wie KI, Quantenverschlüsselung und fortschrittlichen Materialien. Wegen des doppelten Verwendungszwecks dieser neuen und grundlegenden Technologien ist es zunehmend unmöglich, eine künstliche Trennwand zwischen ziviler und militärischer Technologie zu ziehen. Darüber hinaus ist es auch aus geopolitischer Sicht nachteilig, da die Verteidigungstechnologie in Ländern wie den USA, China, Israel, dem Vereinigten Königreich und Frankreich eine immer größere Rolle spielt und ein Motor für allgemeine digitale Innovationsökosysteme ist.

Doch nicht alle Aussichten an der akademischen Front sind düster. Durch mehr Fördermittel für die öffentliche Verwaltung, Einstellungsverfahren und wettbewerbsfähige Gehälter wurde die Universitätsausbildung für ausländische Studierende und die Visumerteilung für qualifizierte Einwanderinnen und Einwanderer erleichtert. Beide Entwicklungen sind zu begrüßen, da sie den Einstieg in den Technologiesektor ermöglichen. Deutschland hat auch unbewusst von geopolitischen Entwicklungen profitiert, da die Krise in der Eurozone 2010–2012 und die Flüchtlingskrise 2015–2016 hochqualifizierte europäische und globale Talente ins Land brachten.[55]

Handlungsempfehlungen

Will die Bundesregierung Deutschlands globale Stellung in der Technologieförderung stärken, muss sie sich auf drei Bereiche konzentrieren:

1. Zusätzliche Finanzierungsquellen für die Kommerzialisierung der Grundlagenforschung schaffen, Forschung und Entwicklung auf dem Gebiet von Gütern mit doppeltem Verwendungszweck ermöglichen und Tech-Unternehmen langfristig Fördermittel bereitstellen

2. Die Skalierbarkeit innerhalb des deutschen föderalen Systems und in ganz Europa durch den digitalen Binnenmarkt angehen

3. Hochqualifizierte IT-Fachleute ausbilden, anwerben und binden, die den künftigen innovationsorientierten Industriestandort Deutschland stärken

Konkrete Maßnahmen wären u.a.:

Anreize für die Koordination zwischen innovationsfördernden Einrichtungen schaffen. Es ist entscheidend, dass die deutschen Innovationsagenturen enger zusammenarbeiten. Die Cyber-Agentur und die Bundesagentur für Sprunginnovationen haben bereits ihre Bereitschaft dazu erklärt.[56] Ein weiterer Schritt wäre die Schaffung eines nationalen strategischen Technologierats und eines offiziellen behördenübergreifenden Koordinationsprozesses, an

53 Ursula Schröder, Akademie kritisiert Zivilklauseln, in: Forschung und Lehre, in: Forschung & Lehre, 19. Mai 2022: https://www.forschung-und-lehre.de/politik/akademie-kritisiert-zivilklauseln-4820 (abgerufen am 10. Juli 2022)

54 Initiative Hochschulen für den Frieden-Ja zur Zivilklausel, Bestehende Zivilklauseln, in: zivilklausel.de, 2022: http://zivilklausel.de/index.php/bestehende-zivilklauseln (abgerufen am 10. Juli, 2022).

55 Hoffmeyer-Zlotnik, Grote, *Anwerbung und Bindung von internationalen Studierenden in Deutschland*, in: bamf.de, 2019: https://www.bamf.de/SharedDocs/Anlagen/EN/EMN/Studien/wp85-internationale-studierende.pdf?__blob=publicationFile&v=18 (abgerufen am 26. April 2022).

56 Marcel Roth, Cyberagentur und Innovationsagentur Sprind wollen stärker zusammen arbeiten, in: Mitteldeutscher Rundfunk, 15. Januar 2022: https://www.mdr.de/nachrichten/sachsen-anhalt/podcast/podcast-digital-leben-folge-fuenfzig-cyberagentur-sprind-zukunft-laguna-hummert-zusammenarbeit-100.html (abgerufen am 26. April 2022).

dem die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) sowie der Zukunftsfonds, die DATI und der Sovereign Tech Fund beteiligt sind. Die derzeitige Regierung sieht die Einrichtung der beiden letztgenannten Stellen vor. Diese Agenturen würden strategische Zielsetzungen vergleichen, potenzielle Kooperationen testen, größere Hindernisse ermitteln und die Erforschung von Technologien mit doppeltem Verwendungszweck und deren Anwendung prüfen. Die daraus resultierende größere Transparenz würde dazu beitragen, Doppelfinanzierungen zu vermeiden und gleichzeitig das Wissen über und den Zugang zu erfolgreichen Programmen zu verbessern. Die Bundesregierung sollte auch eine Übersicht über die Initiativen der Länder schaffen und asymmetrische FuE- und Industrieallianzen sowohl zwischen den Bundesländern als auch mit dem Privatsektor in verbündeten Ländern fördern.

Die Wechselwirkung zwischen Deutschlands sicherheitspolitischer Zeitenwende und Innovation in Dual-Use-Technologien betonen. Das im Rahmen der „Zeitenwende" angekündigte Sondervermögen von 100 Milliarden Euro muss die Modernisierung des Verteidigungssektors mit grundlegenden Forschungs- und Entwicklungskapazitäten für Innovationen in Dual-Use-Technologien verbinden, einschließlich Verteidigungssoftware. Als Teil des Mentalitätswandels müssen Länder und Universitäten mit der Bundesregierung und dem Privatsektor an einer vernünftigen Nutzung der sogenannten Zivilklause arbeiten. Die Universitäten und Hochschulen, an denen Forschung betrieben wird, müssen die Breite der Nutzbarkeit solcher Technologien und ihrer Finanzierungsquellen anerkennen.

Anreize für verlässliche Kapitalinvestitionen mit Schwerpunkt auf industriellen Plattformen, IoT sowie Deep Technology und umweltfreundlichen digitalen Technologien schaffen. Trotz des Gegenwinds durch Sparmaßnahmen, Inflation und einen globalen Wirtschaftsabschwung sollte die deutsche Regierung Anreize für öffentliche Investitionen im Inland schaffen, um den innovationsorientierten Industriestandort Deutschland zu stärken. Die DATI, der Zukunftsfonds und der Sovereign Tech Fund zielen darauf ab, laufen jedoch gleichzeitig Gefahr, in der Haushaltskonsolidierung und im interministeriellen Machtkampf gefangen zu bleiben. Der Technologiesektor aber würde mehr staatliche Finanzierung begrüßen. Einer Umfrage zufolge bevorzugten Start-ups öffentliches Kapital als Finanzierungsquelle (49,7 Prozent), gefolgt von operativem Cashflow (43,4 Prozent), strategischen Investitionen (42,5 Prozent) und Risikokapital (42,2 Prozent).[57] Die Regierung muss strategische Vorgaben machen, um eine langfristige Planung und mutige Innovationen in digitalen Schlüsselbereichen zu ermöglichen. Der Zukunftsfonds möchte Start-ups Fördermittel in Höhe von 10 Milliarden Euro bereitstellen. Mittelfristig könnte Deutschland eine Bündelung des Zukunftsfonds mit neuen institutionellen Investitionen in einer Art deutschen Staatsfonds in Erwägung ziehen, wobei ein Teil der Mittel speziell strategisch wichtigen Risikokapitalvorhaben vorbehalten sein sollte.

Sandboxes, sprich geschützte Forschungsräume in öffentlich finanzierten Forschungseinrichtungen und Agenturen schaffen, die freier von Vorschriften, Bürokratie und öffentlichen Beschaffungsanforderungen sind. Die Anforderungen des Bundes an die Auftragsvergabe schränken die Möglichkeiten Deutschlands ein, ein weltweit wettbewerbsfähiges Innovationsökosystem zu entwickeln. Bürokratische Hürden, Genehmigungsverzögerungen und willkürliche Fristen können Innovation beeinträchtigen, wenn nicht gar verhindern. Forschungseinrichtungen und Innovationsagenturen würden von entsprechenden Finanzierungsanforderungen des öffentlichen Sektors für die Auftragsvergabe und Ausschreibungen, Evaluierung und langfristige Planung profitieren, die mit der raschen globalen Innovation Schritt halten können. Beschleunigte Verfahren würden auch dabei helfen, festzustellen, ob staatliche Investitionen sinnvoll sind.

Das Engagements des Privatsektors in „Expeditionsinvestitionen" und Übernahmen von Technologieführern und Start-ups außerhalb Europas fördern. Für die meisten US-amerikanischen und chinesischen Technologieunternehmen sind Fusionen und Übernahmen von zentraler Bedeutung, um ihre Marktposition zu stärken und Innovationen aus anderen Quellen zu integrieren. Deutschlands führende, von der Regierung unterstützte Unternehmen sollten das Instrument ausländischer Direktinvestitionen nutzen, um Zugang zu bahnbrechenden Innovationen, unterschiedlichen Organisations- und Managementphilosophien sowie wichtigen geistigen Eigentumsrechten zu erhalten.

57 Bundesverband Deutsche Startups e.V., Deutscher Startup Monitor 2021, Oktober 2021, S. 36: https://deutschestartups.org/wp-content/uploads/2021/10/Deutscher-Startup-Monitor_2021.pdf (abgerufen am 24. April 2022))

Den Zugang zu Spitzenforschung und -entwicklung unter geostrategischen Gesichtspunkten betrachten. Die Bundesregierung sollte neben offensiven Maßnahmen wie der Bereitstellung von geistigem Eigentum, der Schaffung von Anreizen für deren Übernahme sowie für die Zusammenarbeit mit dem Privatsektor auch mögliche defensive Instrumente prüfen, mit denen sich die unerwünschte Weitergabe von geistigem Eigentum verhindern lässt, insbesondere im Bereich der Deep Technology.

Den digitalen Binnenmarkt zu einer geopolitischen Priorität machen. Die Zersplitterung des digitalen Marktes in Europa ist nach wie vor ein Hemmschuh für Skalierbarkeit und ein zentrales Problem bei der Ausschöpfung von Europas geopolitischem Potenzial im Technologiebereich. Deutschland sollte eine führende Rolle bei der Verwirklichung des digitalen Binnenmarkts spielen, einschließlich der Bemühungen, den freien Datenfluss und sektorspezifische Datenräume in der EU zu fördern, die Registrierung von Start-ups zu vereinfachen und einen einheitlichen Kapitalmarkt aufzubauen, der zu grenzüberschreitende Investitionen anregt. Diese Bemühungen werden besonders wichtig sein, um mehr europaweite offene Standards und Open-Source-Software zu schaffen und damit die FuE-Basis für widerstandsfähige europaweite Innovationen zu verbreitern.

Die Förderung von IKT-Talenten als kritische Infrastruktur betrachten. Die deutsche Einwanderungspolitik hat begonnen, das digitale Innovationsökosystem zu unterstützen. Dank eines Universitäts- und Hochschulsystems, das internationale Studierende aufnimmt, sowie liberalisierten Aufenthalts- und Arbeitsbedingungen und der Möglichkeit, Englisch als Arbeitssprache zu nutzen, konnte Deutschland Humankapital anziehen. Jetzt muss es jedoch auch die Anwerbung und Bindung von IT-Spitzentalenten zum nationalen strategischen Ziel erklären. Um dies zu erreichen, müssen die Forschungsinstitute auch für die Ausstattung, Ressourcen, Forschungsinfrastruktur sowie wettbewerbsfähigen Gehälter und nötige Flexibilität bei der Einstellung sorgen, die die US-amerikanische, britische und chinesische Konkurrenz bereits anbietet.

KAPITEL 3

Technologie- und Industriepolitik im neuen Systemwettbewerb

Wie Deutschland seine technologischen Fähigkeiten und industrielle Stärke bewahren kann

KAPITELÜBERSICHT

Zentrale Erkenntnisse

1 Als eine der weltweit am stärksten globalisierten Volkswirtschaften steht Deutschland vor der Herausforderung, sich in einem umkämpften internationalen Marktumfeld zu positionieren, das geprägt ist von aggressiven Subventionsstrategien sowie einem globalen Wettlauf um die Kontrolle von Schlüsseltechnologien wie hochentwickelten Chips und fragilen Lieferketten für kritische Komponenten. Hinzu kommen die aufgrund des russischen Angriffskriegs gegen die Ukraine gestiegenen Energiepreise, die die deutsche Industrie zusätzlich belasten.

2 Zugleich durchläuft Deutschlands Industriewirtschaft einen grundlegenden Wandel von hochpräziser Fertigung zu systembasierten industriellen Produkten. Im Zuge dieses Wandels wird der Zugang zu digitalen Spitzentechnologien zu einer wichtigen Grundlage für die künftige industrielle Wettbewerbsfähigkeit des Landes. Dennoch tut sich Deutschland schwer damit, in schnell wachsenden Märkten wie denen für Cloud- und Edge-Infrastrukturen Wert zu schöpfen. Außerdem ist das Land Risiken ausgesetzt, die sich aus seiner Exposition gegenüber nicht vertrauenswürdigen Technologieanbietern sowie möglichen geopolitischen Spannungen in fragilen Hardware-Lieferketten ergeben.

3 Folglich skizziert die Bundesregierung die Konturen einer neuen Technologie- und Industriepolitik. Diese Bemühungen werden jedoch durch die uneinheitliche Umsetzung und komplexe Koordinierung subnationaler (länderübergreifender) und supranationaler (EU-weiter) Industriepolitik erschwert.

4 Um Deutschlands wirschaftliche Wettbewerbsfähigkeit aufrechtzuerhalten, sollte die Bundesregierung die Stärken und Schwächen des Landes im Bereich kritischer Technologien systematisch evaluieren, die Initiativen von Bund und Ländern besser aufeinander abstimmen und international kooperieren – innerhalb der EU, aber auch mit gleichgesinnten Partnern außerhalb der EU –, um komparative Vorteile besser zu nutzen.

Die Haltung der Bundesregierung hinsichtlich der Rolle von Industriepolitik befindet sich im Wandel. Insbesondere im Bereich der Digitalpolitik, die sich lange Zeit auf Datenregulierung, Wettbewerb und offene Märkte konzentriert hat, muss sie sich nun auf ein neues globales Umfeld einstellen: Dieses Umfeld ist von aggressiven Subventionsstrategien und einem globalen Wettlauf um die Kontrolle von Schlüsseltechnologien wie hochentwickelten Chips und fragilen Lieferketten für kritische Komponenten geprägt. China ist zum direkten Wettbewerber geworden, seitdem das Land seinen Fokus von arbeitsintensiver Produktion auf fortschrittliche Fertigung in Bereichen wie elektrische und autonome Fahrzeuge, intelligente Maschinen, Robotik und Netzwerkausrüstung verlagert hat und somit in der Wertschöpfungskette aufsteigt. Währenddessen investieren die USA verstärkt in die eigene innovationsorientiere industrielle Basis, um ihre Vormachtstellung in Bereichen wie fortschrittlichem Chipdesign und KI zu verteidigen.

Diese Herausforderungen haben Deutschland eine aktivere Industriepolitik abgefordert. Auf dem Spiel steht nichts Geringeres als der künftige wirtschaftliche Wohlstand des Landes: Deutschlands technologisch-industrielle Basis ringt mit der Verlagerung von Präzisionsfertigung auf systembasierte industrielle Produkte, die sich auf Daten und Algorithmen, digitale Infrastruktur und Halbleiterlieferketten stützen. Sofern es Deutschland nicht gelingt, seine starke Stellung in den globalen Hightech-Wertschöpfungsketten durch eine geschickte Technologie- und Industriepolitik zu bewahren, werden seine wirtschaftliche Basis und sein geopolitischer Einfluss schrumpfen. Um dies zu vermeiden, muss die Bundesregierung eine solche Politik mit den Grundsätzen des offenen Marktes und der Wahlfreiheit, die der deutschen Wirtschaft zugrunde liegen, sowie den geopolitischen Erfordernissen zur Schaffung strategischer Interdependenzen mit engen Verbündeten und Partnern in Einklang bringen.

Status quo

Der industrielle Wandel macht es für Deutschland notwendig, seine Vorreiterrolle in der Automobilindustrie, im Maschinenbau, in der Medizintechnik und in anderen Sektoren mit Wertschöpfungsketten für Querschnittstechnologien wie KI und mit neu entstehenden digitalen Ökosystemen zu verbinden.[58] Dies führt zu unmittelbaren Herausforderungen für die industrielle Wettbewerbsfähigkeit des Landes, unter anderem da die KMUs – die berühmten Hidden Champions des Mittelstands – neue Technologien bisher verhältnismäßig wenig nutzen. Lediglich sechs Prozent der mittelständischen Unternehmen haben zum Beispiel KI-Strategien eingeführt, um ihre Wettbewerbsfähigkeit zu erhalten.[59] Der Großteil des Mittelstands (77,1 Prozent) gibt außerdem an, den Vorteilen des Datenaustauschs ambivalent gegenüberzustehen – trotz seiner Bedeutung bei der Sicherung von Wettbewerbsvorteilen durch die Optimierung industrieller Prozesse und die Entwicklung neuer Produkte.[60] Darüber hinaus ist die Plattformlandschaft des Landes in Bezug auf das industrielle Internet der Dinge (Industrial Internet of Things, IIoT) und den Datenaustausch fragmentiert. Initiativen zur Schaffung europäischer Datenräume wie Gaia-X kommen nur langsam voran, was auch auf interne Konflikte bezüglich der Beteiligung nichteuropäischer Akteure zurückzuführen ist und auf die politische Herausforderung, ein gemeinsames europäisches Ökosystem auf der Grundlage von Interoperabilität und Vertrauen voranzubringen.[61]

Deutschlands industrielle Basis weist jedoch auch Innovationsstärken auf. So setzt das Land auf Vernetzung und Automatisierung und ist weltweit der viertgrößte Investor im Bereich des Internet der Dinge (IoT),[62] das internetfähige Geräte wie Sensoren und Messgeräte umfasst. Auf Deutschland entfällt zudem ein Drittel der in Europa eingesetzten Industrieroboter.[63] KI-Entwicklung im eigenen Land deckt bereits die Hälfte der deutschen Industrienachfrage ab.[64] Einigen Schätzungen zufolge könnten KI-basierten Lösungen das Bruttoinlandsprodukt (BIP) bis 2030 um 11,3 Prozent beziehungsweise 430 Milliarden Euro steigern.[65] Politische Maßnahmen zur schnelleren Überführung von Deutschlands FuE-Stärken in datenintensive und systemzentrierte Anwendungen im Industriebereich sind daher zentral zur Bewahrung seiner Stellung als führendes Technologieland.[66]

Im Zuge dieser Verlagerung hin zu stärker datengetriebener Wertschöpfung wird der Zugang zu digitalen Spitzentechnologien zu einer wichtigen Grundlage für die künftige industrielle Wettbewerbsfähigkeit des Landes. In diesem Zusammenhang ist die Verfügbarkeit einer sicheren und zuverlässigen Cloud- und Edge-Computing-Infrastruktur von großer

58 KI, eine der wichtigsten Impulsgeberinnen für diesen Wandel, wird bis 2030 voraussichtlich dazu beitragen, dass das globale Bruttoinlandsprodukt (BIP) um etwa 16 Prozent steigt. Das macht sie zum wichtigsten Motor der Weltwirtschaft. Jacques Bughin et al., Notes from the AI frontier: Modeling the impact of AI on the world economy, in: McKinsey & Company Discussion Paper, September 2018: https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy (abgerufen am 19. Mai 2022).

59 J.P. Singh, Deutschland kann Krise – aber auch KI?, in: Tagesspiegel Background, 6. September 2021: https://background.tagesspiegel.de/digitalisierung/deutschland-kann-krise-aber-auch-ki (abgerufen am 19. Mai 2022). Schätzungen zufolge haben insgesamt nur 15 Prozent der deutschen Industrieunternehmen KI-Lösungen implementiert. In den USA sind es 25 Prozent und in China 23 Prozent. acatech, Künstliche Intelligenz in der Industrie, in: acatech Horizonte, Juli 2020, S. 54: https://www.acatech.de/publikation/acatech-horizonte-ki-in-der-industrie/download-pdf/?lang=de (abgerufen am 19. Mai 2022).

60 Gemäß einer Umfrage unter 111 KMU aus dem Jahr 2018. Mit 90,7 Prozent bereitet den Unternehmen der unbefugte Zugriff Dritter auf ihre Daten die größten Sorgen. Institut der deutschen Wirtschaft, Datenwirtschaft in Deutschland. Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, Februar 2021, S. 40: https://www.iwkoeln.de/fileadmin/user_upload/Studien/Gutachten/PDF/2021/Hemmnisse_der_Datenwirtschaft_Studie.pdf (abgerufen am 19. Mai 2022).

61 Silke Hahn, Gaia-X in der Unternehmerdiskussion: Tolle Vision, wann kommt die Realität?", in: Heise Online, 2. Februar 2022: https://www.heise.de/news/Gaia-X-in-der-Unternehmerdiskussion-Tolle-Vision-wann-kommt-die-Realitaet-6340570.html (abgerufen am 19. Mai 2022).

62 Auf Deutschland entfallen rund fünf Prozent der weltweiten IoT-Investitionen. Derzeit wird das Land nur von den USA, China und Japan übertroffen. United Nations Conference on Trade and Development, in: Digital Economy Report 2019. Value Creation and Capture: Implications for Developing Countries, Juli 2019, S. 7: https://unctad.org/system/files/official-document/der2019_en.pdf (abgerufen am 19. Mai 2022).

63 In Deutschland waren 2021 ca. 230.000 Industrieroboter im Einsatz. International Federation of Robots, Jeder dritte Industrie-Roboter in der EU wird in Deutschland installiert, 28. Oktober 2021: https://ifr.org/downloads/press2018/Germany-2021-OCT-IFR_press_release_industrial_robots.pdf (abgerufen am 19. Mai 2022).

64 Die Ergebnisse von Umfragen unter 235 deutschen Unternehmen aus dem Jahr 2021 zeigen, dass etwa 46 Prozent der externen KI-Anwendungen, die von deutschen Unternehmen erworben oder gemietet werden, von deutschen Entwicklungsfirmen stammen. Nur auf die USA entfällt ein weiterer bedeutender Anteil an KI-Lösungsanbietern (38 Prozent). Achim Berg, Künstliche Intelligenz. Wo steht die deutsche Wirtschaft?, April 2021, S. 10: https://www.bitkom-research.de/system/files/document/Bitkom%20Charts%20K%C3%BCnstliche%20Intelligenz%2021%2004%202021_final.pdf (abgerufen am 19. Mai 2022).

65 Die Automobilindustrie und das Gesundheitswesen werden – basierend auf dem deutschen BIP von 2018 – voraussichtlich am stärksten von diesem Wachstum profitieren. PwC, Künstliche Intelligenz sorgt für Wachstumsschub. Wie groß ist das Potenzial und wie kann Ihr Unternehmen davon profitieren?, Februar 2019: https://www.pwc.de/de/digitale-transformation/business-analytics/kuenstliche-intelligenz-sorgt-fuer-wachstumsschub.html (abgerufen am 19. Mai 2022).

66 Tyson Barker und David Hagebölling, Digitale Innovation im geopolitischen Kontext. Stärken und Schwächen von Deutschlands digitalem Innovationsökosystem, DGAP Bericht, Deutsche Gesellschaft für Auswärtige Politik, August 2022: https://dgap.org/system/files/article_pdfs/dgap-report-2022-DE-Innovation%20Ecosystems.pdf (abgerufen am 31. Oktober 2022).

Bedeutung.[67] Dies liegt nicht nur daran, dass die Führungsposition Deutschlands in Schlüsselindustrien wie dem autonomen Fahren, der industriellen Fertigung und dem intelligenten Stromnetz-Management zunehmend von der cloudbasierter Verarbeitung großer Datenmengen abhängt.[68] Es hat auch damit zu tun, dass insbesondere dezentrale Cloud-Infrastrukturen das Fundament für das schnell wachsende IIoT und die Verfügbarkeit einer hochsicheren Datenverarbeitung mit geringer Latenz nahe an der Datenquelle, der sogenannten „Edge" (dem „Rand"), bilden werden.[69] Prognosen zufolge wird Deutschland bis 2025[70] der größte und am schnellsten wachsende Markt für Edge Computing in Europa sein, wenn der Großteil der Geschäftsdaten außerhalb herkömmlicher, zentralisierter Rechenzentren verarbeitet wird.[71]

Und doch kämpft Deutschland, wie ganz Europa, damit, im schnell wachsenden Markt für Cloud- und Edge-Technologie Wert zu schöpfen. Deutsche Cloud-Anbieter wie T-Systems[72] und SAP[73] setzen auf operative Partnerschaften mit US-Hyperscalern, um fortschrittliche Cloud-Technologien mit Datenschutzanforderungen in Einklang zu bringen, insbesondere im Hinblick auf die Begrenzung der rechtlichen Grundlagen und technischen Möglichkeiten nicht-europäischer Akteure für den Zugriff auf Daten, die auf europäischen Servern gespeichert sind.[74] Zugleich verändert die Verschiebung hin zu Edge Computing auch die Möglichkeiten, komparative Vorteile zu nutzen. Im Gegensatz zu einer universellen Cloud-Infrastruktur zeichnet sich Edge Computing durch eine hohe geografische Verteilung der Datenverarbeitung und Ausrichtungen an den spezifischen Anforderungen bestimmter Branchen und Anwendungen aus.[75] Das könnte sich auch auf den Wettbewerb zwischen großen Cloud-Anbietern und etablierten Telekommunikationsunternehmen auswirken.

Eine weitere Herausforderung stellt Deutschlands uneindeutige Strategie für sichere Telekommunikationsnetze dar, welche zunehmend mit cloudbasierten Datenverarbeitungsinfrastrukturen verschmelzen.[76] Chinesische Anbieter spielen derzeit eine bedeutende Rolle in deutschen Telekommunikationsnetzen – so stellt Huawei allein fast die Hälfte der 4G-Basisstationen bereit.[77] Deutschland versucht, den Einfluss chinesischer Unternehmen bei 5G-Netzen zu begrenzen, ist aber nicht bereit, zu europäischen Anbietern zu wechseln.[78] Immerhin haben die deutschen Telekommunikationsbetreiber ein starkes kommerzielles Interesse daran, Anbieter von Netzwerkausrüstung zu diversifizieren und nicht ausschließlich auf die europäischen Unternehmen Nokia und Ericsson – die zweit- und drittgrößten Anbieter von 5G-Basisstationen – zu setzen.[79] Entsprechend

67 Mehr als 80 Prozent der deutschen Unternehmen nutzen Cloud Computing. Bitkom Research, Trendstudie Digitalisierung 2019, November 2019: https://www.bitkom-research.de/de/Trendstudie-Digitalisierung-19 (abgerufen am 19. Mai 2022).

68 Der europäische Cloud-Markt, von dem Deutschland etwa ein Fünftel ausmacht, wird sich bis 2030 voraussichtlich auf rund 500 Milliarden Euro verzehnfachen. Martin Möhle, Cloud Computing in Germany 2021, in: Future Processing 11. Januar 2021: https://www.future-processing.com/blog/cloud-computing-in-germany-2021/ (abgerufen am 19. Mai 2022).

69 Edge Computing bezeichnet die Datenverarbeitung an der „Edge", also am Rand des Netzwerkes und damit näher am Ort der Datenerhebung. Ein wesentlicher Vorteil ist, dass zeitaufwändige Datenübertragungen über große Entfernungen vermieden werden, was eine höhere Geschwindigkeit und geringe Latenz ermöglicht.

70 Einigen Schätzungen zufolge könnten bis zum Jahr 2025 75 Prozent der Datenverarbeitung an die Edge verlagert werden. Rob van der Meulen, What Edge Computing Means for Infrastructure and Operations Leaders, in: Gartner, 3. Oktober 2018: https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders (abgerufen am 19. Mai 2022).

71 Reply, From Cloud to Edge, Dezember 2020, S. 5: https://www.reply.com/en/Shared%20Documents/from-cloud-to-edge-EN.pdf (abgerufen am 19. Mai 2022).

72 T-Systems, Investition in Technologie und gemeinsame Innovation, um Kundenbedürfnisse in Deutschland zu erfüllen, 8. September 2021: https://www.t-systems.com/de/de/newsroom/news/t-systems-und-google-cloud-bauen-souveraene-cloud-fuer-deutschland-450414 (abgerufen am 19. Mai 2022).

73 SAP, Startschuss zur ersten souveränen Cloud-Plattform für den öffentlichen Sektor in Deutschland: SAP und Arvato Systems kündigen Partnerschaft an, 3. Februar 2022: https://news.sap.com/germany/2022/02/cloud-plattform-public-sector-arvato/ (abgerufen am 19. Mai 2022).

74 Diese Partnerschaften zielen insbesondere darauf ab, deutschen Unternehmen und dem öffentlichen Sektor Cloud-Dienste anzubieten, die die rechtlichen Grundlagen und technischen Zugriffsmöglichkeiten gemäß Gesetzen wie dem US-amerikanischen CLOUD Act und FISA Act sowie dem chinesischen Cybersicherheitsgesetz einschränken.

75 Brandon Moser, Edge Computing Examples Across Vertical Industries, 9. September 2021: https://www.digi.com/blog/post/edge-computing-examples-across-vertical-industries (abgerufen am 5. Oktober 2022).

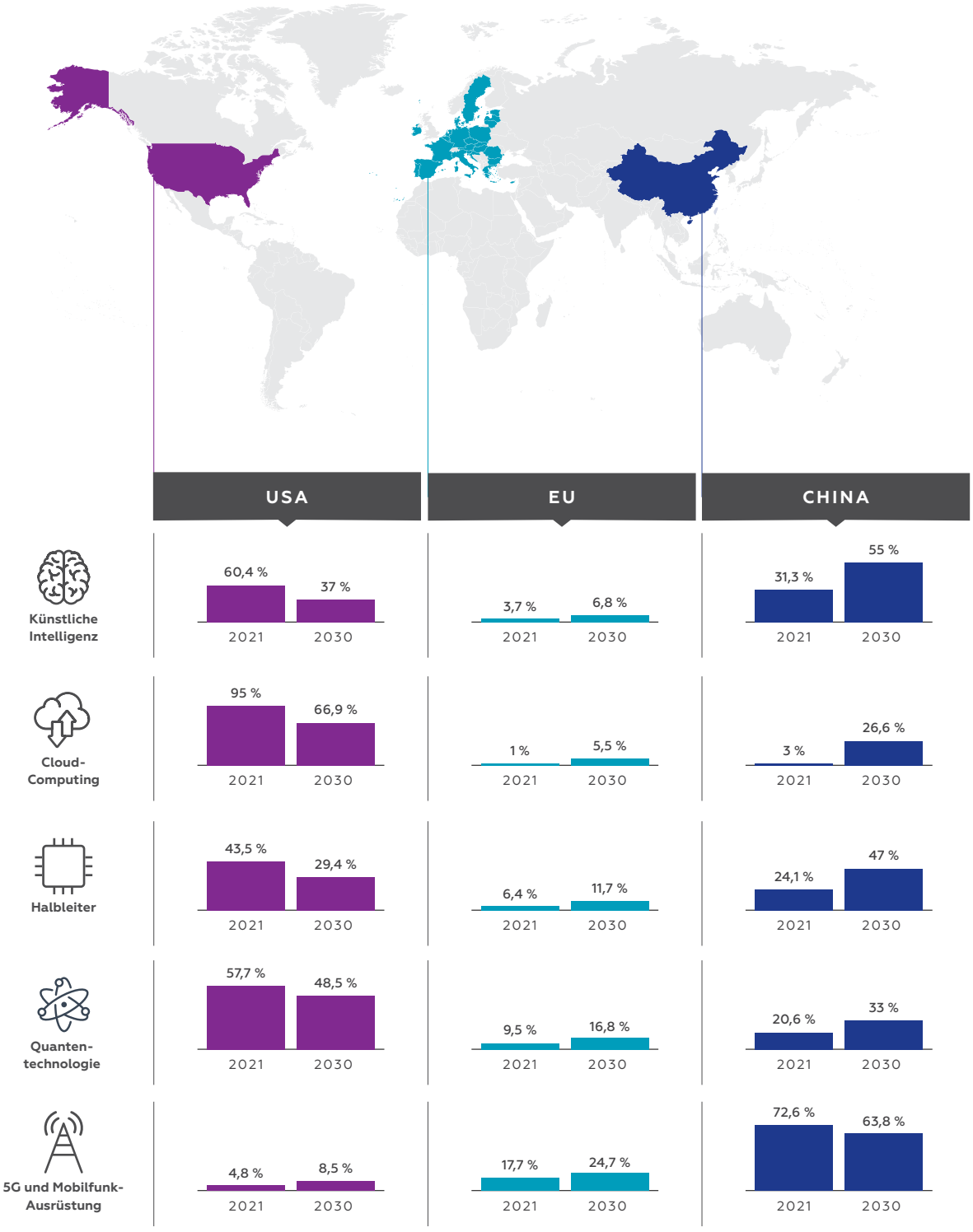
76 Die 5G-Technologie wird seit 2019 für öffentliche Mobilfunknetze angeboten, aber viele Anwendungen sind nach wie vor nur für Campusnetze verfügbar, die Menschen und Systeme in Produktionsstätten, Krankenhäusern, Universitäten und Häfen miteinander verbinden. Bundesministerium für Wirtschaft und Energie (BMWi), Leitfaden 5G-Campusnetze – Orientierungshilfe für kleine und mittelständische Unternehmen, April 2020: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/leitfaden-5G-campusnetze-orientierungshilfe-fuer-kleine-und-mittelstaendische-unternehmen.pdf?__blob=publicationFile&v=8 (abgerufen am 19. Mai 2022).

77 Deutschland ist in dieser Hinsicht kein Sonderfall. Ungefähr die Hälfte aller europäischen Länder verfügt über einen ähnlich hohen Anteil an Ausrüstung chinesischer Hersteller. Deutsche Welle, Germany pressures Huawei to meet security requirements, 21. Juni 2019: https://www.dw.com/en/germany-pressures-huawei-to-meet-security-requirements/a-49294841 (abgerufen am 19. Mai 2022).

78 Dies erfolgt unter anderem durch strengere Anforderungen an die „Vertrauenswürdigkeit" von Herstellern von Ausrüstung im Rahmen des deutschen IT-Sicherheitsgesetzes 2.0 (2021).

79 Zoefie Cheng, Market Share of Top Three Suppliers of Base Stations Projected to Undergo Slight Decline in 2021 While Fourth-Ranked Samsung Scores Wins in Overseas Markets, Says TrendForce, in: TrendForce, 28. Juli 2021: https://www.trendforce.com/presscenter/news/20210728-10872.html (abgerufen am 19. Mai 2022).

5 – BEWERTUNG DER FÜHRUNGSROLLE EUROPAS BEI SCHLÜSSEL-TECHNOLOGIEN DURCH EXPERTINNEN UND EXPERTEN: 2021 VS. 2030



Quelle: Illustration basierend auf Daten in Kaan Sahin, Tyson Barker, Europe's Capacity to Act in the Global Tech Race, Deutsche Gesellschaft für Auswärtige Politik, April 2021: https://dgap.org/sites/default/files/article_pdfs/210422_report-2021-6-en-tech.pdf (abgerufen am 14. September 2022).

unterstützt die Bundesregierung auch die O-RAN Alliance,[80] eine wichtige Industrie- und Forschungsinitiative mit dem Ziel, interoperable Standards für Mobilfunknetze zu definieren[81] – trotz Sicherheitsbedenken bezüglich der O-RAN-Architektur[82] und Unstimmigkeiten mit wichtigen Partnern, darunter Frankreich und der Europäischen Kommission, über die Auswirkungen von O-RAN auf Europas führende 5G-Unternehmen.

Deutschland muss sich auch mit Risiken in der fragilen Lieferkette für Halbleiter auseinandersetzen, der Kerntechnologie, die dem IIoT, intelligenten Stromnetzen, elektrischen und autonomen Fahrzeugen sowie anderen industriellen Komponenten und Produkten zugrunde liegt. Der europäische Anteil an der weltweiten Halbleiterproduktion ist von 44 Prozent im Jahr 1990 auf heute noch etwa acht Prozent gefallen.[83] 2020 rangierte Infineon gemessen an seinem Umsatz als einziges deutsches Unternehmen (und eines von lediglich vier europäischen) unter den 20 größten Halbleiterherstellern.[84] Mehr als drei Viertel der Chipproduktion findet heute in Asien, vor allem in Taiwan, Südkorea und China statt.[85] Spannungen in dieser geopolitisch heiklen Region hätten erhebliche wirtschaftliche Auswirkungen für Deutschland, welche wahrscheinlich weit über die Folgen des russischen Gaslieferstopps hinausgehen würden.

In diesem hochkomplexen Markt bedarf es eines strategischen und umsichtigen Ansatzes in der Industriepolitik Deutschlands und seiner EU-Partner. Angesichts des für den Markteintritt erforderlichen hohen Kapiteleinsatzes[86] erfordert eine Rückverlagerung (fortschrittlicher) Produktionskapazitäten nach Europa umfangreiche und langfristige Subventionen.[87] Dies bedeutet, dass eine Diversifizierung der globalen Beschaffungsmöglichkeiten prioritär sein sollte, ebenso wie die Identifizierung von komparativen Vorteilen in der Wertschöpfungskette für Halbleiter. Dabei ist wichtig, dass Deutschland in bestimmten Anbietermärkten und Produktionssegmenten nach wie vor noch Stärken aufweist. Auf hoher Fertigungspräzision beruhende Komponenten und chemische Spezialprodukte von deutschen Unternehmen wie Zeiss und BASF sind wichtige Bestandteil in der Halbleiterproduktion.[88] Infineon, Bosch, STMicroelectronics und NXP zeichnen sich wiederum durch die Herstellung von Spezialchips aus;[89] unter anderem für industrielle Anwendungen, Fahrzeuge und den Verteidigungssektor.[90]

Dennoch muss Deutschland zukünftige, tiefgreifende Veränderungen im Blick behalten. Immer mehr (industrielle) Unternehmen designen ihre eigenen Chips, während die Inhaber geistigen Eigentums und die Anbieter von Tools für Electronic Design Automation (EDA) fast ausschließlich in den USA

80 Bundesministerium für Digitales und Verkehr (BMDV), BMVI startet Open RAN-Förderung, 9. November 2021: https://www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2021/126-bmvi-startet-open-ran-foerderung.html (abgerufen am 19. Mai 2022).

81 Die 2018 gegründete O-RAN Alliance ist eine Initiative von Netzbetreibern, Anbietern und Forschungseinrichtungen, die darauf abzielt, Industriestandards für „offene, virtualisierte und vollständig interoperable Mobilfunknetze" zu entwickeln.

82 Das Bundesamt für Sicherheit in der Informationstechnik (BSI) äußert in einer Risikoanalyse 2021 Bedenken hinsichtlich der Sicherheit von Open RAN. Laut der Studie orientieren sich die Open-RAN-Spezifikationen am Paradigma „security/privacy by design/default", und das System „beinhaltet vielfältige Sicherheitsrisiken". Stefan Köpsell et al., Open-RAN Risikoanalyse 5GRANR, in: Bundesamt für Sicherheit in der Informationstechnik, Februar 2022, S. 73: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/5G/5GRAN-Risikoanalyse.pdf;jsessionid=9E7EE4E27FFCF263EC0710664967F076.internet472?__blob=publicationFile&v=9 (abgerufen am 19. Mai 2022).

83 Antonio Varas et al., Government Incentives and US Competitiveness in Semiconductor Manufacturing, in: Boston Consulting Group, September 2020, S. 7: https://www.semiconductors.org/wp-content/uploads/2020/09/Government-Incentives-and-US-Competitiveness-in-Semiconductor-Manufacturing-Sep-2020.pdf (abgerufen am 19. Mai 2022)

84 GlobalData, Top 20 semiconductor companies by revenue recorded healthy growth, days Global Data, 8. Juli 2021: https://www.globaldata.com/top-20-semiconductor-companies-revenue-recorded-healthy-growth-says-globaldata/ (abgerufen am 21. Juni 2022).

85 Alex Irwin-Hunt, In charts: Asia's manufacturing dominance, in: Financial Times, 24. März 2021: https://www.ft.com/content/2b0c172b-2de9-4011-bf40-f4242f4673cc (abgerufen am 19. Mai 2022).

86 Das taiwanesische Unternehmen TSMC produziert rund 90 Prozent der modernsten Chips. Yang Jie et al., The World Relies on One Chip Maker in Taiwan, Leaving Everyone Vulnerable, in: The Wall Street Journal, 19. Juni 2021: https://www.wsj.com/articles/the-world-relies-on-one-chip-maker-in-taiwan-leaving-everyone-vulnerable-11624075400 (abgerufen am 19. Mai 2022).

87 Die Kosten für die sich derzeit im Bau befindliche Produktionsanlage von TSMC in Arizona werden beispielsweise auf zwölf Milliarden Dollar geschätzt. Sebastian Moss, TSMC starts work on $12bn Arizona semiconductor fab, gets funding for Japanese chip R&D, in: DCD, 2. Juni 2021: https://www.datacenterdynamics.com/en/news/tsmc-starts-work-on-12bn-arizona-semiconductor-fab-gets-funding-for-japanese-chip-rd/ (abgerufen am 19. Mai 2022).

88 Zeiss, Semiconductor Manufacturing Optics: https://www.zeiss.com/semiconductor-manufacturing-technology/products/semiconductor-manufacturing-optics.html (abgerufen am 30. September 2022); BASF, Chemical Solutions for Semiconductors: https://electronics-electric.basf.com/global/en/electronics/semiconductors_solutions.html (abgerufen am 30. September 2022).

89 Die Märkte für Automobil-, Industrie- und Kommunikationselektronik gehören zu den am schnellsten wachsenden Märkten und lassen sogar das Verbrauchersegment hinter sich. ICInsights, Outlook Remains Bright for Automotive Electronic Systems Growth, 19. November 2018: https://www.icinsights.com/news/bulletins/Outlook-Remains-Bright-For-Automotive-Electronic-Systems-Growth/ (abgerufen am 19. Mai 2022).

90 Jan-Peter Kleinhans, Nurzat Baisakova, The global semiconductor value chain. A technology primer for policy makers, in: Stiftung Neue Verantwortung, Oktober 2020.

ansässig sind.[91] Fortschritte im Bereich Quanten- und Hochleistungs-Computing bieten eine Chance für Deutschland sich zukünftig eine stärkere Position im Hardware-Bereich zu sichern.[92] Doch trotz Deutschlands Exzellenz in der Grundlagenforschung fehlt es seinen Unternehmen bisher noch an wettbewerbsfähigen Hardware-Produkten[93] und das in einem sich immer schneller entwickelnden Markt.[94]

Aktueller politischer Ansatz

Die Bundesregierung ist sich dieser Veränderungen bewusst und skizziert derzeit die Konturen eines neuen industriepolitischen Ansatzes. In mehreren richtungsweisenden Dokumenten, vor allem in der „Hightech-Strategie 2025“ (veröffentlicht 2018)[95] und der „Industriestrategie 2030“ (veröffentlicht 2019),[96] hat die damalige Bundesregierung eine strategischere Perspektive für kritische Technologien entwickelt, die sich auch in den 750 Milliarden Euro schweren EU-Plan „NextGenerationEU“ einbettet.[97] Die deutsche Politik bleibt ihren langjährigen ordoliberalen Grundsätzen von offenen Märkten und Wahlfreiheit treu, gesteht dem Staat aber nun eine größere Rolle zu, um die industrielle Wertschöpfung zu erhalten. Die durch die Pandemie beeinträchtigte Wirtschaftsentwicklung hat diese Sichtweise weiter verankert und Deutschland dazu veranlasst, seinen 130 Milliarden Euro schweren Aufbauplan als „Paket für die Zukunft“ zu bezeichnen, das digitale Investitionen für die wirtschaftliche Erholung priorisiert.[98]

Deutschland hat beträchtliche öffentliche Investitionen in kritische Technologien angekündigt. Die erste, 2018 veröffentlichte KI-Strategie des Landes sah Investitionen in Höhe von drei Milliarden Euro vor, die später auf fünf Milliarden Euro aufgestockt wurden,[99] um bis 2025 den Nachwuchs, die verfügbare Rechenkapazität und international konkurrenzfähige KI-Ökosysteme zu fördern.[100] Außerdem hat die Bundesregierung 2019 650 Millionen Euro bereitgestellt, um die deutsche Quantenphysikforschung zu stärken.[101] Diese Mittel wurden im Jahr 2021 auf zwei Milliarden Euro erhöht, mit dem ausdrücklichen Ziel, bis 2025 einen wettbewerbsfähigen Quantencomputer „Made in Germany“ zu entwickeln.[102]

Dennoch birgt dieser Übergang zu einer stärker staatlich gelenkten technologieorientierten Industriepolitik Herausforderungen. Deutschland mag die

91 Jan-Peter Kleinhans, The lack of semiconductor manufacturing in Europe. Why the 2nm fab is a bad investment, in: Stiftung Neue Verantwortung, April 2021, S. 20: https://www.stiftung-nv.de/sites/default/files/eu-semiconductor-manufacturing.april_.2021.pdf (abgerufen am 19. Mai 2022).

92 Quantencomputing (QC) befindet sich zwar noch in einem frühen Stadium, birgt aber großes Potenzial. QC baut auf Quantenphysik auf und nutzt „Qubits“, die im Gegensatz zu klassischen „Bits“ gleichzeitig verschiedene Werte annehmen können. Dies eröffnet Rechenmöglichkeiten, die weit über die der klassischen digitalen Datenverarbeitung hinausgehen. Quantencomputer sind bei bestimmten Rechenaufgaben, die für die Wettbewerbsfähigkeit der deutschen Industrie maßgeblich sind, exponentiell leistungsfähiger, z. B. bei der Medikamentenherstellung, der Echtzeitverarbeitung von Industrie- und Fahrzeugsensordaten und dem Lieferkettenmanagement. Die Technologie geht mit großem wirtschaftlichem Potenzial einher und wird die Kryptographie verändern, da sie selbst fortschrittliche klassische Verschlüsselungsmethoden unbrauchbar macht.

93 Das Fraunhofer-Forschungskonsortium beispielsweise ist auf Cloud-basierte Quantencomputing-Ressourcen aus den USA und den physischen Zugang zum Q System One von IBM in Ehningen angewiesen. Fraunhofer Gesellschaft, “Fraunhofer Competence Network Quantum Computing: Understanding and using qubits!”: https://www.fraunhofer.de/de/institute/kooperationen/fraunhofer-kompetenznetzwerk-quantencomputing.html (abgerufen am 19. Mai 2022).

94 Während IBMs Q System One mit 27 Qubits arbeitet, will das Unternehmen bis 2023 bereits einen 1000+ Qubit-Chip fertigstellen. Jay Gambetta, “IBM’s roadmap for scaling quantum technology,” IBM (15. September 2020): https://research.ibm.com/blog/ibm-quantum-roadmap (abgerufen am 19. Mai 2022)

95 Bundesministerium für Bildung und Forschung (BMBF), Forschung und Innovation für die Menschen. Die Hightech-Strategie 2025, September 2018: https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/1/31431_Forschung_und_Innovation_fuer_die_Menschen.pdf?__blob=publicationFile&v=6 (abgerufen am 19. Mai 2022).

96 Bundesministerium für Wirtschaft und Energie (BMWi), Industriestrategie 2030. Leitlinien für eine deutsche und europäische Industriepolitik, November 2019: https://www.bmwk.de/Redaktion/DE/Publikationen/Industrie/industriestrategie-2030.pdf?__blob=publicationFile (abgerufen am 19. Mai 2022).

97 Europäische Kommission, Lage der Union: Kommission schlägt einen Weg in die digitale Dekade zur Verwirklichung des digitalen Wandels in der EU bis 2030 vor, 15. September 2021: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4630 (abgerufen am 19. Mai 2022).

98 Bundesregierung, Milliardenhilfe beschlossen, Juni 2020: https://www.bundesregierung.de/breg-de/themen/coronavirus/konjunkturpaket-geschnuert-1757558 (abgerufen am 19. Mai 2022).

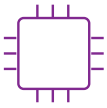
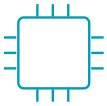
99 Bundesministerium für Wirtschaft und Klimaschutz (BMWK), Kabinett beschließt Fortschreibung der KI Strategie der Bundesregierung, 2. Dezember 2020: https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2020/12/20201202-kabinett-beschliesst-fortschreibung-ki-strategie-bundesregierung.html (abgerufen am 19. Mai 2022).

100 Bundesregierung, Die entscheidende Zukunftstechnologie des 21. Jahrhunderts, Dezember 2020: https://www.bundesregierung.de/breg-de/suche/fortschreibung-ki-strategie-1824340 (abgerufen am 24. Mai 2022)

101 Stefan Krempl, Zitis: Staatliche Hacker sollen Verschlüsselung mit Quantencomputer knacken, in : Heise Online, 26. September 2018: https://www.heise.de/newsticker/meldung/Zitis-Staatliche-Hacker-sollen-Verschluesselung-mit-Quantencomputer-knacken-4175352.html (abgerufen am 19. Mai 2022).

102 Sebastian Grüner, „Deutschland fördert Quantencomputer mit 2 Milliarden Euro“, Golem.de, 11. Mai 2021: https://www.golem.de/news/grundlagenforschung-deutschland-foerdert-quantencomputer-mit-2-milliarden-euro-2105-156422.html (abgerufen am 19. Mai 2022).

6 – DEUTSCHLANDS BETEILIGUNG AN IPCEIS FÜR DIGITALE TECHNOLOGIEN

BEREICH	ZEITPLAN	MITGLIEDSTAATEN	DEUTSCHE FÖRDERMITTEL	TECHNOLOGIE-SCHWERPUNKT	PROJEKTE
Mikroelektronik I 	**2018**: Genehmigung durch die EU-Kommission **2020**: Projektstart **2022**: (geplantes) Projektende	**4 EU-Mitgliedstaaten:** Frankreich, Deutschland, Italien und Österreich (2021 beigetreten) + das Vereinigte Königreich	Insgesamt: ≈ 3,6 Mrd. € Öffentlich: 1 Mrd. € Privat: 2,6 Mrd. €	Energieeffiziente Chips; Leistungshalbleiter; Sensoren; Fortschrittliche optische Ausrüstung; Verbundwerkstoffe	EU: 43 DEU: 18
Mikroelektronik II 	**2021: Prä-Notifizierung** **2022/23: Ausstehende Genehmigung durch die EU** **2023+: (geplanter) Projektstart**	**20 EU-Mitgliedstaaten:** Belgien, Deutschland, Finnland, Frankreich, Griechenland, Irland, Italien, Lettland, Litauen, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn	Insgesamt: 10 Mrd. € Öffentlich: 450 Mio. € (für 2023) Privat: k.A.	Fotonik, Sensoren der nächsten Generation, Prozessoren, KI/ML/DL; Energiespeicher der nächsten Generation, Aktuator, Energieeffizienz; „Softwarisierte" Netzwerke, 5G/6G-Technologie, optische Konnektivität, drahtlose Kurzstreckenverbindungen	EU: k.A. DEU: 32
Cloud Infrastruktur und Services 	**2022**: Ausstehende Genehmigung durch die EU-Kommission **2022**: (geplanter) Projektstart **2026**: (geplantes) Projektende	**12 EU-Mitgliedstaaten:** Belgien, Deutschland, Frankreich, Italien, Lettland, Luxemburg, Niederlande, Polen, Slowenien und Spanien, Tschechische Republik, Ungarn	Insgesamt: k.A. Öffentlich: 750 Mio. € Privat: k.A.	Aufbau einer Cloud-Edge-Infrastruktur, insbesondere für industrielle Anwendungen durch: digitale Infrastruktur; Zusammenschaltungen; Foundation Services; Plattformen und intelligente Verarbeitungsdienste	EU: ≈80 DEU: 22

Quelle: Zusammenstellung der Autoren anhand öffentlich verfügbarer Informationen

Ausgaben anderer EU-Mitgliedstaaten in vielen Bereichen übertreffen, hat aber mit einer uneinheitlichen Umsetzung zu kämpfen. Während das Land sein Ziel, 100 auf KI spezialisierte Professuren zu besetzen, bereits erreicht hat,[103] hat es bis Mitte 2021 nur 250 Millionen Euro seines 5 Milliarden Euro umfassenden Investitionspakets für KI ausgeschüttet.[104] Neben bürokratischen Hürden spiegelt dies auch die Abwesenheit eines kohärenten Prozesses zur nachhaltigen Umsetzung strategischer Prioritäten wider.

Darüber hinaus erschwert die föderale Struktur Deutschlands das Ausschöpfen von Synergien zwischen der Bundes- und Länderpolitik. Der deutsche Föderalismus kann einen gesunden Wettbewerb zwischen den Ländern schaffen, der ihre unterschiedlichen Stärken hervorhebt und das Experimentieren mit innovativen Maßnahmen fördert, um internationale Investitionen und Talente für Spitzentechnologie anzuziehen. Um jedoch den gewünschten „Hebeleffekt" zwischen den Initiativen von Bund und Ländern zu erzielen, muss dieser Wettbewerb in einen koordinierten Ansatz eingebettet sein, der mögliche Synergien herausarbeitet.[105] Eine signifikante Chance besteht in der engeren Verflechtung der Prioritäten des Bundes und

103 Werner Pluta, Forschungsministerium besetzt 100 zusätzliche KI-Professuren, in: Golem.de, 6. Mai 2022: https://www.golem.de/news/kuenstliche-intelligenz-forschungsministerium-besetzt-100-zusaetzliche-ki-professuren-2205-165144.html (abgerufen am 19. Mai 2022).

104 Stand 31. Mai 2021. Bundestag, Schriftliche Fragen mit den in der Woche vom 7. Juni 2021 eingegangenen Antworten der Bundesregierung, Drucksache 19/30613, 11. Juni 2021, S. 159: https://dserver.bundestag.de/btd/19/306/1930613.pdf (abgerufen am 19. Mai 2022).

105 Eine „Hebelwirkung" wird beispielsweise in der KI-Strategie der Regierung benannt. Allerdings werden nur in der aktualisierten Strategie aus dem Jahr 2020 Bereiche genannt, in denen – abgesehen vom Bildungswesen, das in erster Linie in die Zuständigkeit der Länder fällt – eine Zusammenarbeit mit den Ländern konkret denkbar wäre.

der Investitionspolitik der Länder, die eine Reihe von regionalen Initiativen ins Leben gerufen haben. Dazu gehören Bayerns 300-Millionen-Euro-Finanzierung für das Munich Quantum Valley[106] zur Förderung von Quantenwissenschaften und -technologien sowie ein erstes 160-Millionen-Euro-Paket für das baden-württembergische Cyber Valley, das derzeit größte KI-Forschungskonsortium Europas.[107]

Die Koordinierung auf supranationaler Ebene bleibt ebenfalls eine wichtige Herausforderung bei der Gewährleistung einer effektiven Politikumsetzung. Die EU-Institutionen sind zwar führend in Bezug auf die Regulierung digitaler Technologien, doch die Industriepolitik wird vor allem von den Mitgliedstaaten gestaltet. Deutschland kommt bei der Überbrückung dieser Aufgabenteilung und der Förderung einer kohärenteren Gesamtpolitik eine Schlüsselrolle zu. Dazu gehört insbesondere sein Engagement für mehrere wichtige Vorhaben von gemeinsamem europäischem Interesse (Important Project of Common European Interest, IPCEI),[108] einschließlich der für Mikroelektronik, Cloud-Infrastruktur und Batterien. Das IPCEI zum Aufbau der nächsten Generation von Cloud-Infrastrukturen und -Services (IPCEI-CIS),[109] das unter anderem mit 750 Millionen Euro aus deutschen Mitteln finanziert wird, ist jedoch indirekt in Spannungen innerhalb der deutsch-französischen GAIA-X-Initiative verwickelt,[110] die es amerikanischen und chinesischen Hyperscalern ermöglicht, sich an der Standardsetzung für eine föderierte europäische Dateninfrastruktur zu beteiligen. Darüber wird das IPCEI Mikroelektronik[111] durch langsame bürokratische Prozesse in Deutschland und der Europäischen Kommission ausgebremst, und es bleibt unklar, wie diese Projekte und das 17-Milliarden-Euro-Projekt für den Bau der Intel-Chipfabrik in Magdeburg, für deren Finanzierung die Bundesregierung etwa 6,8 Milliarden Euro zur Verfügung stellen wird, strategisch ineinandergreifen.[112]

Hinzu kommt, dass in Deutschland andere finanz- und geopolitische Herausforderungen um öffentliche Mittel konkurrieren. Die derzeitige Bundesregierung steht unter starkem Druck, ab 2023 eine Haushaltskonsolidierung voranzutreiben – trotz der mit der sogenannten Zeitenwende-Politik einhergehenden Kosten wie der Schaffung eines Sondervermögens in Höhe von 100 Milliarden Euro für die Modernisierung der deutschen Streitkräfte.[113] Der russische Angriff auf die Ukraine hat auch zu einem Anstieg der Energie- und Lebensmittelpreise geführt, was die deutschen Klimaziele gleichzeitig weiter antreibt und konterkariert. Es entsteht zunehmend der Eindruck, dass die Technologie- und Industriepolitik an Priorität verlieren könnte.

106 Bayerisches Staatsministerium für Wissenschaft und Kunst, Munich Quantum Valley: Münchener Initiative will Quantencomputer in Bayern entwickeln, 11. Januar 2021: https://www.stmwk.bayern.de/pressemitteilung/12124/munich-quantum-valley-muenchener-initiative-will-quantencomputer-in-bayern-entwickeln.html (abgerufen am 19. Mai 2022).

107 Ministerium für Wissenschaft, Forschung und Kunst, Baden-Württemberg, Fünf Jahre Cyber Valley, 15. Dezember 2021: https://mwk.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/fuenf-jahre-cyber-valley/ (abgerufen am 19. Mai 2022).

108 Ein IPCEI kann von den Mitgliedstaaten subventioniert werden, wenn es sich um ein integratives europäisches Projekt handelt, das ein Marktversagen in einem Schlüsselsektor oder einer Schlüsseltechnologie adressiert, und wenn es positive Spillover-Effekte für die EU-Wirtschaft als Ganzes bewirkt.

109 Bundesministerium für Wirtschaft und Energie (BMWi), Förderbekanntmachung zur geplanten Förderung im Bereich Cloud und Edge Infrastruktur und Services im Rahmen des IPCEI-CIS, April 2022: https://www.bmwk.de/Redaktion/DE/Downloads/F/forderbekanntmachung-zur-geplanten-forderung-im-bereich-cloud-und-edge-infrastruktur-und-services-im-rahmen-des-ipcei-cis.pdf?__blob=publicationFile&v=6 (abgerufen am 19. Mai 2022).

110 Gaia-X European Association for Data and Cloud AISBL, About Gaia-X: https://www.gaia-x.eu/what-is-gaia-x (abgerufen am 19. Mai 2022).

111 Als Mitinitiator des IPCEI Mikroelektronik mobilisiert die Bundesregierung bis 2023 fast eine Milliarde Euro, um den Bau moderner Chipfabriken und die Produktion energieeffizienter mikroelektronischer Komponenten zu unterstützen. Deutschland beteiligt sich auch am neuen IPCEI Mikroelektronik II, das auf hochleistungsfähige und spezialisierte Chips abzielt, z. B. für KI-Anwendungen und autonomes Fahren. Bundesministerium für Wirtschaft und Energie (BMWi), IPCEI Mikroelektronik: Zwei europäische Großprojekte für eine Schlüsseltechnologie der Zukunft, September 2021: https://www.bmwi.de/Redaktion/DE/Downloads/I/infopapier-ipcei-mikroelektronik.pdf?__blob=publicationFile&v=6 (abgerufen am 19. Mai 2022).

112 Joachim Hofer, Die Chip-Industrie entdeckt Deutschland – das neue Intel-Werk ist nur der Anfang, in: Handelsblatt, 7. Oktober 2022: https://www.handelsblatt.com/technik/it-internet/halbleiter-die-chip-industrie-entdeckt-deutschland-das-neue-intel-werk-ist-nur-der-anfang/28711740.html (abgerufen am 31. Oktober 2022).

113 Christian Mölling, Torben Schütz, Zeitenwende in der Verteidigungspolitik. Bundeswehr-Sondervermögen effektiv und nachhaltig ausgeben, in DGAP Policy Brief Nr. 16, Deutsche Gesellschaft für Auswärtige Politik, Mai 2022: https://dgap.org/sites/default/files/article_pdfs/dgap-policy%20brief-2022-16-dt_1.pdf (abgerufen am 19. Mai 2022).

Handlungs-empfehlungen

Die Bundesregierung muss Deutschlands industriepolitischen Instrumente wirksam einsetzen, um seinen Zugang zu kritischen Technologien zu sichern und seine wirtschaftliche Wettbewerbsfähigkeit aufrechtzuerhalten. Zu diesem Zweck sollte es:

Nationale Stärken und Schwächen im Bereich kritischer Technologien behördenübergreifend erfassen. Die Bundesregierung sollte in Anlehnung an die Bemühungen ihrer Partner eine behördenübergreifende Initiative starten, um drei industriepolitische Ziele auszuarbeiten: technologische Führung, Ebenbürtigkeit mit Mitbewerbern und Risikoreduzierung bei Abhängigkeiten.[114] Diese Ziele sollten mit strategischen Prioritäten im Wirtschafts- und Sicherheitsbereich verzahnt und mit den eigenen Fähigkeiten und denen von Partnern abgeglichen werden.

Die Kohärenz der strategischen Industriepolitik zwischen Bund und Ländern sowie zwischen den Ländern selbst verbessern. Die Bundesregierung sollte sich darauf konzentrieren, dass die Industriepolitik der Länder mit den nationalen Technologiezielen im Einklang steht. Das Bundesministerium für Bildung und Forschung (BMBF) sollte ein Dashboard für industrielle Initiativen auf Landesebene einrichten, das ungenutztes Potenzial bei asymmetrischer FuE und industriellen Partnerschaften identifiziert. Hochrangige Beamtinnen und -beamte, Forschungskonsortien und die Industrie könnten dieses Instrument nutzen, um Synergien zwischen Initiativen in einzelnen Forschungsbereichen und branchenübergreifend zu ermitteln und zu nutzen, etwa zwischen hardware- (z. B. Quantencomputing) und softwarebezogenen (z. B. Verarbeitung natürlicher Sprache) FuE-Initiativen.

Transnationale Industriekonsortien ausbauen – in Europa und mit gleichgesinnten Partnern. Die EU steht im Technologiesektor vor der Wahl: den Weg gemeinsam oder alleine gehen. Als größte Volkswirtschaft der EU verfügt Deutschland über einen erheblichen Handlungsspielraum, um eine strategische und kohärente europäische Technologie- und Industriepolitik voranzutreiben. Das Land sollte grenzüberschreitende Konsortien für Innovationen fördern, indem es sich für ein verschlanktes Verfahren zur Notifizierung bei IPCEIs einsetzt, eine angemessene Personalbesetzung für die Bearbeitung sicherstellt, und Finanzmittel bereitstellt, die seinen High-Tech-Ambitionen entsprechen. Sofern Partnerstaaten wichtige Komponenten der Wertschöpfungskette bereitstellen, sollte Deutschland die Europäische Kommission ermutigen, ein IPCEI-Schema zu schaffen, das ausländische Lieferanten einbezieht, um positive Spillover-Effekte zu verstärken.

Den Schwerpunkt auf nationale – und europäische – Wettbewerbsvorteile sowie strategische Interdependenzen innerhalb einer größeren Gemeinschaft gleichgesinnter Partner legen. Globale Lieferketten sind oft zu komplex, um komplette Technologie-Stacks nach Europa zu verlagern. Deshalb sollte Deutschland seine Industriepolitik so gestalten, dass sie eine größere Gemeinschaft gleichgesinnter Partner unterstützt, in deren Mittelpunkt die EU steht, die aber auch wichtige Partner wie die USA, Japan und Südkorea einschließt. Diese Gemeinschaft sollte drei Ziele verfolgen: IT-Sicherheit, die Widerstandsfähigkeit von Lieferketten und industrielle Wettbewerbsfähigkeit. In diesem Kontext sollte Industriepolitik zur Steigerung der Wettbewerbsfähigkeit direkt an komparative Vorteile Deutschlands anknüpfen, wie etwa beim Edge Computing und bei der Nutzung industriellen Knowhows (z. B. in den Sektoren Automobil, Medizinprodukte und Energienetze) für die Herstellung spezieller Chips.

Das öffentliche Beschaffungswesen darauf ausrichten, Schwachstellen in der IT-Sicherheit und Lieferketten zu verringern. Die Bundesregierung ist der größte Abnehmer von IT-Systemen in Deutschland und kann ihre Kaufkraft nutzen, um strategische Verwundbarkeiten zu reduzieren, insbesondere in den sicherheitskritischen Bereichen ihres Technologie-Stacks. Beschaffungsanforderungen sollten die Skalierung einer sicheren europäischen Cloud-Infrastruktur für öffentliche Dienste unterstützen. Reformen sollten die Benachteiligung von Open Source-Lösungen bei der Beschaffung beseitigen, indem sie Sicherheit, Offenheit und Interoperabilität zu Schlüsselkriterien machen. Die Reformen sollten auch den Eintritt von (kleineren) europäischen Mitbewerbern durch ein vereinfachtes Ausschreibungsverfahren und transparentere Genehmigungsfristen erleichtern.

114 Im Zusammenhang mit den USA: The White House, National Strategy for Critical and Emerging Technologies, Oktober 2020: https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf (abgerufen am 19. Mai 2022).

KAPITEL 4

Deutschlands Rolle in Europas digitaler Ordnungsmacht

Gestaltung eines globalen Technologie-Regelwerks im Sinne Europas

KAPITELÜBERSICHT

Zentrale Erkenntnisse

1 Die Stärken und zuweilen auch die Grenzen des deutschen Einflusses auf die Regulierung digitaler Technologien lassen sich anhand von vier Elementen aufzeigen:

- Deutschland antizipiert die Regulierung digitaler Technologien durch die EU und versucht, vollendete Tatsachen zu schaffen.
- Deutschland nimmt überdurchschnittlich großen Einfluss auf die formalen Entscheidungsphasen der EU-Regulierungspolitik im Digitalbereich.
- Deutschland nutzt gleichzeitig die EU als Sprungbrett, um auf weltweite regulatorische Normen Einfluss zu nehmen.
- Deutschland entdeckt die Bedeutung der deutschen Privatwirtschaft und der mit ihr assoziierten technischen Normungsgremien zur Prägung globaler technischer Vorschriften allmählich wieder.

2 Als EU-Mitgliedstaat engagiert sich Deutschland in drei wichtigen Bereichen der Datenverwaltung und Cybersicherheit: digitale Identitäten und offene Daten, rechtmäßiger Zugang zu elektronischen Messaging-Diensten und Regeln für die Nutzung souveräner Cloud-Dienste.

3 Die weitgehend erfolgreiche Rolle Deutschlands als wichtiger Impulsgeber für den regulatorischen Ansatz der EU im Bereich der digitalen Technologien, und damit als Triebfeder des „Brüssel-Effekts" bei der Gestaltung der globalen Märkte, wird hierzulande wenig anerkannt oder verstanden. Die Diskrepanz zwischen Regulierung, Technologie und internationalem Kontext zeigt sich in Bereichen wie Datenschutz, Inhaltsmoderation und Marktmacht von Online-Plattformen. Selbst substanzielle Debatten zur Regulierung von Quantencomputing, Metaverse (AR/VR) und 6G lassen in Deutschland noch auf sich warten.

4 Deutschland muss seinen Ansatz im Bereich der Digital-Regulierung ändern, um dem dynamischen und universellen Charakter aufkommender digitaler Technologien besser zu entsprechen – insbesondere in einem zunehmend angespannten internationalen Umfeld, in dem technische Regeln eine Komponente geopolitischer Macht darstellen. Dazu gehört: *erstens*, dass die politischen Zielkonflikte, die mit den Entscheidungen zur Regulierung digitaler Technologien verbunden sind, direkt adressiert werden; *zweitens*, dass die Überprüfungen und Auslaufklauseln in diesem Bereich ausgeweitet werden, um Flexibilität zu fördern; und *drittens*, dass Möglichkeiten zur Durchsetzung von Regeln unter Einbeziehung der Zivilgesellschaft, von Unternehmen und anderen nichtstaatlichen Akteuren stärker genutzt werden. Deutschland muss auch das Engagement seiner außen- und sicherheitspolitischen Gemeinschaft in der EU-Technologiediplomatie und bei der globalen Durchsetzung von Regeln verstärken.

Einleitung

Deutschland ist eine wichtige – vielleicht sogar die wichtigste – Kraft bei der Gestaltung des EU-Regulierungsansatzes für digitale Technologien, welcher eine wichtige Grundlage für Europas Macht im geopolitischen Technologie-Wettbewerb bildet. Deutschland steht im Mittelpunkt der ehrgeizigen Bemühungen der EU, Digital-Regulierung mit Menschenrechten, Rechtsstaatlichkeit und Demokratie zu verbinden. Diese Regulierung von Plattformen, Algorithmen und Daten ist im EU-Gesetz über digitale Dienste (Digital Services Act, DSA), im Gesetz über digitale Märkte (Digital Market Act, DMA), im Daten-Governance-Gesetz (Digital Governance Act, DGA), im Gesetz über künstliche Intelligenz (Artificial Intelligence Act, AI Act), im Datengesetz (Data Act) und im EU Cloud Rulebook festgelegt.[115] Deutschlands zentrale Rolle bei der Gestaltung dieser Regeln bedeutet, dass es der EU nur dann gelingen wird, ihr Regelwerk zu aktualisieren, wenn auch Deutschland seine Denkansätze an die neuen Gegebenheiten

115 Tyson Barker, „2021 Is the Year the Internet Gets Rewritten", Foreign Policy, 19. Januar 2021: https://foreignpolicy.com/2021/01/19/2021-is-the-year-the-internet-gets-rewritten/ (abgerufen am 1. Juni 2022).

anpasst. Das bedeutet unter anderem, dass die Bundesregierung anerkennen muss, dass Regulierung zu einer geopolitisch bedeutsamen Komponente geworden ist, andere Staaten ein teils abweichendes Gleichgewicht zwischen Regulierung und Innovation wählen und somit manchmal Vorteile aus den Kosten ziehen, die der EU als regulatorische Vorreiterin entstehen. Während Europa die nächste Welle der Daten-Governance in der Cloud, im Edge Computing und im Internet der Dinge (IoT) in Angriff nimmt, haben Deutschland und damit auch die EU die Chance, einen Rechtsrahmen zu schaffen, der europäische Werte und die globale Wettbewerbsfähigkeit fördert.

Status quo

Deutschland ist auf nationaler und vor allem auf EU-Ebene ein selbstbewusster, beharrlicher und kompetenter Akteur bei der Ausgestaltung digitaler Ordnungspolitik. Deutschland kennt die Hebel der Regulierungsmacht im Bereich der digitalen Technologien in Brüssel und hat über verschiedene Kanäle – Bund und Länder, Privatsektor und die deutsche Zivilgesellschaft – die Möglichkeit, das europäische Regelwerk so zu gestalten, dass es mit einem ordoliberalen, regelzentrierten Ansatz für digitale Souveränität vereinbar ist. Hinsichtlich der Strahlkraft dieses Ansatzes für die Regulierung digitaler Technologien weltweit, bleibt das deutsche Bewusstsein jedoch nach wie vor wenig ausgeprägt. Die Stärken und zuweilen auch die Grenzen der deutschen Einflussnahme auf die Regulierung digitaler Technologien lassen sich anhand von vier Elementen aufzeigen.

Erstens versucht Deutschland immer wieder, die Entwicklung der EU-Regulierung in Hinblick auf die digitale Sphäre zu antizipieren und diesbezügliche Debatten in Brüssel auf seine eigenen Bedürfnisse hin auszurichten, und das vermutlich mehr als jeder andere Mitgliedstaat. Die EU ihrerseits neigt wiederum dazu, die deutsche Debatte zu verfolgen, um den Weg für eine reibungslose rechtliche Verankerung ihrer eigenen Prioritäten zu ebnen. Folglich sind deutsche Rechtstraditionen (z. B. beim Festlegen des Datenschutzes als Grundlage für die Datenschutz-Grundverordnung (DSGVO))[116] und ordoliberales Denken (z. B. die Skepsis gegenüber Kartellen und digitaler Marktkonzentration) auf EU-Ebene sehr einflussreich. Gleichzeitig befindet sich Deutschland in einer Art Echokammer und ist der Ansicht, dass seine eigenen Prioritäten auch auf europäischer Ebene Vorrang haben – und nicht etwa die grenzüberschreitende Liberalisierung digitaler Dienste mit gleichgesinnten Nicht-EU-Staaten oder ein stärkerer regulatorischer Fokus auf die Cyberrisiken der von staatlich kontrollierten, chinesischen Unternehmen entwickelten IKT-Infrastruktur.

Natürlich spiegelt das EU-Regelwerk nicht immer die deutschen Prioritäten wider, und andere Akteure – etwa die Europäische Kommission, das Europäische Parlament, der Privatsektor, einschließlich US-Technologieunternehmen, und andere Mitgliedstaaten wie Frankreich und die technikbegeisterten nordischen und baltischen Staaten sowie Irland – beeinflussen in der Regel den Übergang von der EU-Debatte zur Gesetzgebung. Ein Beispiel dafür sind die Widersprüche zwischen dem DMA und der zehnten Novelle des deutschen Gesetzes gegen Wettbewerbsbeschränkungen. Gleiches trifft auch auf die Widersprüche zwischen der DSA-Regelung bezüglich illegaler Inhalte und dem deutsche Netzwerkdurchsetzungsgesetz (NetzDG) zu. Dennoch ist die deutsche Vorwegnahme der rechtlichen Debatten in der EU in fast jeder Hinsicht von Berlins digitaler Technologiepolitik geprägt – von der Prüfung ausländischer Direktinvestitionen (FDI/ADI) bis hin zur Sorgfaltspflicht im Bereich der Technologielieferketten.[117] So hat die deutsche Datenethikkommission (DEK) 2017 einen Rahmen für KI-Risikokategorien und -bewertung entworfen, der sich im KI-Whitepaper der EU 2020 und im Entwurf des EU AI Act wiederfindet.[118] Das deutsche IT-Sicherheitsgesetz 2.0 und Gaia-X haben jeweils die EU-Diskussion über die Richtlinie zur Netz- und Informationssicherheit 2 (NIS 2) und das europäische Cybersicherheit-Zertifizierungssystem für Cloud-Dienste (EUCS) angestoßen.

Zweitens ist Deutschland auch als größter Mitgliedstaat der EU in der digitalen Ordnungspolitik überrepräsentiert. Deutsche besetzen Schlüsselpositionen als Beamtinnen und Beamten in der Europäischen

116 Informationelle Selbstbestimmung.

117 Bundesministerium für Arbeit und Soziales, „CSR-Supply Chain Act", (22. Juli 2021): https://www.csr-in-deutschland.de/EN/Business-Human-Rights/Supply-Chain-Act/supply-chain-act.html (abgerufen am 1. Juni 2022).

118 Tyson Barker, „The Digital Technology Environment and Europe's Capacity to Act", DGAP Report No. 7, Deutsche Gesellschaft für Auswärtige Politik (November 2021), S. 23: https://dgap.org/sites/default/files/article_pdfs/Mercator%20Study%20Tech_Highres.pdf (abgerufen am 1. Juni 2022).

Kommission, als gut positionierte Administratorinnen und Administratoren des Europäischen Rates und als Mitglieder des Europäischen Parlaments (MdEP), die als Berichterstatterinnen und Berichterstatter für wichtige Gesetzespakete[119] und als einflussreiche Ausschussvorsitzende[120] dienen sowie als wichtige Mitarbeiterinnen und Mitarbeiter des Parlamentssekretariats. Obwohl viele dieser Offiziellen ein breites ideologisches Spektrum repräsentieren, bewahren sie sich eine deutsche politische Sensibilität. Nur Frankreich kann mit Deutschland mithalten, was den Einsatz von Personal zur Gestaltung der digitalen Ordnungspolitik der EU angeht, insbesondere in der Kommission (z. B. DG CONNECT) und in wichtigen Aufsichtsbehörden wie dem Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK).

Zuweilen spiegeln diese Beamtinnen und Beamten sowie Vertreterinnen und Vertreter die Interessen deutscher Institutionen wider, einschließlich wichtiger deutscher Unternehmen.[121] Dies ist an sich kein Problem, sondern eher ein natürlicher Nebeneffekt, der auf das komplexe Zusammenwirken der deutschen Europapolitik in Brüssel und des politischen Diskurses der deutschen Wirtschaft zurückzuführen ist. Unternehmen können Deutschlands Stellung im Digitalbereich stärken. Ohne ausreichendes Gegengewicht besteht jedoch das Risiko, dass sie den deutschen Einfluss auf eng gesteckte Unternehmensziele umlenken. Und, was noch problematischer ist: Dies könnte zu gemeinsamen unternehmensstrategischen Schwachstellen führen. Dazu gehört auch eine erhöhte Anfälligkeit gegenüber möglichen Vergeltungsmaßnahmen Chinas für behördliche Prüfungen der Datenverarbeitungs- und Cybersicherheitspraktiken chinesischer Unternehmen, die in der EU tätig sind. Unternehmen in Australien, Kanada und dem Vereinigten Königreich, Deutschlands Verbündete außerhalb der EU, sind darüber weniger besorgt, da sie nicht so stark vom chinesischen Markt abhängig sind. Aufgrund der Marktabhängigkeit von China ist Deutschland gezwungen, ein Gleichgewicht zwischen seinem Bedarf an chinesischen Verbraucherinnen und Verbrauchern und seinem Engagement für seine eigenen Werte im Bereich der digitalen Technologien zu finden.

Internationale und geopolitische Belange prägen zwar die deutsche und europäische digitale Ordnungspolitik, doch sind diese auch noch immer von früheren Erfahrungen mit den USA und Misstrauen in Bezug auf Datenschutz und Spionage geprägt. Seit den Enthüllungen rund um die National Security Agency (NSA) durch den Whistleblower Edward Snowden 2013 richten sich die deutschen Bedenken hinsichtlich des Datenschutzes vor allem auf die USA. Jüngste EU-Initiativen – insbesondere der DSA, DMA und Vorschläge bezüglich Cloud – betreffen aufgrund ihrer Marktdominanz hauptsächlich amerikanische Technologieunternehmen. Aber der Grad, zu dem dies als Mittel zur Einschränkung des technologischen Einflusses der USA wahrgenommen wird, kann Fragen aufwerfen. Die unverhältnismäßige Konzentration auf die USA entspricht nicht den heutigen geopolitischen Bedrohungen (Box 1). Der ko-regulatorische Ansatz und die weitreichenden Durchsetzungsbefugnisse der Kommission gemäß DSA und DMA schaffen in beiden Fällen die nötige Flexibilität, um den neuen Risiken in den sich ständig verändernden Online-Informationsökosystemen und der Dynamik der Marktmacht der Plattformen Rechnung zu tragen. Sobald DSA und DMA in Kraft treten, wird sich konkret zeigen, inwieweit diese für die Plattformlandschaft des Jahres 2023, und nicht des Jahres 2015, geeignet sind.

Drittens ist die EU für Deutschland und andere Mitgliedstaaten ein Sprungbrett, um weltweit auf Regulierung Einfluss zu nehmen. Bei globalen Technologieunternehmen wurde die Datenschutz-Grundverordnung der EU bekanntlich zur Referenz für Datenschutz, und das auch in Ländern außerhalb der EU. Vier Jahre nach Inkrafttreten der DSGVO nutzen Länder wie Argentinien, Südkorea, Japan und Kenia sowie subnationale Regierungen wie die von Kalifornien mit ihrem California Privacy Rights Act (CPRA) die DSGVO als Grundlage für ihre eigenen Datenschutzbestimmungen. Selbst der wachsende Druck auf Washington, ein föderales US-Datenschutzgesetz zu erlassen, geht zum Teil von Europa aus. Und das Schrems-II-Urteil aus dem Jahr 2020, mit dem der Europäische Gerichtshof das Privacy Shield-Abkommen aus dem Jahr 2016 für die transatlantische Übermittlung personenbezogener Daten für unwirksam erklärte, zwang die USA dazu, erhebliche Änderungen vorzunehmen, um Beschwerden aus Europa nachzukommen und Kontrollen der Datenerfassung durch Geheimdienste zu verschärfen. Die EU hat als Vorreiterin in Sachen Regulierung die

119 Zum Beispiel von DSGVO, DMA und der NIS-Richtlinie.
120 Zum Beispiel von dem Ausschuss für Binnenmarkt und Verbraucherschutz und dem Ausschuss für internationalen Handel.
121 Wie zum Beispiel Deutsche Telekom, SAP, Infineon, Bosch, Axel Springer und Bertelsmann.

DEUTSCHLANDS STARKER USA-FOKUS

Die transatlantischen Technologiebeziehungen sind nach wie vor die Hauptschlagader der digitalen Welt. Die Unterseekabel, die den Nordatlantik durchqueren, übertragen 55 Prozent mehr Daten als die transpazifischen Unterseekabel. Allerdings verschieben sich die globalen digitalen Aktivitäten, wie auch wirtschaftlichen Aktivitäten, von den USA in den indopazifischen Raum und in den globalen Süden, auch wenn Deutschland bei der Durchsetzung von Vorschriften weiterhin stark auf den Atlantik ausgerichtet ist.

Die Datenstrategie Deutschlands vom Januar 2021 konzentrierte sich stark auf Gaia-X als Mittel zur Emanzipation Europas von US-Cloud-Diensten (und den Bestimmungen des Gesetzes Clarifying Lawful Overseas Use of Data (CLOUD), das US-Behörden den Zugriff auf bestimmte Daten in anderen Ländern ermöglicht), zum Teil durch den Einsatz von Open-Source-Software wie OpenStack. Der aktuelle deutsche Diskurs über Datenlokalisierung, Plattformabhängigkeit und Verschlüsselung wird nach wie vor von den Enthüllungen rund um die NSA, die Wahl des ehemaligen US-Präsidenten Donald Trump im Jahr 2016 und dem Cambridge-Analytica-Skandal im Jahr 2017 überschattet.

Die Bemühungen der EU um die Durchsetzung von Rechtsvorschriften konzentrieren sich ebenfalls hauptsächlich auf den euro-atlantischen Raum. Die Durchsetzung der DSGVO durch die 17 deutschen Datenschutzbehörden (DSB) richtet sich nach wie vor primär gegen US-Dienstleister und -Plattformen. Dies war angesichts der dominierenden Rolle der US-amerikanischen digitalen Dienste auf dem europäischen Markt in den letzten zehn Jahren gerechtfertigt. Der Fokus auf die Überprüfung von US-Technologieunternehmen steht jedoch im Gegensatz zu der mangelnden Prüfung von systematischen Verstößen durch Unternehmen aus Staaten mit Angemessenheitsbeschluss wie dem Vereinigten Königreich, Kanada und Japan und sogar durch europäische Unternehmen selbst. Am interessantesten ist vielleicht die verhältnismäßig unzureichende Prüfung systematischer Verstöße, insbesondere in Bezug auf Anforderungen für rechtmäßigen Zugriff, durch autoritäre Staaten wie China und Russland.

Es gibt jedoch einige Anzeichen dafür, dass der Fokus langsam von den USA abrückt. Der Entwurf der EU für eine KI-Verordnung, der von der deutschen EU-Ratspräsidentschaft 2020 und der Datenethikkommission der Bundesregierung mit erarbeitet wurde, schenkt den chinesischen Praktiken größere Aufmerksamkeit als frühere ähnliche EU-Verordnungen. Die strengsten Bestimmungen des Kommissions-Entwurfs betreffen das Sozialkreditsystem, welches die Verordnung verbietet, und die biometrische Fernidentifizierung in Echtzeit, die nur Strafverfolgungsbehörden in streng definierten Situationen nutzen dürfen. Diese Maßnahmen beziehen sich implizit auf das Vorgehen Chinas. Die Förderung konformen Verhaltens ist seit langem kennzeichnendes Element der chinesischen Gesellschaft, aber die KI-gestützte biometrische Identifizierung in Kombination mit umfassender Videoüberwachung und einem Sozialkreditsystem bildet ein mächtiges und gefährliches Instrument zur sozialen Kontrolle.

globale Regulierungslandschaft in Richtung ihres Modells geprägt. Das ist für Deutschlands Anliegen zwar vorteilhaft, birgt aber auch Nachteile. Viele Nicht-EU-Staaten und die meisten EU-Mitgliedstaaten tun sich schwer damit, die Bestimmungen der Datenschutz-Grundverordnung einzuhalten, was freie Datenflüsse erschwert. Darüber hinaus stehen der EU andere, potenziell vielversprechendere Wege offen, um ein international anwendbares Regelwerk zu erarbeiten.

Die EU und gleichgesinnte Staaten wie Australien, Kanada und das Vereinigte Königreich haben einen (zwischenstaatlichen) Regulierungsdiskurs in Bereichen begonnen, die über den Datenschutz hinausgehen. Zu diesen Bereichen gehören Inhaltsmoderation, Plattform-Governance, die Marktmacht einzelner Unternehmen, Datenschutz und risikobasierte KI-Ansätze. Dies ist jedoch ein mühsames Unterfangen, da Unterschiede in den internen Gesetzgebungsverfahren, den Regulierungs-

kompetenzen, den föderalen Strukturen und den verfassungsrechtlichen Grenzen zu unterschiedlichen Ergebnissen führen.

Gleichzeitig hat China gelernt, die Regulierungsprinzipien der EU zu kopieren, um weit weniger hochgesinnte Ziele zu verfolgen. Chinas Diskurs über die Marktmacht der Technologieriesen und Datenschutz spiegelt die Debatte in Deutschland und Europa, doch mit dem Ziel, internationale Kritik zu beschwichtigen und gleichzeitig die absolutistische Macht der Kommunistischen Partei zu festigen. Das chinesische Anti-Sanktionsgesetz von 2021, das exterritoriale Sanktionen innerhalb des Landes außer Kraft setzt, wurde dem EU-Recht nachempfunden.[122] Chinesische Vorschriften zum Schutz personenbezogener Daten (einschließlich der Globalen Initiative für Datensicherheit 2020),[123] zum Wettbewerb, zu Algorithmen und zuletzt zur Content-Governance mit „positiver Energie"[124] lehnen sich an europäische Überlegungen an und übernehmen mitunter sogar den Wortlaut des Unionsrechts. Dennoch zielen diese Bemühungen darauf ab, den chinesischen Technologiesektor und andere Akteure in den Dienst parteistaatlicher Interessen zu stellen.

Viertens wäre Europas Gestaltungsmacht ohne Deutschlands Einfluss und den seines Privatsektors in globalen technischen Normungsgremien viel geringer. Das Deutsche Institut für Normung e.V. (DIN), die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik e.V. (DKE) und der Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE) bilden einen Kern nationaler Gremien, deren Arbeit in ihre europäischen und internationalen Pendants einfließt. Deutschland ist eines von sechs ständigen Mitgliedern des Rates der Internationalen Organisation für Normung (ISO) und stellt 18 Prozent der ISO-Sekretariate, 19 Prozent der Sekretariate der Internationalen Elektrotechnischen Kommission (IEC) und 29 Prozent der IEC-Arbeitsgruppenvorsitzenden.[125] Es stellt auch Kandidaten für Schlüsselpositionen auf, wie zum Beispiel für den Posten des Direktors des Sektors für Telekommunikationsnormung der Internationalen Fernmeldeunion (ITU) im Jahr 2022.[126]

Aber so wie sich Deutschland manchmal des großen Einflusses seines Privatsektors auf die europäische Regulierung nicht bewusst ist, so hat es den relativen Rückgang seines Einflusses – und folglich desjenigen der EU – bei der internationalen Standardsetzung nur langsam erkannt. Die Rolle des deutschen Privatsektors ist geschrumpft, seitdem insbesondere chinesische Staatsunternehmen und dem Staat nahestehende Unternehmen die Kontrolle über wichtige technische Arbeitsgruppen erlangt und Musternormen eingebracht haben.[127] Chinas Drängen auf regionale Standardsetzungsvereinbarungen im Rahmen seiner Seidenstraßeninitiative könnte auch zu Lock-in-Effekten für Drittländer führen, die zu einem merkantilistischen digitalen internationalen System neigen, das China und den digital gestützten Autoritarismus begünstigt. Dies ist Teil eines umfassenderen Plans, den Henry Kissinger als Chinas „geduldige Anhäufung relativer Vorteile" bezeichnet hat.[128] Deutschland hat, wie der Rest Europas, erst spät erkannt, dass die technische Normung mit geopolitischen Risiken behaftet ist, und dies zu einer Zeit, in der die Beteiligung des deutschen Privatsektors in internationalen Normungsgremien bereits zurückgegangen ist

122 Kelly Austin et al., „China's ‚Blocking Statute' – New Chinese Rules to Counter the Application of Extraterritorial Foreign Laws" Gibson Dunn, 13. Januar 2021: https://www.gibsondunn.com/chinas-blocking-statute-new-chinese-rules-to-counter-the-application-of-extraterritorial-foreign-laws/ (abgerufen am 1. Juni 2022).

123 Botschaft der Volksrepublik China in den Vereinigten Staaten von Amerika, „Global Initiative on Data Security", 8. September 2020: https://www.mfa.gov.cn/ce/ceus//eng/zgyw/t1812951.htm (abgerufen am 1. Juni 2022).

124 Maria Siow, „Positive energy: the darker side of China's social media catchphrase", South China Morning Post, 21. Juni 2020: https://www.scmp.com/week-asia/people/article/3089846/positive-energy-darker-side-chinas-social-media-catchphrase (abgerufen 1. Juni 2022).

125 Deutsches Institut für Normung, „DIN", 4. August 2022: https://www.iso.org/member/1511.html (abgerufen am 10. August 2022).

126 Internationale Fernmeldeunion, „Elections", (2022): https://www.itu.int/pp22/en/elections/candidates/ (abgerufen am 1. Juni 2022).

127 Tim Rühlig, „Technical standardisation, China and the future international order. A European perspective", E-Paper, Heinrich Böll Stiftung Brussels (Februar 2020): https://eu.boell.org/sites/default/files/2020-03/HBS-Techn%20Stand-A4%20web-030320.pdf (abgerufen am 1. Juni 2022).

128 Tom McTague, „Joe Biden Has a Europe Problem", The Atlantic, 21. Januar 2021: https://www.theatlantic.com/international/archive/2021/01/joe-biden-europe/617753/ (abgerufen am 1. Juni 2022).

Aktueller politischer Ansatz

Die derzeitige Debatte der Bundesregierung über die Regulierung digitaler Technologien konzentriert sich auf eine Reihe von Fragen der Daten-Governance und der Cybersicherheit im Zusammenhang mit der nahtlosen digitalen Interaktion mit der öffentlichen Verwaltung, dem rechtmäßigen Zugang zu elektronischen Messaging-Diensten und Regeln für die Nutzung souveräner Cloud-Dienste. Damit ändert sich der Schwerpunkt im Vergleich zu den jüngsten EU-Regulierungswellen insofern, als dass Datenschutz erheblich stärker als Aspekt von Cybersicherheit und weniger in Bezug auf staatliche und staatsnahe private Akteure eingeordnet wird. Dies könnte Gelegenheit für eine Neukalibrierung der Rolle Deutschlands auf europäischer Ebene bieten, um die demokratischen Grundsätze der Daten-Governance – und zwar auf flexible Weise und im Einklang mit dem deutschen Verständnis von digitaler Souveränität – zu definieren. Was genau unternimmt Deutschland also?

EIN DIGITAL BEFÄHIGTER STAAT

Erstens konzentrieren sich die deutschen Bemühungen auf der Nachfrageseite auf die Einführung sektorübergreifender und sicherer elektronischer digitaler Identitäten (eIDs), die auf den Erfahrungen der nordischen und baltischen EU-Mitgliedstaaten sowie der Ukraine basieren, die eIDs bereits eingeführt haben.[129] Das deutsche eID-Karte-Gesetz ist im September 2021 in Kraft getreten und hat die rechtliche Grundlage für digitale Identifikation über Smartphones mit sicherer und durch die Bundesdruckerei unterstützter Authentifizierungstechnologie geschaffen. Die Regierung hatte für Ende 2021 erste digitale ID-Dienste versprochen, die jedoch bisher nicht verfügbar sind. Auch bezüglich digitaler Führerscheine, ID-Wallets und Smart eIDs bestehen noch immer Probleme.[130] Auf der Angebotsseite verpflichtet das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (OZG) aus dem Jahr 2017 Bund, Länder und Kommunen dazu, ihre Verwaltungsdienste bis Ende 2022 digital anzubieten – eine Frist, die die Regierungen auf allen politischen Ebenen wahrscheinlich nicht werden einhalten können.[131] Ziel des OZG ist es, Behördenportale miteinander zu verbinden, damit Unternehmen sowie Bürgerinnen und Bürger mit einem einzigen Benutzerkonto auf Online-Dienste zugreifen können.[132] Dabei besteht die Gefahr, dass bürokratische Verzögerungen bei der Umsetzung, mangelnde Koordination zwischen den Behörden und letztlich eine uneinheitliche und ungleichmäßige Datenverfügbarkeit auch zu einer suboptimalen Nutzung durch Forscherinnen und Forscher sowie den privaten Sektor führen.

RECHTMÄSSIGER ZUGRIFF AUF ONLINE-KOMMUNIKATION

Eine weitere erwähnenswerte Maßnahme ist der Versuch der deutschen Bundesregierung, Bedingungen festzulegen, unter denen Strafverfolgungsbehörden Messaging-Dienste dazu verpflichten können, Zugriff auf verschlüsselte Kommunikation zu gewähren – ein anhaltender Konfliktpunkt zwischen der Strafverfolgung und Ende-zu-Ende-Verschlüsselung. Dies steht seit der Veröffentlichung des FBI-Dokuments „Lawful Access“ vom Januar 2021 auch in der EU auf der Agenda: Aus diesem geht hervor, welche Daten Strafverfolgungsbehörden von verschiedenen Messenger-

129 Das Bundesministerium für Wirtschaft und Klimaschutz schätzt, dass entwickelte Volkswirtschaften mit einer gut funktionierenden Infrastruktur für digitale Identitäten ihr Bruttoinlandsprodukt um 3 bis 4 Prozent steigern können. Bundesministerium für Wirtschaft und Klimaschutz, „Im Fokus: Sichere digitale Identitäten“, (Oktober 2021): https://www.bmwk.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2021/11/05-im-fokus-digitale-identitaeten.html (abgerufen am 1. Juni 2022).

130 Viola Heeger, „Digitale Identitäten: Deutschland im Verzug“, Tagesspiegel Background Digitalisierung & KI, 20. December 2021: https://background.tagesspiegel.de/digitalisierung/digitale-identitaeten-deutschland-im-verzug (abgerufen am 1. Juni 2022).

131 Bundesministerium des Innern und für Heimat, „Onlinezugangsgesetz (OZG)“, (2022): https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-node.html (abgerufen am 1. Juni 2022).

132 Auf europäischer Ebene enthält die eIDAS-Verordnung (Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, mit der die Richtlinie 1999/93/EG aufgehoben wurde) europaweit verbindliche Regelungen in den Bereichen „elektronische Identifizierung“ und „elektronische Vertrauensdienste“. Die Verordnung schafft einen einheitlichen Rahmen für die grenzüberschreitende Nutzung nationaler elektronischer Identifizierungsmaßnahmen und damit auch für die Nutzung des deutschen Online-Ausweises und der Vertrauensdienste.

Diensten erhalten können.[133] Anbieter wie Apple, Signal und Telegram wehren sich weiterhin dagegen.[134]

Letztes Jahr kündigte die Europäische Kommission selbst einen Gesetzesentwurf zur „Chat-Kontrolle" an, der schnell wieder von der Tagesordnung verschwand; möglicherweise aufgrund der massiven Proteste von mehr als 30 Organisationen aus der Zivilgesellschaft.[135] Doch im Mai 2022 legte die Kommission einen Vorschlag „zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern" vor.[136] Damit sollen insbesondere Anbieter interpersoneller Kommunikation in die Pflicht genommen werden, „Material über sexuellen Kindesmissbrauch aufzudecken, zu melden, zu sperren und aus ihren Diensten zu entfernen".[137] Dies könnte Nachrichten- und Hosting-Dienste wie WhatsApp und Signal dazu verpflichten, ihre Verschlüsselungsverfahren zu schwächen oder andere umstrittene Lösungen einzuführen, wie zum Beispiel Hash-Abgleiche oder das Scannen der Geräte von Endnutzerinnen und Endnutzern („Client-Side-Scanning" oder CSS).[138] Kritikerinnen und Kritiker behaupten, dass der Vorschlag die demokratischen Grundsätze untergrabe, indem er alle europäischen Bürgerinnen und Bürger unter Verdacht stelle und die Vertraulichkeit und Sicherheit des Internets unterminiere.

SOUVERÄNE CLOUD-DIENSTE UND INDUSTRIEDATEN

Die politischen Bemühungen in Deutschland und der EU kreisen um die Schaffung einer Cloud-Infrastruktur, die auf europäischen Regeln basiert und durch eine föderierte europäische Dateninfrastruktur ergänzt wird, die die Marktdominanz der Hyperscaler mit ihren enormen Datenverarbeitungskapazitäten durch Interoperabilitäts- und Portabilitätsanforderungen einschränken kann. Das Ziel ist letztlich, eine wettbewerbsfähige Cloud-Umgebung nach europäischen Regeln zu schaffen, die eine Grundlage für die Infrastruktur für das industrielle Internet und das Internet der Dinge bildet.

Ob dieser von Deutschland geleitete Cloud-Ansatz am Ende der eigenen ordoliberalen, regelzentrierten Vorstellung von digitaler Souveränität Nachdruck verleihen wird, bleibt unklar. Gaia-X, ein industriegetriebenes Spin-off einer deutsch-französischen Regierungsinitiative, ist eine Option für eine interoperable Cloud-Standardarchitektur für Europa und vielleicht auch darüber hinaus. Doch die Ausrichtung von Gaia-X auf eine regelbasierte digitale Souveränität sowie die Einbeziehung US-amerikanischer und chinesischer Akteure in die Governance, hat die Erwartungen einiger europäischer Akteure – auch in Frankreich – nicht erfüllt. Dies hat einige europäische Akteure dazu veranlasst, konkurrierende Initiativen wie die European Cloud Industrial Alliance (EUCLIDIA) und das EUCS zu gründen. Diese stützen sich auf das französische Cloud-Zertifizierungssystem SecNumCloud, das die öffentliche Verwaltung von außereuropäischen Cloud-Anbietern abschirmen soll. Trotz der Ankündigung verwandter Dienste wie einer föderierten Cloud-Infrastruktur-Architektur (Structura-X) und sektorspezifischer Kooperationen in den Bereichen Mobilität (Catena-X), Landwirtschaft (AgriGaia) und Finanzwesen (EuroDat) scheint Gaia-X mit den Mängeln früherer ähnlicher Bemühungen zu kämpfen: geringe Akzeptanz, unsichere private Nachfrage und schwindende politische Unterstützung in Deutschland.

Unterdessen nehmen die Diskussionen über die Datenlokalisierung in Deutschland zu. Internationale Datenströme sind nach wie vor umstritten und spiegeln Deutschlands Ambivalenz in Bezug auf den Wert und Nutzen von Datenzugang wider. Neben einigen Vertreterinnen und Vertretern der deutschen Regierung, Politikerinnen und Politikern, Rechtsexpertinnen und Rechtsexperten sowie NGOs in Deutschland gibt es auch in Frankreich Stimmen, die infrage stellen, ob

133 Martin Holland, „FBI über Messenger: An welche Daten von WhatsApp & Co. US-Strafverfolger kommen", Heise Online, 2. Dezember 2021: https://www.heise.de/news/FBI-ueber-Messenger-An-welche-Daten-von-WhatsApp-Co-US-Strafverfolger-kommen-6282456.html?wt_mc=rss.red.ho.ho.atom.beitrag.beitrag (abgerufen 1. Juni 2022).

134 Der iMessage-Dienst von Apple bietet eine Ende-zu-Ende-Verschlüsselung und gibt Nutzerdaten nur auf Vorladung heraus, und Chat-Informationen sind nur verfügbar, wenn sie in iCloud gesichert wurden. Telegram kann mögliche IP-Adressen und Telefonnummern bereitstellen. Signal veröffentlicht nur Datum und Uhrzeit der letzten Nachricht. Bei WhatsApp, dem weltweit beliebtesten Messenger-Dienst, können die Ermittler jedoch auf Nutzerdaten, gesperrte Konten, Kontakte und Nachrichtenziele zugreifen.

135 Thomas Rudl und Markus Reuter, „Warum die Chatkontrolle so gefährlich ist", Netzpolitik, 4. November 2021: https://netzpolitik.org/2021/eu-kommission-warum-die-chatkontrolle-so-gefaehrlich-ist/ (abgerufen am 1. Juni 2022).

136 Europäische Kommission, „Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse", COM(2022)209 final, (Mai 2022): https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF (abgerufen 1. Juni 2022).

137 Ebd., S. 2.

138 Stefan Krempl, „Chatkontrolle: Informatiker und IT-Verbände gegen EU-weite Massenüberwachung", Heise Online, 29. März 2022: https://www.heise.de/news/Chatkontrolle-Informatiker-und-IT-Verbaende-gegen-EU-weite-Massenueberwachung-6656545.html (abgerufen am 1. Juni 2022).

US-Cloud-Anbieter sensible Daten überhaupt speichern sollten. Ihre Bedenken betreffen die Ungewissheit über den Datenschutz bei der transatlantischen Datenübermittlung nach dem Schrems-II-Urteil und die Ermächtigung der US-Strafverfolgungsbehörden im Rahmen des US CLOUD Act auf Daten zuzugreifen, die auf Servern von US-Cloud-Anbietern in Europa gespeichert sind.[139]

Deutschland erwägt daher Regeln für die Cloud-Nutzung in der Verwaltung und in sensiblen Bereichen, da die EU ein Cloud-Zertifizierungsverfahren einführen möchte, das Fragen bezüglich Datenlokalisierung berücksichtigt. Deutschland schloss sich Frankreich, Italien und Spanien an – gegen die Niederlande, Schweden und Irland – und unterstützte die „Souveränitätsanforderungen" im EUCS und dem Gaia-X-Labelling-Framework, die im Wesentlichen Datenlokalisierung als Anforderung unterstützen. Die höchsten Sicherheitsstufen von EUCS und Gaia-X, nämlich „Hoch" und „Stufe 3", würden die Auswahl an Providern einschränken und die EU möglicherweise von Hyperscalern wie Amazon, Microsoft und Google, die ihren Sitz in den Vereinigten Staaten haben, sowie von europäischen Unternehmen mit amerikanischer Präsenz, darunter die Deutsche Telekom, SAP und Bertelsmann, abschneiden. Obwohl diese Zertifizierungssysteme derzeit noch freiwillig sind, wird davon ausgegangen, dass sie in Zukunft in irgendeiner Form für die Erbringung öffentlicher Dienstleistungen in der EU erforderlich sein werden – mit schwerwiegenden Auswirkungen auf die Datennutzung in digitalen Lieferketten. Digitale Smart-City-, Gesundheits- und Bildungsdienste gehören zu den Bereichen, die davon betroffen sein werden.

DEUTSCHLANDS GEOPOLITISCHE SCHWACHPUNKTE IN DER REGULIERUNG

Während sich die deutsche Politik in den Bereichen digitale Identität, Cybersicherheit, Strafverfolgung und Cloud-Governance weiterentwickelt, sind drei Schwachpunkte offensichtlich. Diese können Deutschlands Fähigkeit und die der EU, Governance und Innovation in Einklang zu bringen sowie ihre Gestaltungskraft zu maximieren, beeinträchtigen.

Erstens wird die weitgehend erfolgreiche Rolle Deutschlands als wichtiger Impulsgeber für den regulatorischen Ansatz der EU im Bereich der digitalen Technologien – und damit als Triebfeder des „Brüssel-Effekts" bei der Prägung globaler Märkte – in Deutschland selbst kaum anerkannt oder verstanden. Vielmehr ist die deutsche Technologiediskussion nach innen gerichtet und beachtet kaum, welchen Einfluss Deutschland auf die EU und die Welt haben. Die Politik überlässt es oft den Technokraten, reaktiv nationale Präferenzen auf europäische Ebene zu heben. Die Debatte neigt auch dazu, die potenziell globalen Auswirkungen deutscher Regularien auszublenden, und es gelingt ihr nicht, die deutschen Vorbehalte in Bezug auf Digitalisierung und Datenflüsse, die weiterhin im EU-Recht zum Ausdruck kommen, konsequent zu adressieren.

Zweitens gibt es nach wie vor geopolitische Herausforderungen im Zusammenhang mit der Umsetzung und Durchsetzung bestehender Regularien, insbesondere der DSGVO, des DSA und des DMA, was eine Diskrepanz zwischen Vorschriften und dem Kontext, in dem sie festgelegt wurden, widerspiegelt. Der überwiegend euro-atlantische Fokus deutscher und europäischer Rechtsdurchsetzung entspricht dem internationalen digitalen Status quo zwischen 2012 und 2015. Seitdem sind chinesische und russische staatsnahe Akteure zu bedeutenden Anbietern von Cloud-Diensten, Plattformdiensten, geschlossenen Messaging-Systemen und intelligenter Infrastrukturtechnologie geworden. Auch das Internet der Dinge hat an globaler Bedeutung gewonnen. Die Durchsetzung der Rechtsvorschriften konnte nicht Schritt halten, was in Deutschland und Europa zu Schwachstellen in der Digital-Governance geführt hat.

Drittens kommt die Gestaltung von Regeln für neue Technologien in Deutschland regelmäßig nur langsam zustande, obwohl das Land in der Lage ist, die EU-Debatte zu antizipieren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat erstmals ein Grundschutz-Profil für die Cybersicherheit von LEO-Satelliten-Netzwerken herausgegeben, die als Grundlage für Modellstandards der Europäischen Weltraumorganisation dienen sollen.[140] Und die öffentlich finanzierte Forschung und Entwicklung im Bereich der Quantenverschlüsselung wird

139 Einige haben sogar den Grad der Kontrolle durch die chinesische Firewall als positives Modell für ein europäisches Internet angeführt. Nick Sohnemann et al., „New Developments in Digital Services", Europäisches Parliament, Fachabteilung Wirtschaft, Wissenschaft und Lebensqualität der Generaldirektion Interne Politikbereiche der Union (Mai 2020): https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648784/IPOL_STU(2020)648784_EN.pdf (abgerufen am 11. März 2021).

140 Catherine Stupp, "Germany Offers Model for Space-Industry Cybersecurity Standards," The Wall Street Journal, 17. August 2022: https://www.wsj.com/articles/germany-offers-model-for-space-industry-cybersecurity-standards-11660728604 (abgerufen am 12. September 2022)

dazu beitragen, Standards für die Post-Quanten-Kryptografie zu entwickeln, auch in Zusammenarbeit mit Partnern wie dem US National Institute of Standards and Technology (NIST).[141] Nichtsdestotrotz gibt es zwischen technologischer Entwicklung und Governance in Deutschland, Europa und gleichgesinnten Staaten nach wie vor eine ausgeprägte Diskrepanz. Dies ist für das von Deutschland und Europa gewünschte strategische Regulierungsumfeld kaum förderlich. Da die Marktgröße Deutschlands und der EU im Vergleich zum Rest der Welt schrumpft, nimmt auch ihre Regulierungsmacht ab. Mittelfristig wird der wachsende Einfluss der Nachfrage in Indien und im globalen Süden ihre Rolle bei der Festlegung globaler Regeln, Normen und ihre Marktmacht neu definieren.

Handlungs-empfehlungen

Drei Faktoren sind ausschlaggebend dafür, ob die Bundesregierung in der Lage sein wird, die globale Regelsetzung zu beeinflussen: die Kohärenz ihrer Vision, die Beständigkeit bei der Regeldurchsetzung in Deutschland und in der EU sowie die Fähigkeit, Vorschriften zu erlassen, die die europäische Innovationsfähigkeit (auch für neue kritische Technologien) bewahren und stärken, ohne protektionistischen Tendenzen Vorschub zu leisten. Um deutsche Regeln und Normen in einen konsequenteren geostrategischen Ansatz einzubetten, sollte die Bundesregierung:

Politische Abwägungen im Zusammenhang mit digitalpolitischen Entscheidungen adressieren. Bei den schwierigsten Aspekten der Digital-Regulierung stehen wichtige deutsche Prioritäten wie Datenschutz und Sicherheit oft im Widerspruch zueinander. Dies zwingt politische Entscheidungsträgerinnen und -träger dazu, Ziele gegeneinander abzuwägen. Debatten über Themen wie Datenschutz, Strafverfolgung und nationale Sicherheit sollten den Gesamtkontext berücksichtigen, eine transparente Aufsicht ermöglichen und auf dem Grundsatz aufbauen, dass Aktivitäten, die offline illegal sind, dies auch online sind.

Musterklauseln und -module erarbeiten, die in Regularien von Partnerländern integriert werden können. Es könnte ein Verzeichnis von Open-Source-Regeln geschaffen werden, das den Prozess für außereuropäische Partner beschleunigt, wenn es darum geht, Angemessenheit mit der EU in Bezug auf den Austausch personenbezogener und industrieller Daten, die IoT-Sicherheit und die Moderation von Inhalten zu erreichen und die oben erwähnten Herausforderungen mit der DSGVO zu bewältigen. Musterklauseln und -module sollten so gestaltet werden, dass ihrem Missbrauch durch autoritäre Regierungen zur Rechtfertigung von Massenüberwachung, Zensur und Datendiebstahl entgegengewirkt wird. Die Bundesregierung sollte auch die Fähigkeit anderer europäischer Staaten unterstützen, ihre eigenen Vorschriften zu erlassen; die EU wiederum könnte Partnerländern helfen, deren Auswirkungen zu evaluieren.

Geopolitische Folgenabschätzungen für Entwürfe deutscher und europäischer Digital-Regulierung durchführen. Wie wir dargelegt haben, könnten Maßnahmen von Deutschland und der EU unbeabsichtigt digitalem Autoritarismus Vorschub leisten oder unerwünschte globale Trends wie Datenlokalisierung, Zensur, Schwächung von Cybersicherheit oder Internetfragmentierung begünstigen. Autoritäre Staaten wie China und Russland haben bereits gezeigt, dass sie bereit sind, solche unbeabsichtigten Folgen auszunutzen, indem sie Regeln spiegeln und kombinieren, um Massenüberwachung, Zensur und digitale Kontrolle über ihre Bürgerinnen und Bürger zu rechtfertigen. Eine aufmerksame Bewertung der Auswirkungen der deutschen und der EU-Technologiepolitik außerhalb Europas könnte solchem Missbrauch entgegenwirken.

Dem zunehmenden Staatszentrismus bei der europäischen technischen Standardsetzung entgegentreten. Der internationale Einfluss europäischer Organisationen wie des Europäischen Komitees für Normung (CEN), des Europäischen Komitees für elektrotechnische Normung (CENELEC) und des Europäischen Instituts für Telekommunikationsnormen (ETSI) beruht weitgehend auf ihrer Offenheit für private Akteure, einschließlich außereuropäischer Unternehmen. Es geht nicht darum, technische Standardsetzung einfach dem Privatsektor zu überlassen.

141 Barbara-Henrika Alfing, "Bochum researchers win worldwide post-quantum cryptography competition", Ruhr Universität Bochum, 6. Juli 2022: https://news.rub.de/english/press-releases/2022-07-06-future-proof-data-encryption-bochum-researchers-win-worldwide-post-quantumcryptography-competition (abgerufen am 12. September 2022)

Die Bundesregierung sollte jedoch ein großes Interesse daran haben, die Führungsrolle des Privatsektors mit den staatlichen und europäischen Interessen in Einklang zu bringen. Sie muss die Bemühungen anführen, den pluralistischen Charakter der europäischen Normung zu erhalten. Wenn sich das Gleichgewicht zu sehr zugunsten des Staates verschiebt, besteht die Gefahr, dass die Leistungsfähigkeit Deutschlands und Europas in diesem Bereich beeinträchtigt wird. Außerdem könnte dies einen ungewollten Präzedenzfall für autoritäre Regime schaffen.

Die Kapazitäten des privaten Sektors in der technischen Standardsetzung stärken. Die Bundesregierung sollte steuerliche Anreize und einen Mechanismus für staatliche Förderung deutscher Unternehmen, Start-ups und Verbände schaffen, damit sie in Normungsgremien mitwirken, Vorsitze übernehmen, neue einschlägige Normen entwickeln und mit gleichgesinnten Staaten zusammenarbeiten. Finanzielle Unterstützung könnte durch Zuschüsse des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) und des Bundesministeriums für Digitales und Verkehr (BMDV) erfolgen.

Die europäische Cloud-Zertifizierung und die Gaia-X-Architektur in die globalen Cloud-Governance-Bemühungen einbetten. Da Industriedaten zu einer neuen Front in der globalen Technologieregulierung werden könnten, sollte die Bundesregierung nach Wegen suchen, das Datenraummodell Gaia-X zu internationalisieren, um außereuropäische Partner, insbesondere die Vereinigten Staaten, einzubeziehen. Der EU-USA Trade and Technology Council (TTC) könnte demokratische Datenräume für Industriedaten auf der Grundlage der Gaia-X-Architektur in nationalen Hubs in gleichgesinnten außereuropäischen Ländern entwickeln. Die deutsche G7-Präsidentschaft, die sich in ihrer Endphase befindet, wäre eine Möglichkeit, die gemeinsame Arbeit für freie Datenflüsse auf Grundlage einer vertrauenswürdigen europäischen Regulierung und Architektur für die Speicherung, Verarbeitung und Übertragung von Daten in Gang zu setzen. Japan könnte diese Arbeit während seiner G7-Präsidentschaft 2023 fortsetzen. Schließlich könnte Deutschland den Aufbau von Kapazitäten in den Global Gateway-Partnerländern zur Nutzung europäischer Cloud Computing-Architekturen unterstützen, um die Interoperabilität zu erhöhen und die Menschenrechte zu wahren. Dieses Vorhaben stünde im Einklang mit dem Versprechen der Regierung, die digitale Souveränität im globalen Süden zu stärken.

Digital-Regulierung und technische Standardsetzung in die Zeitenwende und die Nationale Sicherheitsstrategie integrieren. Die Bundesregierung muss sich intensiver mit den Auswirkungen der Regulierung digitaler Technologien auf Deutschlands nationale Sicherheit und Verteidigungsindustrie befassen. Sie muss sicherstellen, dass Deutschland in der Lage ist, Technologien mit doppeltem Verwendungszweck in vergleichbarer Weise zu übernehmen und einzusetzen wie andere Länder, etwa Frankreich, Kanada, Japan und das Vereinigte Königreich. Dies erfordert mehr Flexibilität bei der Berücksichtigung der nationalen Sicherheitsinteressen. Die Bestimmungen des Gesetzes über künstliche Intelligenz könnten beispielsweise Anwendungen von Deep Learning verbieten, die von den Streitkräften anderer Staaten genutzt werden. Die vom deutschen Wettbewerbsrecht und der DMA vorgeschriebene Entflechtung digitaler Dienste wird auch unbeabsichtigte Folgen für die Fähigkeit von Unternehmen haben, ihre Cybersicherheit zu stärken. Die politischen Verantwortlichen in Deutschland müssen ihre Regulierungsmaßnahmen im Bereich der Technologie besser mit nationalen, EU- und NATO-Sicherheitsinteressen in Einklang bringen. Sie haben dies erfolgreich getan, als sie im IT-Sicherheitsgesetz 2.0 aus dem Jahr 2021 Kriterien für vertrauenswürdige Telekommunikationsausrüstung aufstellten.

Das Engagement der deutschen außen- und sicherheitspolitischen Gemeinschaft bei der Gestaltung und Durchsetzung von Regulierungsvereinbarungen erhöhen. Die deutschen Nachrichtendienste, die Außenpolitik, die Strafverfolgungs- und die Verteidigungsbehörden haben alle Anteil an der Durchsetzung nationaler Technologievorschriften. Während die USA eine stärkere Einbeziehung von Datenschützern in die Rahmengespräche fördern sollten, sollte die deutsche Regierung erkennen, dass es für diese Behörden an der Zeit ist, mehr Gewicht zu bekommen. Die post-Privacy Shield Transatlantic Data Privacy Framework-Ära (TDPF) wird eine erste Chance dafür bieten. Das deutsche Außenministerium und die nationalen Sicherheitsbehörden haben ein unmittelbares Interesse an der Aufrechterhaltung einer offenen Datenbrücke zwischen der EU und den USA, die gleichzeitig privaten Akteuren den Zugang zu US-Gerichten sowie einklagbare Rechte und Beschränkungen für die wahllose Erhebung personenbezogener Daten zusichert. Sie müssen eine Führungsrolle übernehmen, um sicherzustellen, dass das TDPF eine dauerhafte Lösung ist, angesichts der Gelegenheit, die es bietet, klare Regelungen für einen freien euro-atlantischen Datenverkehr zu schaffen.

Multistakeholder-Ansatz unter Einbeziehung von Zivilgesellschaft, Unternehmen und anderen nichtstaatlichen Akteuren ermöglichen. Deutschland und Europa haben begonnen, neue Modelle für die Regulierung von Technologien zu entwickeln. Die bisherige Regulierung war hochgradig reglementiert und entsprach damit den Entwicklungspfaden industrieller Technologien, die in Fabrikhallen zum Einsatz kamen. Die Regulierung der digitalen Sphäre muss jedoch agil, auf dem Ökosystem basierend und auf die Schaffung von Anreizen ausgerichtet sein. In Anlehnung an das DSA/DMA-Modell muss sie ein Geflecht von Beziehungen, Zuständigkeiten und Aufsichtsfunktionen umfassen, das schneller Alarm schlagen kann, wenn regulatorische Schwachstellen erkennbar werden. Diese flexiblen Strukturen ermöglichen eine ständige und gleichzeitig kompromissfähige Aufsicht.

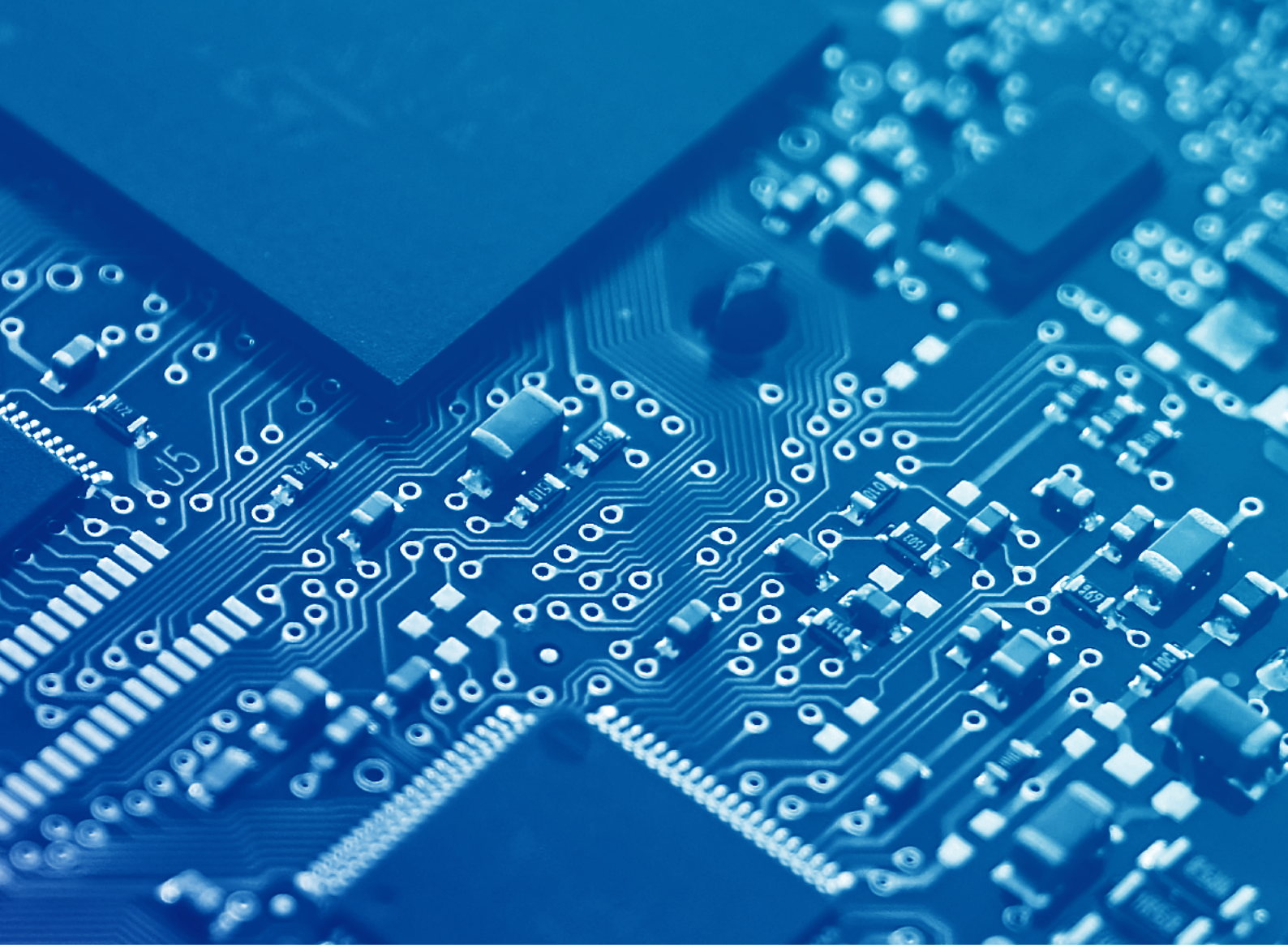
Evaluierungen und Auslaufklauseln in der digitalen Regulierung ausweiten, um Flexibilität zu fördern. Angesichts der Geschwindigkeit des Wandels digitaler Technologien ist regulatorische und rechtliche Flexibilität zentral. Evaluierungen und Auslaufklauseln würden die Regulierungsbehörden dazu zwingen, die Wirksamkeit und Relevanz von Vorschriften zu prüfen. Solche Klauseln würden auch die Kohärenz mit der Regulierung in anderen Demokratien fördern. Das bereits erwähnte Beispiel der Datenschutz-Grundverordnung zeigt die Notwendigkeit solcher Bemühungen, die mit dem Gebot der Gewährleistung von Rechtssicherheit und der Bedeutung von Reformen für eine zukunftssichere Regulierung in Einklang stehen.

7 – DEUTSCHE UND EU-REGULIERUNG DIGITALER TECHNOLOGIEN (2015-HEUTE)

Deutsche Initiative	Zielsetzungen	EU-Initiative	Zielsetzungen
2015 **IT-Sicherheitsgesetz**	• führende Standards für IT-Systemsicherheit setzen • digitale Infrastrukturen schützen, insbesondere in kritischen Technologie-Bereichen (kritische Infrastrukturen/KRITIS) • eine neue Warnpflicht in der Telekommunikationsbranche einführen	2016 **NIS-Richtlinie (NIS Directive)**	• eine nationale Aufsicht über kritische Infrastruktursektoren und kritische Anbieter digitaler Dienste mandatieren • Anforderungen an die Cybersicherheitsfähigkeiten der Mitgliedstaaten festlegen, einschließlich Cybersicherheitsstrategien und Computer Security Incident Response Teams (CSIRTS) • grenzübergreifende Zusammenarbeit fördern
2017 **Netzwerkdurchsetzungsgesetz (NetzDG)**	• Rahmenwerke für die Moderation von strafbaren Inhalten wie Hassreden und Fake News definieren • Meldepflichten und Sanktionen für Online-Plattformen festlegen	2020 **Gesetz über digitale Dienste (Digital Services Act, DSA) – Entwurf**	• die EU-weiten Rechtsvorschriften in Bezug auf digitale Plattformen reformieren • Standards für die Moderation von Inhalten, Werbung und Algorithmen setzen • Verpflichtungen, einschließlich Melde- und Aktionsverfahren, bei rechtswidrigen Inhalten definieren
2017 **Datenethikkommission**	• ethische Richtlinien zur Datenpolitik entwickeln • einen Rahmen für den Umgang mit Algorithmen, KI und digitaler Innovation bereitstellen • Fragen zur Datenethik klären • einen Ansatz zur Überwindung sozialer Konflikte in der Datenpolitik definieren	2021 **Gesetz über künstliche Intelligenz (AI Act) – Entwurf** (basierend auf dem KI Whitepaper der Europäischen Kommission von 2020)	• einen „menschenzentrierten" Rechtsrahmen für vertrauenswürdige KI entwerfen • Auseinandersetzung mit den Risiken, die mit bestimmten Anwendungen von KI verbunden sind • das Vertrauen der Nutzerinnen und Nutzer in KI-basierte Lösungen stärken und Unternehmen bei deren Entwicklung fördern
2018 **Nationale Forschungsdateninfrastruktur (NFDI)**	• Datenbestände im In- und Ausland vernetzen • Wissenschafts- und Forschungsdaten systematisch entwickeln, nachhaltig speichern und zugänglich machen	2018 **European Open Science Cloud (EOSC)**	• ein offenes, multidisziplinäres Umfeld für europäische Forscherinnen und Forscher, Innovatorinnen und Innovatoren, Unternehmen sowie Bürgerinnen und Bürger schaffen • eine erstklassige Dateninfrastruktur, Hochgeschwindigkeitsverbindungen und leistungsstarke Computer für die europäische Wissenschaft, Industrie und öffentliche Einrichtungen bereitstellen
2019 **Gaia-X-Initiative**	• einen gemeinsamen Rahmen für Software-Governance entwickeln, mit dem Ziel, die digitale Souveränität Europas zu gewährleisten • ein gemeinsames Regelwerk implementieren, das auf bestehende Technologie-Stacks angewendet werden kann • Transparenz, Kontrollierbarkeit, Übertragbarkeit und Interoperabilität von Daten und Diensten erreichen	2021 **Allianz für Industriedaten, Edge und Cloud**	• die Position der EU-Industrie im Bereich der Cloud- und Edge-Technologien stärken • die Anforderungen von EU-Unternehmen und öffentlichen Verwaltungen erfüllen, die sensible Daten verarbeiten • die Entwicklung und Bereitstellung von Cloud- und Edge-Kapazitäten der nächsten Generation für den öffentlichen und privaten Sektor fördern • Important Project of Common European Interest for Next Generation Cloud Infrastructure and Services (IPCEI-CIS) trägt zur Überprüfung der EU-Industriestrategie bei
2019 **Blockchain-Strategie der Bundesregierung**	• die Möglichkeiten, die die Blockchain bietet, nutzen und ihr Potenzial für die digitale Transformation mobilisieren • fünf Handlungsfelder: Blockchain im Finanzsektor; Finanzierung von Projekten und Reallaboren; klare und sichere Rahmenbedingungen; digitale Verwaltungsdienstleistungen; Wissen, Vernetzung und Zusammenarbeit		
2021 **Datenstrategie der Bundesregierung**	• die innovative und verantwortungsvolle Nutzung von Daten fördern • Datenkompetenz und eine Datenkultur entwickeln • die Dateninfrastruktur effektiv und nachhaltig gestalten • eine tragfähige staatliche Dateninfrastruktur aufbauen und die Datenkompetenz der Beamtinnen und Beamten stärken	2022 **Datengesetz**	• Fairness durch Regeln für die Nutzung der von IoT-Geräten erzeugten Daten sicherstellen • einen Rahmen zur Förderung des Datenaustauschs zwischen Unternehmen und staatlichen Stellen entwickeln • Business-to-Business-Datenübermittlung unterstützen • den Rahmen für die integrierte Planung und Berichterstattung (IPR) im Hinblick auf eine weitere Verbesserung des Datenzugangs und der Datennutzung evaluieren
		2020 **Daten-Governance-Gesetz – Entwurf**	• das Vertrauen in Datenübermittlung stärken • die Mechanismen für den Datenaustausch zwischen den einzelnen Sektoren und der EU stärken, die Datenverfügbarkeit verbessern und technische Hindernisse für die Wiederverwendung von Daten überwinden
		2021 **EU Cloud Code of Conduct**	• zu einem Umfeld des Vertrauens und der Transparenz auf dem europäischen Cloud-Computing-Markt beitragen • den Prozess zur Risikobewertung von Cloud-Service-Anbietern (CSPs) für Cloud-Kunden vereinfachen
2021 **IT-Sicherheitsgesetz 2.0**	• Sicherheitslücken zum Schutz kritischer Infrastrukturen (KRITIS) schließen • die Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ausweiten, um eine stärkere Zusammenarbeit mit den Strafverfolgungsbehörden zu ermöglichen	2021 **Reform der NIS-Richtlinie**	• das NIS-Mandat ausweiten, um Fragmentierungs- und Umsetzungsprobleme zu adressieren • den Informationsaustausch, die Meldepflicht und die Sanktionsregelungen innerhalb der EU koordinieren • strengere Anforderungen für kritische Infrastrukturen, z. B. für die Sicherheit von Lieferketten, einführen

Quelle: Eigene Darstellung

Deutsche Initiative	Zielsetzungen	EU-Initiative	Zielsetzungen
2021 **Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)**	• die bisher im Telekommunikationsgesetz (TKG) und im Telemediengesetz enthaltenen Vorschriften zum Schutz des Fernmeldegeheimnisses und von Daten in einem neuen Stammgesetz zusammenführen • bestehende Bestimmungen an die europäische Datenschutzgrundverordnung und an neue Definitionen im Telekommunikationsgesetz anpassen	2017 **E-Privacy-Richtlinie – Entwurf**	• Datenschutzregeln für neue Akteure wie WhatsApp, Facebook Messenger und Skype durchsetzen • den EU-Datenschutz standardisieren • Kommunikationsinhalte und Metadaten schützen • die Cookie-Zustimmungsregelung vereinfachen • Benutzerinnen und Benutzer effektiver vor Spam schützen
		2020 **Daten-Governance-Gesetz – Entwurf**	• den sicheren Austausch sensibler Daten, die sich im Besitz • öffentlicher Einrichtungen befinden, ermöglichen, und den Datenaustausch durch öffentliche Akteure regeln • das Vertrauen zu Datenmittlern steigern • die Mechanismen für den EU-weiten Datenaustausch stärken
2021 **10. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen (GWB)**	• das Bundeskartellamt (BKartA) dazu befähigen, präventive Maßnahmen zur Eindämmung der Marktmacht großer digitaler Plattformen zu ergreifen • Änderungen in Bezug auf kartellrechtliche Ermittlungsverfahren, Kronzeugenregelung und Kartellschadensersatzansprüche einführen	2020 **Gesetz über digitale Märkte (Digital Market Act, DMA**	• unlautere Geschäftspraktiken digitaler Gatekeeper eindämmen • ein faires Geschäftsumfeld für Unternehmen schaffen, die von Gatekeepern abhängig sind • freiere Innovation durch Technologie-Start-ups ermöglichen • unfaire Bedingungen beseitigen, die die technologische Entwicklung einschränken • die Auswahl an Dienstleistungsunternehmen für Kunden ausweiten
2021 **Novelle des Telekommunikationsgesetzes (TKG)**	• einen maßgeschneiderten und zukunftsweisenden Rechtsrahmen für den deutschen Telekommunikationsmarkt schaffen • die Rechte von Endnutzerinnen und -nutzern stärken • den Ausbau von Glasfaser- und Mobilfunknetzen beschleunigen	2018 **Richtlinie (EU) 2018/1972:** über den europäischen Kodex für die elektronische Kommunikation	• den Rahmen für die Regulierung elektronischer Kommunikationsnetze und -dienste konsolidieren und reformieren
2020 **Gesetzentwurf zur Umsetzung von Richtlinie (EU) 2018/1972**	• Netze mit sehr hoher Kapazität und ihre Nutzung ausbauen • nachhaltigen und wirksamen Wettbewerb und die Interoperabilität von Telekommunikationsdiensten gewährleisten • Zugänglichkeit und Sicherheit von Netzen und Diensten sicherstellen • die Interessen der Endnutzerinnen und -nutzer stärken		
2021 **17. Novelle der Außenwirtschaftsverordnung (AWG)**	• Im Rahmen der AWG kritische Infrastrukturen und Schlüsseltechnologien umfassend vor ausländischen Investitionen schützen • anzeigepflichtigen Erwerb auf neue Branchen im sektorübergreifenden Screening ausweiten • die relevanten Schwellenwerte für Meldepflichten senken • das sektorspezifische Screening ausweiten • die Fristen für sektorübergreifende und -spezifische Prüfungen standardisieren	2019 **Verordnung zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union**	• die strategischen Interessen Europas wahren bei gleichzeitiger Offenhaltung des EU-Marktes für Investitionen • europäische Bedenken hinsichtlich der Auswirkungen ausländischer Übernahmen berücksichtigen • die Meldung bestehender nationaler Mechanismen zur Investitionsüberwachung an die Europäische Kommission (EK) regulieren • formelle Kontaktstellen und sichere Kanäle in jedem Mitgliedstaat und innerhalb der EK für den Informationsaustausch einrichten • Verfahren entwickeln, die es den Mitgliedstaaten und der EK ermöglichen, rasch auf Bedenken hinsichtlich ausländischer Direktinvestitionen zu reagieren
		2021 **Richtlinie (EU) 2021/821** über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung der Durchfuhr und der Verbringung betreffender Güter mit doppeltem Verwendungszweck	• den bisherigen Rechtsrahmen zur Modernisierung der EU-Ausfuhrkontrollregelung für Güter mit doppeltem Verwendungszweck aktualisieren • eine Regelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck schaffen • Güter mit doppeltem Verwendungszweck wirksam kontrollieren, wenn sie aus der EU ausgeführt oder durch die EU durchgeführt werden • neue Catch-All-Kontrollen implementieren • nationale Kontrolllisten erstellen und neue Kontrollen für technische Unterstützung einführen – auch für die militärische Endverwendung • mehr Informationsaustausch und Transparenz gewährleisten
2017 **Open-Data-Gesetz**	• Bundesbehörden verpflichten, unbearbeitete Daten, die bei der Erfüllung öffentlich-rechtlicher Aufgaben oder durch Dritte gewonnen wurden, in öffentlich zugänglichen Netzen zu veröffentlichen • eine gesetzliche Grundlage für die Beschaffung von Daten aller öffentlichen Behörden schaffen, die der Aufsicht der Bundesregierung unterliegen	2019 **Open-Data-Richtlinie**	• die Datenwirtschaft in der EU durch Erhöhung des Umfangs der in öffentlichem Besitz befindlichen und öffentlich finanzierten Daten stärken, die zur Weiterverwendung zur Verfügung stehen • öffentliche Stellen verpflichten, Daten nach Möglichkeit zur Wiederverwendung zur Verfügung zu stellen • Echtzeit-Zugang zu dynamischen Daten mit geeigneten technischen Mitteln bereitstellen • das Angebot an wertvollen öffentlichen Daten zur Weiterverwendung erhöhen, auch von öffentlichen Unternehmen • das Entstehen neuer Formen von Ausschließlichkeitsbindungen bekämpfen



KAPITEL 5

Deutschlands wirtschaftliche Sicherheit und Technologie

Exportkontrollen, Investitionsprüfung und Marktzugangsinstrumente optimieren

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.[142] 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

142 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).[143] 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

143 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).

8 – 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.[144] 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.[145] Deutschland hat seine Ausfuhrkontrollen nach 2015 verschärft, was zur Insolvenz von FinFisher im Jahr 2022 geführt hat.[146] 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.[147]

Auch die Investitionsprüfung wurde im Zuge des zunehmenden technologischen Wettstreits zwischen den USA und China überarbeitet. Auf nationaler Ebene hat Deutschland das Außenwirtschaftsgesetz (AWG)[148]

144 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).

145 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).

146 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).

147 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).

148 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)[149] reformiert, um die Kontrolle ausländischer Direktinvestitionen zu stärken und zu modernisieren.[150] 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.[151] 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.[152]

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“,[153] 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.[154]

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

149 Ebd.

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

151 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).

152 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).

153 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).

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

zur Überprüfung von ausländischen Direktinvestitionen beeinflusst. Der US-Kongress hat 2018 damit 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.[155] 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.[156] 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.[157] 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.[158] 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.[159] 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)

155 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).

156 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).

157 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).

158 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).

159 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.

und US-amerikanischer Hyperscaler-Cloud-Dienste (Amazon Web Services und Microsoft Azure Cloud) in Deutschland und anderen Mitgliedstaaten, in der 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.[160]

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.[161] Deutschland hat auch die Sorgfaltspflichten für Lieferketten in Bezug auf Menschenrechte aktualisiert, einschließlich der Nutzung von Zwangsarbeit.[162]

Die Europäische Kommission hat sich ihrerseits für ein stärkeres Onshoring und Friendshoring von Technologie und strategisch wichtigen Komponenten eingesetzt, auch mittels ihrer Industriepolitik.[163] Das Europäische Chip-Gesetz ist neben den wichtigen Vorhaben von gemeinsamem europäischem Interesse (Important Projects of Common European

160 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).

161 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).

162 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).

163 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).

Interest, IPCEI) der ehrgeizigste Versuch, einen Rahmen für den Zugang zu kritischen Technologien und deren Resilienz zu schaffen. Gemäß dem Gesetz soll die 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.[164]

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.[165] 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.[166] 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).[167] Einige der EU- und NATO-Partner Deutschlands sind der Ansicht, dass die Nutzung von Huawei-Komponenten

164 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).

165 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).

166 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).

167 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).

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 mit der IT-Sicherheitssoftware Kaspersky gewarnt und hat der deutschen Privatwirtschaft empfohlen, diese nicht mehr einzusetzen.[168]

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.[169] 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.[170] 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.[171] Fälle von Infiltrationen im des Wissenschaftsbereichs von durch autoritäre Regierungen beauftragten Personen geben der EU Anlass zur Sorge.[172] 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.[173] 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.

Handlungsempfehlungen

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:

168 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).

169 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).

170 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).

171 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).

172 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).

173 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).

Gemeinsam mit Verbündeten einen multilateralen Ausschuss für Technologiekontrolle im 21. Jahrhundert schaffen. Dieser neue Ausschuss würde den Informationsaustausch und die Koordinierung 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.[174]

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.[175] 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[176] 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.[177]

174 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).

175 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).

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

177 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).

Die europäische Beteiligung an neu entstehenden Vereinbarungen über den Zugang zu Technologien und deren Kontrolle im indopazifischen Raum fördern. Eine stärkere strategische Konvergenz 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.[178]

178 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).

KAPITEL 6

Deutschlands globale Technologie-Diplomatie

Internationale Allianzen, Partnerschaften und Normen im Technologiebereich stärken

KAPITELÜBERSICHT

Zentrale Erkenntnisse

1 Die Verschmelzung technologischer, geopolitischer und ideologischer Ambitionen befördert Spannungen in Internet Governance-Diskursen, Cyberdiplomatie, technischer Standardsetzung und der globalen Konnektivitätsinfrastruktur.

2 Die Bundesregierung hat die Unterstützung einer globalen, offenen und sicheren digitalen Vernetzung zu einem wichtigen Bestandteil ihrer Außenpolitik erklärt. Sie hat jedoch bisher die Ausarbeitung einer entsprechenden internationalen Technologieagenda noch nicht zu einer strategischen Priorität gemacht.

3 Um eine globale Technologieordnung zu schaffen, die die Interessen Deutschlands als Hightech-Vorreiter, globalisierte Volkswirtschaft und liberale Demokratie widerspiegelt, sollte sich die Bundesregierung darauf konzentrieren, Synergien mit der internationalen Digitalpolitik der EU auszuschöpfen, die Kooperation mit gleichgesinnten Partnern zu stärken und sich mit dem Globalen Süden für eine inklusive und demokratische globale digitale Agenda einzusetzen.

Einleitung

Russlands Krieg gegen die Ukraine hat die auf Stabilität ausgerichtete deutsche Strategie des „Wandels durch Handel" erschüttert. Er hat damit ebenfalls erhebliche Auswirkungen auf die deutsche digitale Außenpolitik, die sowohl wichtige geopolitische als auch ideologische Dimensionen hat.[179] China drängt in seinem Bestreben, die Vereinigten Staaten bis zur Mitte dieses Jahrhunderts als Großmacht zu überbieten, bereits jetzt auf Technologieführerschaft. Autoritäre Regierungen nutzen zudem digitale Technologien, die einst als Mittel gegen die Unterdrückung der Zivilgesellschaft gepriesen wurden, um ihre Macht im eigenen Land zu festigen.

Die Verschmelzung von technologischen, geopolitischen und ideologischen Ambitionen befördert Spannungen in Internet Governance-Diskursen, Cyberdiplomatie, technischer Standardsetzung und der globalen Konnektivitätsinfrastruktur. Um diesem Trend entgegenzuwirken, muss die Bundesregierung ihre internationalen Anstrengungen verstärken und eng mit Partnern und Verbündeten zusammenarbeiten. Sie muss sich aktiv für eine Governance-Landschaft einsetzen, welche Deutschlands Interessen und Werte als Hightech-Vorreiter, globalisierte Volkswirtschaft und liberale Demokratie widerspiegelt.

Status quo

Im Mittelpunkt der Fragmentierung, die die internationale digitale Governance durchdringt, steht der Wettbewerb um die Kontrolle über globale digitale Konnektivität. Das ursprüngliche Konzept eines offenen, globalen, dezentralisierten und von mehreren Stakeholder-Gruppen verwalteten Internets steht im Widerspruch zu den Bestrebungen einiger Staaten, Informationsflüsse und die politische Meinungsäußerung stärker zu kontrollieren. So stellten China und Russland gemeinsam klar, dass sie „jeden Versuch, ihr souveränes Recht einzuschränken, nationale Segmente des Internets zu regulieren und ihre Sicherheit zu gewährleisten" für inakzeptabel halten.[180] Ebenso besorgniserregend ist die zunehmende Einführung von Systemen zur Inhaltsüberwachung sowie Internetsperren, wie beispielsweise während der Proteste gegen die Regimes in Belarus (Sommer 2020)[181], Kasachstan (Winter 2021–2022)[182] und Iran (Herbst 2022).[183]

179 David Hagebölling, „The Geopolitical Struggle for Technology Leadership", Internationale Politik Quarterly (12. April 2022): https://ip-quarterly.com/en/geopolitical-struggle-technology-leadership (abgerufen am 15. September 2022).

180 „Russia and China call for internationalization of Internet governance — statement", TASS, 4. Februar 2022: https://tass.com/economy/1398177 (abgerufen am 22. Juni 2022).

181 Andrei Makhovsky und Tom Balmforth, „Internet blackout in Belarus leaves protesters in the dark", Reuters, 11. August 2020: https://www.reuters.com/article/us-belarus-election-internet-idUSKCN2571Q4 (abgerufen am 15. September 2022).

182 Elizabeth Zach und Amalia Oganjanyan, „Internet blackout in Kazakhstan amid protests silenced a DW Akademie partner for nearly a week", Deutsche Welle, 4. März 2022: https://www.dw.com/en/internet-blackout-in-kazakhstan-amid-protests-silenced-a-dw-akademie-partner-for-nearly-a-week/a-61017740 (abgerufen am 15. September 2022).

183 Matt Burgess, „Iran's Internet Shutdown Hides a Deadly Crackdown", Wired, 23. September 2022: https://www.wired.co.uk/article/iran-protests-2022-internet-shutdown-whatsapp (abgerufen am 27.10.2022).

Diese konkurrierenden Visionen führen zu einer Verschärfung der Auseinandersetzungen rund um das Internet selbst, vor allem innerhalb der Gremien, die es verwalten und weiterentwickeln.[184] Als Antwort hierauf haben die demokratischen Staaten des Globalen Nordens – darunter auch Deutschland – ihre Unterstützung für technische Internet Governance nochmals bestärkt. Diese fußt vor allem auf einer Reihe von Multistakeholder-Gremien, darunter die Internet Society (ISOC), die Internet Corporation for Assigned Names and Numbers (ICANN)[185] und die Internet Engineering Task Force (IETF). Einige Länder treiben zudem ambitionierte Regulierungsinitiativen voran, wie das EU-Gesetz über digitale Märkte (DMA), um die Zentralisierung und Vermittlung privater und kommerzieller Online-Aktivitäten durch große Tech-Unternehmen zu begrenzen. Entscheidend ist hierbei, dass demokratische Staaten im Begriff sind eine gemeinsame politische Vision zu entwickeln, wie etwa geschehen bei dem Appell von Christchurch („Christchurch Call") für ein freies, offenes und sicheres Internet, dem Appell von Paris für Vertrauen und Sicherheit im Cyberraum („Paris Call") und kürzlich durch die Erklärung der G7-Staaten über resiliente Demokratien im Rahmen des Elmauer Gipfels.[186]

Bei diesen Bemühungen stehen die Demokratien autoritären Staaten gegenüber, insbesondere China, Russland und Iran, die nationale Souveränität und staatliche Kontrolle priorisieren. Auf internationaler Ebene verstärken diese Staaten ihre Bemühungen, Governance-Funktionen von den von Deutschland und seinen Partnern unterstützten Multistakeholder-Gremien auf andere Organisationen zu übertragen. Das chinesische Unternehmen Huawei wählte beispielsweise die zwischenstaatliche Internationale Fernmeldeunion (ITU), um eine „NewIP"-Initiative[187] zur Weiterentwicklung des Internetprotokolls (IP) einzubringen. Dies könnte nicht nur die Arbeit der Multistakeholder-Gremien und die Interoperabilität mit der bestehenden IP-Architektur untergraben, sondern, so befürchten einige, auch mehr Möglichkeiten für Informationskontrolle in dieser „logischen" Schicht des Internets schaffen.[188] China fördert seine Agenda für Cyber-Souveränität zudem durch den parallelen Aufbau von Institutionen. Jüngstes Beispiel hierfür ist die Gründung der Welt-Internet-Konferenz in Wuzhen als internationale Organisation.[189]

Diese Bruchlinien kennzeichnen auch die internationale Diplomatie in Bezug auf Cybernormen. Mit dem Abschlussbericht der United Nations Open-ended Working Group (OEWG) wurde im vergangenen Jahr zum ersten Mal ein Konsens über Cybernormen in einem für alle Mitgliedstaaten der Vereinten Nationen (VN) offenen Prozess erzielt. Besonders hervorzuheben ist, dass der Bericht eine Einigung über den Wortlaut und Empfehlungen für verantwortungsvolles staatliches Handeln, die aus den Sitzungen der United Nations Group of Governmental Experts (UN GGE) hervorgegangenen sind, enthält.[190] Es bestehen jedoch weiterhin Uneinigkeiten, insbesondere in Bezug auf die Einbeziehung nichtstaatlicher Akteure und die Konzentration auf die Umsetzung von Normen – beides Punkte, die Deutschland unterstützt.[191] Ein von Deutschland ebenfalls unterstützter französisch-ägyptischer Vorschlag für ein Aktionsprogramm,[192] mit dem die Zusammenarbeit durch ein ständiges UN-Forum gestärkt werden soll, droht aus dem Blickfeld zu geraten, wenn dieser nicht zeitnah Gestalt annimmt.

Auch im Bereich der Cyberkriminalität bestehen weiterhin Differenzen. Nach einem Jahrzehnt gescheiterter Versuche erreichte Russland im Dezember 2019

184 David Hagebölling, „Internet Governance. Außenpolitik im Rückgrat der digitalen Welt", DGAP Memo Nr. 14, Deutsche Gesellschaft für Auswärtige Politik (September 2021): https://dgap.org/sites/default/files/article_pdfs/dgap-memo-btw21_14_dh_en_0.pdf (abgerufen am 22. Juni 2022).

185 Die 78. ICANN-Jahreshauptversammlung wird vom 21. bis 23. Oktober 2023 in Hamburg stattfinden.

186 G7 Germany, „2022 Resilient Democracies Statement", (27. Juni 2022): https://www.g7germany.de/resource/blob/974430/2057608/61edf594f5ca30fb7b2ae4b79d16f1e6/2022-06-27-g7-resilient-democracies-statement-data.pdf?download=1 (abgerufen am 15. August 2022).

187 Huawei, „New IP-Initiative", 2022: https://www.huawei.com/de/deu/magazin/aktuelles/new-ip (abgerufen am 22. Juni 2022).

188 Madhumita Murgia und Anna Gross, „Inside China's controversial mission to reinvent the internet", Financial Times, 27. März 2020: https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f (abgerufen am 27. Juni 2022).

189 World Internet Conference, „Xi sends congratulatory letter to inauguration of World Internet Conference organization", (13. Juli 2022): https://www.wuzhenwic.org/2022-07/13/c_788406.htm (abgerufen am 15. August 2022).

190 Generalversammlung der Vereinten Nationen, „Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report", A/AC.290/2021/CRP.2, 10. März 2021: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (abgerufen am 22. Juni 2022).

191 Valentin Weber, „How to Strengthen the Program of Action for Advancing Responsible State Behavior in Cyberspace", Just Security, 10. Februar 2022: https://www.justsecurity.org/80137/how-to-strengthen-the-programme-of-action-for-advancing-responsible-state-behavior-in-cyberspace/ (abgerufen 22. Juni 2022).

192 Regierungen von Frankreich, Ägypten und anderen Staaten, „The future of discussions on ICTs and cyberspace at the UN", 8. August 2020: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf (abgerufen am 27. Juli 2022).

die Zustimmung zu einer Resolution der UN-Generalversammlung,[193] in der die Ausarbeitung eines neuen Übereinkommens über Cyberkriminalität beschlossen wurde.[194] Die Verhandlungen über das Übereinkommen begannen in diesem Jahr und werden bis zur 78. Tagung der Generalversammlung im Jahr 2023 fortgesetzt.[195] Die Resolution ist jedoch ein Rückschlag für Deutschland, das die bestehende Budapest-Konvention stärken möchte, und es besteht die Sorge, dass ein neues Übereinkommen die Grundrechte unter dem Vorwand der Bekämpfung von Cyberkriminalität untergraben könnte.[196] Dies gilt auch für die Erklärung vom XIV. BRICS-Gipfel in Peking vom Juni 2022, in der die BRICS-Staaten ihre Unterstützung für das Ad-hoc-Komitee für ein neues Übereinkommen über Cyberkriminalität bekräftigten.[197]

Der Diskurs über Internet Governance und Cybernormen spiegelt auch einen besorgniserregenden globalen Trend unter den G77+-Staaten wider, von denen viele demokratisch sind, sich aber zwischen zwischenstaatlichen und Multistakeholder-Visionen der Internet Governance positionieren. Die G7-Erklärung über resiliente Demokratien unterstützen auch die +5 Länder (Argentinien, Indien, Indonesien, Senegal und Südafrika), die zum Gipfel in Elmau eingeladen waren.[198] Viele dieser Länder haben jedoch gezögert, den Appell von Paris und die Erklärung zur Zukunft des Internets (DFI)[199] zu zentralen Elementen einer globalen digitalen Ordnung zu machen – letztere wurde von Deutschland, der EU und mehr als 60 anderen Ländern unterzeichnet, um eine positive und menschenrechtsorientierte Vision für das Internet zu formulieren.[200]

Die zunehmende ideologische Fragmentierung schlägt sich auch in den Bemühungen nieder, Einflussmöglichkeiten im Bereich der technischen Infrastruktur auszuweiten, insbesondere im Globalen Süden. Die digitale Komponente der chinesischen Seidenstraßeninitiative (BRI) zielt darauf ab, Dutzende von Ländern durch chinesische Glasfaserkabel, Satellitennavigationssysteme, Rechenzentren und 5G/6G-Netzwerkinfrastruktur zu verbinden sowie Technologien für intelligente Städte und Häfen, vorhersagende Polizeiarbeit und Gesundheitsdatenanalyse zu fördern.[201] Diese digitale BRI erstreckt sich auf die unmittelbare Nachbarschaft der EU, einschließlich des Balkans[202] und Nordafrikas,[203] und auf Deutschland selbst, wo Duisburg als europäischer Endpunkt der BRI gilt.[204]

Als Reaktion auf die BRI hat die G7 unter deutschem Vorsitz erklärt, in den kommenden fünf Jahren im Rahmen ihrer Partnerschaft für globale Infrastruktur und Investitionen (PGII)[205] gemeinsam 600 Milliarden US-Dollar an öffentlichen und privaten Investitionen mobilisieren zu wollen. Es bleibt jedoch unklar, wie diese Mittel mobilisiert werden sollen und vor allem, wie ehrgeizig und wettbewerbsfähig die informations- und kommunikationstechnologische (IKT) Komponente der PGII im Vergleich zur der der BRI sein

193 Diese von der Generalversammlung der Vereinten Nationen verabschiedete Resolution wurde von Belarus, Kambodscha, China, der Demokratischen Volksrepublik Korea, Myanmar, Nicaragua und Venezuela mitgetragen. Generalversammlung der Vereinten Nationen, „Countering the use of information and communications technologies for criminal purposes. Report of the Third Committee", A/74/401, 25. November 2019: https://undocs.org/en/A/74/401 (abgerufen am 22. Juni 2022).

194 Generalversammlung der Vereinten Nationen, „Countering the use of information and communications technologies for criminal purposes", A/RES/74/247, 20. Januar 2020: https://undocs.org/A/Res/74/247 (abgerufen am 22. Juni 2022).

195 Vereinte Nationen, „General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over ‚Rushed' Vote at Expense of Further Consultations", 26. Mai 2021: https://www.un.org/press/en/2021/ga12328.doc.htm (abgerufen am 22. Juni 2022).

196 Rat der Europäischen Union, „Prioritäten der EU bei den Vereinten Nationen während der 76. Generalversammlung der Vereinten Nationen, September 2021 - September 2022 - Schlussfolgerungen des Rates (12. Juli 2021)",: https://www.consilium.europa.eu/media/51240/st10393-en21.pdf (abgerufen am 22. Juli 2022).

197 BRICS, „XIV BRICS Summit Beijing Declaration", (23. Juni 2022): http://www.brics.utoronto.ca/docs/220623-declaration.html (abgerufen am 15. August 2022).

198 G7 Germany, „Erklärung von 2022 über resiliente Demokratien", (27. Juni 2022): https://www.g7germany.de/resource/blob/974430/2057606/66c1e8dc967c2b5bcd0f10bb15411d69/2022-06-27-g7-resiliente-demokratien-data.pdf?download=1 (abgerufen am 15. September 2022).

199 Weißes Haus, „A Declaration for the Future of the Internet," (22. April 2022): https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf (abgerufen am 15. September 2022).

200 Tatsächlich war die DFI nicht in der Lage, die Unterstützung der systemrelevanten demokratischen Technologiemächte des globalen Südens, zu denen Indien, Südafrika, Brasilien, Indonesien, Malaysia und Mexiko gehören, zu gewinnen.

201 Tyson Barker, „Withstanding the Storm: The Digital Silk Road, Covid-19 and Europe's Options", in Alessia Amighini (Hrsg.), „China After COVID-19. Economic Revival and Challenges to the World", Juni 2021, S. 108-138: https://dgap.org/sites/default/files/article_pdfs/ispi-report-2021-china-after-covid.pdf (abgerufen am 22. Juni 2022).

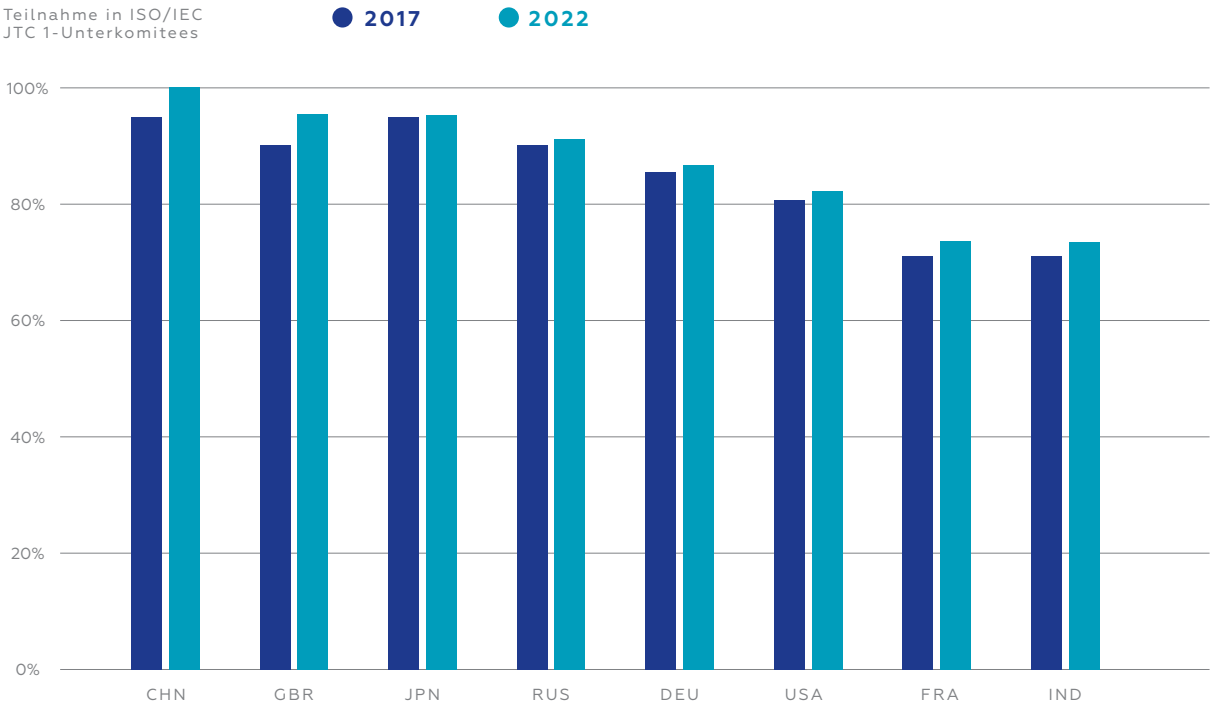
202 Stefan Vladisavljev, „Surveying China's Digital Silk Road in the Western Balkans", War on the Rocks, August 3, 2021: https://warontherocks.com/2021/08/surveying-chinas-digital-silk-road-in-the-western-balkans/ (abgerufen am 22. Juni 2022).

203 Tin Hinane El Kadi, „The Promise and Peril of the Digital Silk Road", Chatham House, 6. Juni 2019: https://www.chathamhouse.org/2019/06/promise-and-peril-digital-silk-road (abgerufen am 22. Juni 2022).

204 Philipp Oltermann, „Germany's ‚China City': how Duisburg became Xi Jinping's gateway to Europe", The Guardian, August 1, 2018: https://www.theguardian.com/cities/2018/aug/01/germanys-china-city-duisburg-became-xi-jinping-gateway-europe (abgerufen am 15. September 2022).

205 G7 Germany, „Kommuniqué der G7 Staats- und Regierungschefs" 28. Juni 2022, S. 15-16: https://www.g7germany.de/resource/blob/974430/2059932/10a1cf2421ccdcdd442648a1e64d7ed8/kommuniqu%C3%A9-g7-arbeitsuebersetzung-data.pdf?download=1, (abgerufen am 28. Juni 2022)

9 – LÄNDERVERTRETUNG BEI DER IKT-STANDARDSETZUNG IM RAHMEN DER ISO/IEC



Quelle: Darstellung der Autoren auf Grundlage von Daten der offiziellen ISO und IEC Websites

wird, die bereits geschätzte 79 Milliarden US-Dollar an entsprechenden Investitionen ausgezahlt hat.[206] Darüber hinaus bleibt abzuwarten, wie die PGII mit der Ende 2021 gestarteten und 300 Milliarden Euro schweren Global Gateway-Initiative der EU zusammenwirkt.[207] Angesichts des schwierigen geopolitischen Kontextes bleibt die Kombination verschiedener nationaler, EU- und G7-Initiativen zu einer kohärenten und wettbewerbsfähigen strategischen Antwort auf Chinas BRI eine zentrale Herausforderung für Deutschland und gleichgesinnte Staaten.

Eine solche infrastrukturbezogene Geopolitik geht auch mit einem relativen Rückgang der Fähigkeit Deutschlands und seiner europäischen Partner einher, globale technische Standards zu definieren. Insbesondere China hat mit großem Erfolg technische Expertinnen und Experten in die wichtigsten internationalen Organisationen für Standardsetzung entsandt. Zwischen 2011 und 2018 hat sich der chinesische Anteil an den Sekretariaten der Technischen Komitees/Unterkomitees und Arbeitsgruppen der Internationalen Organisation für Normung (ISO) fast verdoppelt, beziehungsweise mehr als verdreifacht.[208] Chinesische Vertreterinnen und Vertreter haben im Jahr 2020 erstmals mehr neue technische Führungspositionen in der ISO übernommen als deutsche.[209] Derzeit ist China sogar das einzige Land, das in allen Unterausschüssen des Joint Technical Committee (JTC 1) vertreten ist. Dieses spielt bei der Entwicklung von IKT-Normen im Rahmen der ISO/Internationalen Elektrotechnischen Kommission (IEC), einschließlich

206 Sheridan Prasso, „China's Digital Silk Road Is Looking More Like an Iron Curtain", Bloomberg, 10. Januar 2019: https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain (abgerufen am 15. September 2022).

207 Europäische Kommission, „Global Gateway", (Dezember, 2021): https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/global-gateway_de (abgerufen am 22. Juni 2022).

208 Tim Rühlig, „The Shape of Things to Come. Der Wettlauf um die Kontrolle der technischen Normung", Dezember 2021, S. 24: https://www.europeanchamber.com.cn/en/publications-archive/966/The_Shape_of_Things_to_Come_The_Race_to_Control_Technical_Standardisation (abgerufen am 22. Juni 2022).

209 Ebd., S. 25.

der Bereiche Cloud Computing, Internet der Dinge und KI, eine zentrale Rolle.[210] Chinesische Staatsangehörige haben außerdem zurzeit, beziehungsweise hatten bis vor Kurzem, hochrangige Führungsposition in der ISO[211], der ITU[212] und der IEC[213] inne.

Für Deutschland und Europa birgt der schleichende Wandel vom Vorreiter zum Übernehmer neuer technischer Standards die Gefahr, dass die Industrie erhebliche Anpassungskosten zu tragen hat.[214] Auf Deutschland entfallen zwar in der ISO und IEC[215] immer noch mehr Sekretariate als auf die Vereinigten Staaten, China und andere wichtige Länder, doch das staatszentrierte Standardisierungssystem Chinas hat es Peking ermöglicht, seinen strategischen Einfluss in Bereichen wie KI und 5G auszuweiten.[216] Das stellt auch ein politisches Problem dar. Standards können Werte wie einen hohen Datenschutz (oder dessen Nichtvorhandensein) begünstigen und sogar zu einer Bedrohung der nationalen Sicherheit werden, wenn sie (absichtliche) Cyberschwachstellen beinhalten, die unwissentlich weltweit übernommen werden.[217]

Inmitten dieser Fragmentierung beginnt sich jedoch eine neue institutionelle Architektur für die Governance aufkommender Technologien zu entwickeln. KI ist ein gutes Beispiel hierfür, insbesondere mit Blick auf die von der G7 initiierten Globale Partnerschaft zur Künstlichen Intelligenz (GPAI), den Rat für künstliche Intelligenz der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), den Ad-hoc-Ausschuss für künstliche Intelligenz des Europarates (CAHAI) und die KI-Grundsätze der großen Tech-Unternehmen. Es wird erwartet, dass ähnliche Governance-Ökosysteme, Normen und Standards für Quantentechnologien, die Verwendung von Kryptowährungen, Distributed-Ledger-Technologie (Web3) sowie intelligente und grüne Technologien entwickeln werden. Dies wird Deutschland, der EU und ihren Partnern ein wichtiges diplomatisches Terrain eröffnen.

Aktueller politischer Ansatz

Deutschlands Bekenntnis zum Multilateralismus und zu einer regelbasierten Ordnung prägt seinen Ansatz in der internationalen Technologiepolitik stark. Die Förderung des Multilateralismus und die Unterstützung globaler, offener und sicherer digitaler Konnektivität steht im Mittelpunkt der Außenpolitik der Ampelkoalition.[218]

Im Einklang mit diesem Bekenntnis ist Deutschland ein wichtiger Akteur beim Aufbau einer multilateralen Architektur für die technologische Zusammenarbeit. Dem UN High-level Panel on Digital Cooperation folgend hat Deutschland gemeinsam mit den Vereinigten Arabischen Emiraten Vorschläge für einen Rahmen für die globale digitale Zusammenarbeit unterbreitet, zu dem auch ein reformiertes Internet Governance Forum (IGF) gehört.[219] Deutschland hat

210 Die Daten wurden von den ISO- und IEC-Webseiten erhoben und zusammengestellt.

211 Xinhua, „ISO wählt ersten chinesischen Präsidenten", Xinhua, September 21, 2013: http://www.china.org.cn/world/2013-09/21/content_30091790.htm (abgerufen am 22. Juni 2022).

212 International Telecommunication Union (ITU), „Office of the Secretary-General", 2022: https://www.itu.int/en/osg/Pages/default.aspx (abgerufen am 3. September 2022).

213 International Electronical Commission (IEC), „IEC Leadership", 2022: https://www.iec.ch/leadership (abgerufen am 22. Juni 2022).

214 Zu Anpassungskosten und Machtpolitik bei der Festlegung internationaler Standards siehe Walter Mattli und Tim Büthe, „Setting International Standards: Technological Rationality or Primacy of Power?", World Politics, 56(1) (2011), S. 1-42: https://www.cambridge.org/core/journals/world-politics/article/setting-international-standards-technological-rationality-or-primacy-of-power/950CCFEEFE34691BF6E2584141B0023A (abgerufen am 22. Juni 2022).

215 Tim Rühlig, „The Shape of Things to Come. Der Wettlauf um die Kontrolle der technischen Normung", Dezember 2021, S. 24: https://www.europeanchamber.com.cn/en/publications-archive/966/The_Shape_of_Things_to_Come_The_Race_to_Control_Technical_Standardisation (abgerufen am 22. Juni 2022)

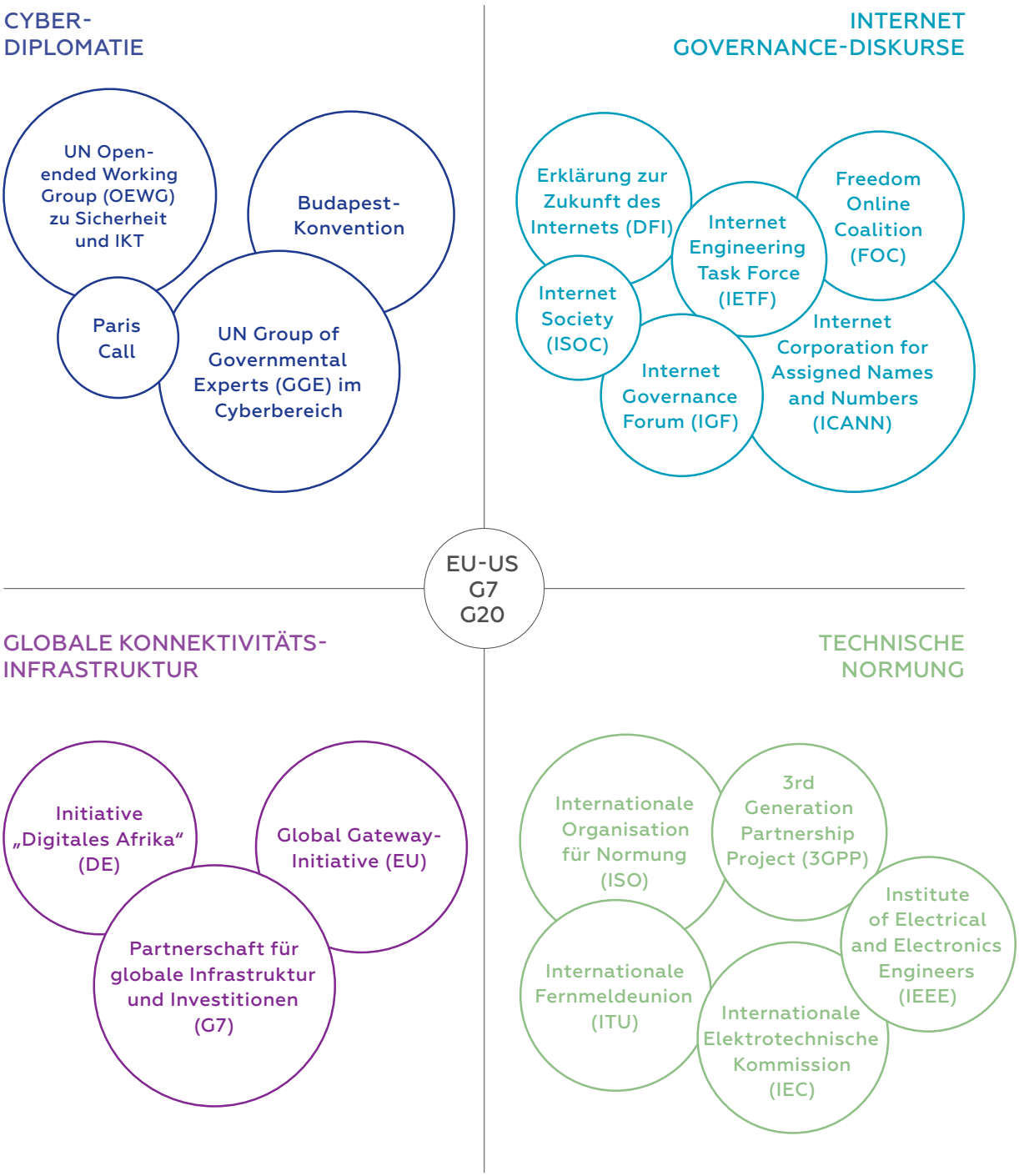
216 Valentina Pop et al., „From Lightbulbs to 5G, China Battles West for Control of Vital Technology Standards", The Wall Street Journal, 8. Februar 2021: https://www.wsj.com/articles/from-lightbulbs-to-5g-china-battles-west-for-control-of-vital-technology-standards-11612722698 (abgerufen am 22. Juni 2022).

217 Tim Rühlig, „The Rise of Tech Standards Foreign Policy", DGAP Online Kommentar, Deutsche Gesellschaft für Auswärtige Politik (Februar 2022): https://dgap.org/en/research/publications/rise-tech-standards-foreign-policy (abgerufen am 22. Juni 2022).

218 Sozialdemokratische Partei Deutschlands (SPD), BÜNDNIS 90/DIE GRÜNEN and Freie Demokratische Partei (FDP), „Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit", (Dezember 2021), S. 114-115: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (abgerufen am 22. Juni 2022).

219 Die Bundesregierung der Bundesrepublik Deutschland und die Regierung der Vereinigten Arabischen Emirate, „Recommendation 5A/B. Options for the Future of Global Digital Cooperation", (September 2020): https://www.global-cooperation.digital/GCD/Redaktion/EN/Downloads/options-for-the-future-of-global-digital-cooperation.pdf?__blob=publicationFile&v=2 (abgerufen am 22. Juni 2022).

10 – ZENTRALE INSTITUTIONEN UND INITIATIVEN FÜR DEUTSCHLANDS INTERNATIONALE TECHNOLOGIEPOLITIK



Quelle: Eigene Darstellung

das IGF im Jahr 2019 ausgerichtet und erwägt dessen neuerliche Ausrichtung im Jahr 2025. Außerdem treibt es auch die Schaffung einer normativen Ordnung im Cyberraum voran. Es unterstützt den Appell von Paris[220] und engagiert sich in der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), der Arbeit des Europarates zu künstlicher Intelligenz (CAHAI) und zu Datenschutz (Konvention 108+) sowie in der OEWG der Vereinten Nationen zu IKT im Kontext der internationalen Sicherheit.

Gleichzeitig gelingt es Deutschland nicht, seine Beteiligung in kleinen und informellen Gruppen optimal zu nutzen, um mit gleichgesinnten Staaten eine zukunftsweisende Technologieagenda zu entwickeln. Die deutsche G20-Präsidentschaft 2017 hat gezeigt, dass Deutschland in der Lage ist, Technologie als zentrales Thema zu verankern, unter anderem durch die Ausrichtung des ersten Treffens der G20 Digitalminister.[221] Der Ansatz der Bundesregierung in Bezug auf digitale Themen bleibt jedoch in erster Linie von wirtschaftlichen Überlegungen geprägt. Während seiner derzeitigen G7-Präsidentschaft hat Deutschland seine Bedenken bezüglich Herausforderungen wie der Fragmentierung des Internets und dem digitalen Autoritarismus verstärkt geäußert.[222] Dennoch hat sich Deutschland bisher dafür entschieden, digitale Fragen nicht zu einer strategischen Priorität zu machen.[223]

Die Bundesregierung nutzt jedoch aktiv ihr umfangreiches diplomatisches und entwicklungspolitisches Netzwerk, um sich mit den Staaten des Globalen Südens über digitale Themen auszutauschen. Vor Kurzem hat Deutschland den regelmäßigen Digitaldialog mit wichtigen Ländern wie Brasilien, Japan und Indien wiederbelebt, um gemeinsame Forschungs- und Entwicklungsprojekte vorzubereiten, Cyber-Themen zu diskutieren und die Arbeit im multilateralen Rahmen zu koordinieren.[224] Solche bilateralen Formate haben sich als nützlich erwiesen, und die Bundesregierung bemüht sich derzeit um ähnliche Dialoge mit Südkorea, Indonesien und Argentinien. Deutschland hat auch die strategische Bedeutung Afrikas im Digitalbereich erkannt. Seit 2015 hat es im Rahmen seiner Initiative „Digitales Afrika" 164 Millionen Euro in digitale Projekte investiert[225] und mehr als 200 öffentlich-private Partnerschaften im afrikanischen Technologiesektor initiiert.[226] Das Bundesministerium für Digitales und Verkehr und das Auswärtige Amt planen außerdem einen institutionalisierten Digitaldialog unter Beteiligung der Privatwirtschaft, der Zivilgesellschaft und subnationaler Regierungen der Afrikanischen Union, Kenias, Südafrikas und Ghanas. Eine verstärkte digitale Zusammenarbeit mit Ägypten wird ebenfalls in Erwägung gezogen.

Mit der wachsenden strategischen Bedeutung digitaler Technologien, hängt Deutschlands Einfluss auf die Gestaltung ihrer globalen Governance zunehmend davon ab, dass Synergien mit den Bemühungen der EU erzielt werden. Deutschlands Technologie-Diplomatie ist in eine Hinwendung zu einer eindeutig (geo-)strategisch geprägten Sichtweise auf Technologiepolitik auf EU-Ebene eingebettet. Der Digitale Kompass 2030 der EU bekräftigt, dass Technologie ein Faktor für „globalen Einfluss" ist,[227] und Brüssel betont, mehr als der deutsche politische Diskurs, die Verbindung zwischen digitaler Souveränität und europäischen Werten.[228]

Die EU hat damit begonnen, diese Verbindung in eine handlungsorientierte Außenpolitik zu überführen. Dazu gehören Formate wie der Handels- und Technologierat (TTC) zwischen der EU und den USA (auf

220 The Paris Call for Trust and Security in Cyberspace, „Home", (2021): https://pariscall.international/en/ (abgerufen am 22. Juni 2022

221 Bundesministerium für Wirtschaft und Klimaschutz (BMWK), „G20 - Digitalisierung global gestalten", (2022): https://www.bmwi.de/Redaktion/EN/Artikel/Digital-World/g20-shaping-digitalisation-at-global-level.html (abgerufen am 22. Juni 2022).

222 G7-Treffen der Digitalminister, „Ministerial Declaration", (Mai 2022): https://www.bundesregierung.de/resource/blob/998440/2038510/e8ce1d2f3b08477eeb2933bf2f14424a/2022-05-11-g7-ministerial-declaration-digital-ministers-meeting-en-data.pdf?download=1 (abgerufen am 22. Juni 2022).

223 Der Abschnitt über die Digitalisierung steht in dem 28-seitigen Kommuniqué des G7-Gipfels an letzter Stelle. G7 Germany, „Kommuniqué der G7 Staats- und Regierungschefs" 28. Juni 2022, S. 15-16: https://www.g7germany.de/resource/blob/974430/2059932/10a1cf2421ccdcdd442648a1e64d7ed8/kommuniqu%C3%A9-g7-arbeitsuebersetzung-data.pdf?download=1, (abgerufen am 28. Juni 2022)

224 Auswärtiges Amt, Deutsch-indische Cyberkonsultationen, 14. Dezember 2017: https://www.auswaertiges-amt.de/de/aussenpolitik/themen/cyber-aussenpolitik/indien-cyberkonsultationen/1890390 (abgerufen am 28. Juni 2022).

225 Kooperation International, „Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung: Start der digitalen Lernplattform „Africa Cloud" angekündigt", (November 2019): https://www.kooperation-international.de/aktuelles/nachrichten/detail/info/bundesministerium-fuer-wirtschaftliche-zusammenarbeit-und-entwicklung-start-der-digitalen-lernplattf/ (abgerufen am 22. Juni 2022).

226 Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, „Strategische Partnerschaft Technologie in Afrika" (2022): https://www.bmz.de/de/mitmachen/wirtschaft/digitales-afrika-13718 (abgerufen am 22. Juni 2022).

227 Europäische Kommission, „Digitaler Kompass 2030: der europäische Weg in die digitale Dekade ", 9. März 2021, S. 21, https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0016.02/DOC_1&format=PDF (abgerufen am 28. Juni 2022).

228 Die Präsidentin der Europäischen Kommission, Ursula von der Leyen, definierte „technologische Souveränität" als „die Fähigkeit, die Europa haben muss, um seine eigenen Entscheidungen zu treffen, basierend auf seinen eigenen Werten und unter Einhaltung seiner eigenen Regeln". Europäische Kommission, „Shaping Europe's digital future: op-ed by Ursula von der Leyen, President of the European Commission", 19. Februar 2020: https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260 (abgerufen am 22. Juni 2022).

dessen Tagung in Paris beispielsweise neue IKT-Sicherheitsleitlinien für vertrauenswürdige Anbieter in Entwicklungsinitiativen auf den Weg gebracht wurden, die die EU-Toolbox für 5G-Cybersicherheit erweitern), der neue TTC mit Indien[229] und die Global Gateway-Initiative.[230] Vor dem Hintergrund der russischen Aggression gegen die Ukraine entwickelt sich insbesondere der europäisch-amerikanische TTC zu einem Instrument für demokratische Koordinierung in Fragen, die von Investitionsüberwachung und Ausfuhrkontrollen bis hin zu resilienten Halbleiterlieferketten reichen.[231] Die EU eröffnet außerdem ein Büro im Silicon Valley, um die transatlantische Koordination zu Digitalthemen zu stärken.[232]

Handlungs-empfehlungen

Deutschlands Erfolg als Gestalter einer globalen Technologieordnung, die seine führende Position als Hightech-Industrienation sichert und demokratische Regierungsformen stützt, wird davon abhängen, wie erfolgreich es seine Werte und Interessen in Allianzen, Partnerschaften und Normen verankert. Hierzu sollte Deutschland:

Die Idee einer demokratischen Vertrauenszone („trust zone") im Bereich der digitalen Technologien vorantreiben. Diese Vertrauenszone würde den Austausch von Wissen, Kapital und Daten regeln, um die Wettbewerbsfähigkeit und die Vertrauenswürdigkeit von strategisch wichtigen IKT-Infrastrukturen wie Netzausrüstung, Cloud-/Edge-Diensten und Smart-City-Technologien zu steigern. Sie sollte auf regulatorischen Best Practices und einem strategischen Ansatz für Industriepolitik aufbauen, der gegenseitige Abhängigkeiten nutzt, um die Zusammenarbeit zu festigen und den Zugang zu kritischen Technologien und Materialien zu sichern. In diesem Sinne sollte die Bundesregierung einen starken institutionellen Kern in Form eines ambitionierten G7-Ministertreffens zum Thema Digitalisierung, einer erweiterten digitalen Agenda der OECD und vertiefter TTC-Treffen zwischen der EU und den USA unterstützen.

Eine globale Konnektivitätsdoktrin mit offenem Internetzugang als Grundrecht einführen. Deutschland sollte mit den EU-Mitgliedern und anderen gleichgesinnten Demokratien zusammenarbeiten, um gemeinsam finanzierte „Konnektivitätspakete" zu entwickeln, die die Entwicklung der digitalen Infrastruktur mit dem Aufbau von Cyber-Kapazitäten und langfristiger Unterstützung lokaler NGOs für digitale Rechte verbinden. Die Zusammenarbeit muss jedoch über die nationalen Regierungen hinausgehen. Deutschland sollte die EU und die NATO, sowie gleichgesinnte Staaten, dazu bewegen, Ressourcen (z. B. Satelliten) bereitzustellen, die den Zugang zum Internet erweitern, die digitale Kluft verringern, den UN-Zielen für nachhaltige Entwicklung in Bezug auf Konnektivität (9.c) dienen sowie offene Informationsflüsse während Internetsperren durch autoritäre Regime und in Konfliktgebieten aufrechterhalten.

Eine deutsche Open Tech-Stiftung gründen. Die Ampelkoalition verweist ausdrücklich auf die digitale Souveränität im Globalen Süden als Priorität, um die freie Wahl von Anbietern, Plattformen und IKT-Infrastruktur zu gewährleisten, Lock-in-Effekte zu vermeiden und ein menschen-, nicht staatszentriertes Konzept der digitalen Selbstbestimmung zu garantieren. Der neu eingerichtete Sovereign Tech Fund bietet die Möglichkeit, Open Source und Open Technology vor allem in Deutschland finanziell zu unterstützen. Er sollte durch eine deutsche Open Tech-Stiftung (German Open Tech Foundation, GOTF) ergänzt werden, um international, insbesondere für Gemeinschaften im Globalen Süden, Mittel für die Entwicklung von Technologien bereitzustellen, welche die Demokratie und Privatsphäre stärken und im Einklang mit dem globalen Verständnis von digitaler Souveränität der Bundesregierung stehen.

Der Politisierung von Standardsetzung im Bereich kritischer und neuer Technologien entgegenwirken. Da der Anteil von Nichtmarktwirtschaftsländern in den Gremien für technische

229 Europäische Kommission, „EU-India: Joint press release on launching the Trade and Technology Council", 25. April 2022: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2643 (abgerufen am 22. Juni 2022).

230 Europäische Kommission, „Global Gateway", Dezember 2021: https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/global-gateway_de (abgerufen am 22. Juni 2022).

231 Europäische Kommission, „EU-US Trade and Technology Council Inaugural Joint Statement", 29. September 2021: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951 (abgerufen am 22. Juni 2022).

232 Euractiv, „Neues EU-Büro im Silicon Valley für Big-Tech-Diplomatie", (28 Juli 2022): https://www.euractiv.de/section/innovation/news/neues-eu-buero-im-silicon-valley-fuer-big-tech-diplomatie/ (abgerufen am 15. August 2022).

Standardisierung zunimmt, sollte Deutschland eine internationale Studiengruppe initiieren, die ermittelt, ob und welche politischen Instrumente eingesetzt werden, um die Standardsetzung im Bereich kritischer und neu entstehender Technologien zu beeinflussen. Dies sollte die Grundlage für ein koordiniertes Engagement mit den internationalen Standardsetzungs-Gremien bilden, um den Vorrang technischer Kriterien zu gewährleisten und ihren Ruf als unparteiische Institutionen zu wahren. Die Bundesregierung sollte auch qualitativ hochwertige Beiträge fördern, indem sie zum Beispiel die Beteiligung des akademischen Sektors sowie kleiner und mittelständischer Unternehmen (KMU) an der Ausarbeitung technischer Standards ermöglicht, etwa in dem sie diese als förderbare Forschungs- und Entwicklungsarbeit berücksichtigt.

Das Entstehen einer digitalen „Bewegung der Blockfreien Staaten" verhindern. Eine globale demokratische Technologieordnung muss über die transatlantische Gemeinschaft hinausreichen. Besorgniserregend ist, dass die Staaten der G77+ angesichts der zunehmenden geopolitischen Bedeutung von Technologie ein klares Bekenntnis zu einer gemeinsamen demokratischen Technologieagenda scheuen. Indien ist in dieser Hinsicht ein zentraler, aber komplexer Partner. Deutschland hat seinen Digitaldialog mit Indien bereits wiederaufgenommen und das Land zum diesjährigen G7-Gipfel eingeladen. Mit Blick auf die G20-Präsidentschaft Indiens im Jahr 2023 sollte Deutschland nun darauf aufbauen und Indiens demokratische Verantwortung betonen, eine integrative digitale Agenda zu fördern, in deren Mittelpunkt klimafreundliche Technologien sowie offene und freie Konnektivität stehen.

Kooperatives Engagement im EU-US-Technologiedialog zeigen, insbesondere im TTC. Deutschland sollte einen bilateralen Digitaldialog mit den Vereinigten Staaten institutionalisieren, der die politischen Ergebnisse des TTC aufnehmen und verstärken kann.[233] Deutschland sollte sich aber auch in anderen Bereichen engagieren, etwa bei einem konstruktiven Abschluss des post-Privacy Shield Transatlantic Data Privacy Framework und dessen Implementierung. Das Deutsch-Amerikanische Zukunftsforum, das im Rahmen der Erklärung von Washington[234] vom Juli 2021 ins Leben gerufen wurde und dessen erstes Treffen im November 2022 stattfinden wird, könnte ein weiteres Instrument zur Vertiefung des Engagements sein, insbesondere im Hinblick auf demokratiefördernde Technologien und Normen.

Asymmetrische Technologieallianzen mit subnationalen Verwaltungseinheiten bilden. Städte und Bundesstaaten übernehmen zunehmend Aufgaben der digitalen Governance, die nationale Regierungen nicht übernehmen wollen oder können. In den Vereinigten Staaten haben Städte und Bundesstaaten beim Datenschutz eine Vorreiterrolle übernommen; teilweise indem sie Richtlinien für KI-gestützte Gesichtserkennungstechnologien und gegen algorithmische Diskriminierung in sensiblen Bereichen, wie bei der Einstellung von Personal, aufgestellt haben. In China, Brasilien und Indien wird die technologische Industrie- und Regulierungspolitik ebenfalls durch subnationale Regierungen vorangetrieben. Im Einklang mit den neuen Schlussfolgerungen des Europäischen Rates zur digitalen Diplomatie sollte Deutschland mit Entscheidungsträgerinnen und -trägern auf dieser Ebene zusammenarbeiten, um Technologieallianzen zu bilden, die die deutschen und EU-Werte im Bereich der Regulierung widerspiegeln und die subnationale Übernahme von Normen für die Internet und Cyber-Governance unterstützen.

233 Tyson Barker, "The Hidden G2 for Democratic Tech Governance is the EU-US Relationship," (Juni 2022): https://dgap.org/sites/default/files/article_pdfs/dgap_analysis_no._2_june_10_2021_18_pp_0.pdf (abgerufen am 15. August 2022).

234 The Federal Government, "A German-American partnership for the future," (16. Juli 2021): https://www.bundesregierung.de/breg-en/news/federal-chancellor-usa-trip-1942938 (abgerufen am 15 August 2022).

KAPITEL 7

Ethisch und einsatzfähig

Aufkommende und disruptive Technologien, die Bundeswehr und die Zeitenwende

KAPITELÜBERSICHT

Zentrale Erkenntnisse

1 Deutschlands künftiger Beitrag zur Sicherheit Europas und seiner Verbündeten hängt davon ab, ob die Bundeswehr aufkommende und disruptive Technologien (Emerging and Disruptive Technologies, EDTs) wie künstliche Intelligenz, 5G/6G-Mobilfunktechnologie, Low Earth Orbit (LEO) Satelliten-Konnektivität sowie Quantencomputing und -kommunikation effektiv nutzen kann.

2 Selbst inmitten des russischen Angriffskriegs gegen die Ukraine bleibt Deutschland einem konzeptionellen, institutionellen und ethischen Silodenken verhaftet, das zu Entkopplungen zwischen dem Verteidigungs- und Technologiesektor ebenso wie zu Diskrepanzen mit seinen Verbündeten führt.

3 Damit Deutschland nicht nur die unmittelbaren militärischen Anforderungen erfüllen kann, sondern die Bundeswehr auch für zukünftige Einsätze gewappnet ist, sollte die Zeitenwende nicht nur eine Erhöhung des Verteidigungshaushalts bewirken, sondern auch die Basis für eine Vereinbarkeit von ethischen und militärischen Anforderungen an EDTs schaffen.

Einleitung

Der russische Angriffskrieg gegen die Ukraine hat Deutschland aufgerüttelt und dazu veranlasst, seine Verteidigungspolitik drastisch anzupassen. Nach jahrzehntelangem Stillstand füllt die Bundeswehr nun Lücken bei grundlegenden militärischen Fähigkeiten. Zudem setzt sich in der deutschen Politik zunehmend die Erkenntnis durch, dass eine stärkere Integration intelligenter Systeme, die organisatorische Ausrichtung an Hightech-Kriegsführung und die Verschmelzung von Cyber- und physischem Raum für die künftige Leistungsfähigkeit des deutschen Militärs von entscheidender Bedeutung sind.

Dennoch verharrt der deutsche politische Diskurs noch in einem konzeptionellen, institutionellen und ethischen Silodenken, das wenig Innovation zulässt und zu Entkopplungen zwischen dem Verteidigungs- und Technologiesektor ebenso wie zu Diskrepanzen zwischen Deutschland und seinen Verbündeten führt. Für die Modernisierung der deutschen Streitkräfte ist es von zentraler Bedeutung, dass ethische Bedenken mit (zukünftigen) Einsatzrealitäten abgeglichen werden und politische Entscheidungen der engen Verknüpfung zwischen Entwicklung und Nutzung militärischer und ziviler Technologien Rechnung tragen.

Status quo

Aufkommende und disruptive Technologien (Emerging and Disruptive Technologies, EDTs) wie künstliche Intelligenz, 5G/6G-Mobilfunktechnologie, Low Earth Orbit (LEO) Satelliten-Konnektivität sowie Quantencomputing und -kommunikation werden das Umfeld für Bundeswehr-Operationen nachhaltig verändern. Die Bundeswehr sieht die stärkere Integration von maschineller Intelligenz in militärische Operationen, insbesondere durch den massenhaften Einsatz unbemannter Systeme, als eine der zentralen Herausforderungen in diesem Jahrzehnt an.[235] Hochautomatisierte unbemannte Luftfahrtsysteme (Unmanned Aerial System, UAS) spielten in den jüngsten Konflikten wie dem Krieg um Bergkarabach eine wichtige Rolle.[236] Auch im Bereich der strategischen Planung und Vorausschau werden EDTs unverzichtbar, wo etwa KI-Algorithmen Erkenntnisse aus den von immer mehr Sensoren erzeugten Datenmengen gewinnen. Das Weltraumkommando der Bundeswehr setzt zum Beispiel bereits zwei Machine-Learning-Anwendungen bei der Erstellung von Lagebildern ein.[237]

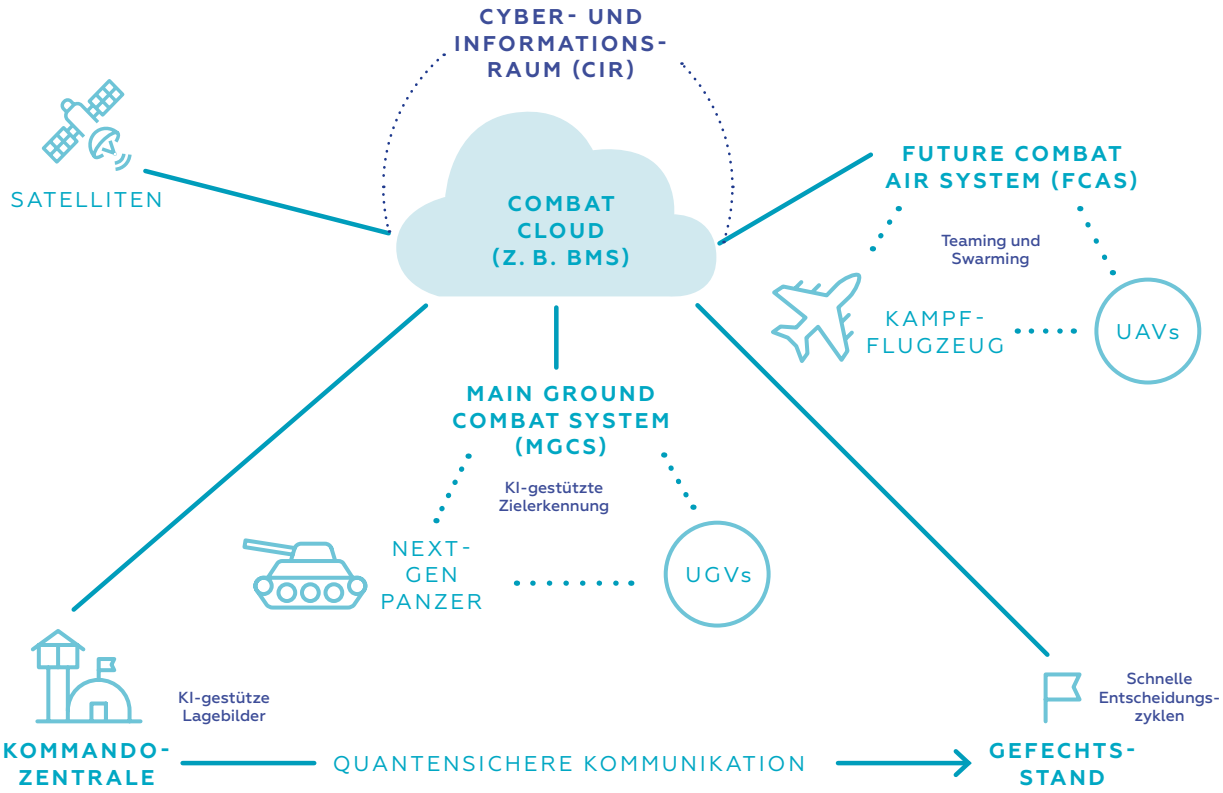
In diesem sich wandelnden Umfeld hängt die Fähigkeit der Bundeswehr, die Möglichkeiten von EDTs bei künftigen Einsätzen auszuschöpfen, entscheidend von der engen Kooperation mit Verbündeten Deutschlands in der EU und der NATO ab, und damit auch von

235 Kommando Heer, „Thesenpapier I: Wie kämpfen Landstreitkräfte künftig?“, Kommando Heer (2017) https://augengeradeaus.net/wp-content/uploads/2018/03/180327-Thesenpapier-I-Wie-ka%CC%88mpfen-LaSK-zuku%CC%88nftig.pdf (abgerufen am 18. Juli 2022).

236 Deutscher Bundestag, Zum Drohneneinsatz im Krieg um Bergkarabach im Jahre 2020, WD2-3000-113/20 (Januar 2021): https://www.bundestag.de/resource/blob/825428/5b868defc837911f17628d716e7e1e1d/WD-2-113-20-pdf-data.pdf (abgerufen am 31. Mai 2022).

237 BWI, „Künstliche Intelligenz: BWI entwickelt Lösungen für die Bundeswehr“ 24. Januar 2022: https://www.bwi.de/news-blog/blog/artikel/kuenstliche-intelligenz-bwi-entwickelt-loesungen-fuer-die-bundeswehr (abgerufen am 31. Mai 2022).

11 – WIE AUFKOMMENDE UND DISRUPTIVE TECHNOLOGIEN DIE KRIEGSFÜHRUNG VON MORGEN VERÄNDERN



Quelle: Darstellung der Autoren

der fortlaufenden Investition von politischem Kapital in gemeinsame Initiativen. Deutschlands derzeitige Bemühungen, EDTs zu nutzen, sind eng verbunden mit gemeinsamen europäischen Verteidigungsprojekten für zukünftige Kampfsysteme, darunter das Future Combat Air System (FCAS)[238] mit Frankreich und Spanien und das Main Ground Combat System (MGCS)[239] mit Frankreich. Beide Systeme werden voraussichtlich erst in den 2040er Jahren einsatzbereit sein, der Bundeswehr aber erweiterte Funktionen zur Verfügung stellen, zum Beispiel die tiefgreifende Integration in eine gemeinsame Combat Cloud und intelligente Mensch-Maschine-Kooperation.[240]

Das deutsche Verteidigungswesen sieht sich mit der Herausforderung konfrontiert, sich organisatorisch auf die High-Tech-Kriegsführung vorzubereiten. Konflikte werden zunehmend in Maschinengeschwindigkeit ausgetragen, was eine schnellere Entscheidungsfindung an der Front erfordert. Dies bedarf dezentraler Kommandostrukturen mit hochvernetzten Einheiten in der Bundeswehr. Die Bundeswehr führt auch deshalb ein Battle Management System (BMS) ein – ein neues digitales Führungssystem, das den Zugriff auf Echtzeitinformationen und somit eine digital vernetzte Kampfführung ermöglicht.[241] Sie möchte das BMS bis

238 Airbus, „Future Combat Air System (FCAS)": https://www.airbus.com/en/products-services/defence/multi-domain-superiority/future-combat-air-system-fcas (abgerufen am 31. Mai 2022) .

239 Hensoldt, „MGCS – The Smart Tank is Rolling in" (April 2021): https://www.hensoldt.net/stories/mgcs/ (abgerufen am 31. Mai, 2022).

240 „FCAS-Anforderungen festgelegt", FlugRevue, 31. August 2021: https://www.flugrevue.de/militaer/industrie-muss-sich-einigen-fcas-anforderungen-festgelegt/ (abgerufen am 31. Mai 2022); André Uzulis, „MGCS – Ein neues Kampfsystem für das Heer", *.loyal das Magazin*, (1. April 1, 2021): https://www.reservistenverband.de/magazin-loyal/mgcs-ein-neues-kampfsystem-fuer-das-heer/ (abgerufen am 31. Mai 2022).

241 Das BMS basiert auf der SitaWare-Softwarefamilie, die von vielen NATO-Partnern verwendet wird. Bundeswehr, „Battle Management System – CIR digitalisiert": https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/auftrag/digitalisieren/gefechtsfuehrung-der-zukunft-das-battle-management-system (abgerufen am 31. Mai 2022).

2023 einsatzbereit machen, sobald sie Führungsverantwortung in der Very High Readiness Joint Task Force der NATO übernimmt.[242]

Die Bundesregierung hat außerdem wichtige Schritte unternommen, um sich auf die Verschmelzung von Cyber- und physischem Raum vorzubereiten, die mit aktuellen verteidigungstechnologischen Entwicklungen einhergeht. So hat Deutschland beispielsweise sein Netzwerk an Cyber-Institutionen erheblich ausgebaut und eine hohe Position in Ranglisten nationaler Cyber-Fähigkeiten errungen.[243] Mit der zunehmenden Nutzung digitaler Technologien in Systemen und Kommandostrukturen hat die Bundeswehr ihre Ressourcen in einem eigenen militärischen Organisationsbereich, dem Cyber- und Informationsraum (CIR), gebündelt.[244] Zudem baut das Bundesministerium der Verteidigung seine Fähigkeiten im Bereich sicherer Quantenkommunikationsnetze aus, unter anderem durch ein spezielles Labor in seinem Forschungsinstitut für Cybersicherheit, CODE.[245] Dieses Labor entwickelt MuQuaNet, einen Prototypen eines solchen Netzes.[246]

Gerade weil die Bundeswehr mit einer potenziellen militärischen Eskalation im Cyberraum umgehen muss, gewinnen auch ethische Bedenken an Relevanz. KI kann beispielsweise zur Automatisierung von Cyberaktivitäten eingesetzt werden, was einen größeren Umfang und eine höhere Häufigkeit von Cyberangriffen ermöglicht.[247] Außerdem könnte sie die Risikobereitschaft steigern, da Abwehrtechniken möglicherweise langsamer entwickelt und skaliert werden können als offensive Techniken.[248] Gleichzeitig ist die Zuordnung von Cyberangriffen kompliziert und zeitaufwändig.[249] Die Bundeswehr könnte sich beispielsweise gezwungen sehen, auf der Grundlage von uneindeutigen Informationen über Verantwortung oder Absicht (wie z. B. Spionage vs. Sabotage) gegen einen vermeintlichen böswilligen (staatlichen oder nichtstaatlichen) Akteur vorzugehen.[250] Während KI und andere EDTs die Risiken im Cyberraum erhöhen, befindet sich Deutschland noch im Prozess zur Entwicklung einer kohärenten und angemessene Antwort auf diese Herausforderungen.

Die Zusammenarbeit zwischen dem Verteidigungs- und Technologiesektor sowie die organisationale Anpassung der Bundeswehr stellen nach wie vor große Herausforderungen dar. Die erheblichen ethischen Bedenken der deutschen Gesellschaft hinsichtlich der Reduzierung menschlicher Beteiligung und Verantwortung durch die Nutzung von EDTs erschwert dies ebenfalls. Die Bundeswehr ist sich dieser Bedenken bewusst und versucht, sie mit realen Bedingungen auf dem Kampffeld, Kommandostrukturen und Entscheidungsprozessen in Einklang zu bringen. Ein Beispiel hierfür ist die explizite Abbildung ethisch-rechtlicher Implikationen in der KI-gestützten Simulationsumgebung „GhostPlay".[251] Gleichzeitig kann die Abweichung Deutschlands von der robusteren und pragmatischeren Herangehensweise seiner Bündnispartner an Dual-Use EDTs, also EDTs mit doppeltem Verwendungszweck, die gemeinsame Planung – und insbesondere die Bestimmung der technischen Merkmale – von gemeinsamen Verteidigungsprojekten wie FCAS, die die Nutzung fortschrittlicher maschineller Intelligenz beinhalten, erschweren.

242 Bundeswehr, "Digitalisierung im Heer": https://www.bundeswehr.de/de/organisation/heer/organisation/faehigkeiten/digitalisierung (abgerufen am 31. Mai 2022).

243 Z. B. Julia Voo, „National Cyber Power Index 2020. Methodology and Analytical Considerations", China Cyber Policy Initiative/Belfer Center for Science and International Affairs (September 2020): https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf (abgerufen am 31. Mai 2022); Internationale Fernmeldeunion (ITU), „Global Cybersecurity Index 2020," (2022): https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (abgerufen am 31. Mai 2022).

244 Bundeswehr Cyber- und Informationsraum: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum (abgerufen am 31. Mai 2022).

245 Universität der Bundeswehr München, „CODE – Über Uns": https://www.unibw.de/code/im-profil/ziele (abgerufen am 28. Juni 2022).

246 Universität der Bundeswehr München, „Q-Lab": https://www.unibw.de/code/forschung/zentrallabore/q-lab (abgerufen am 31. Mai 2022).

247 James Johnson, Eleanor Krabill, „AI, Cyberspace, and Nuclear Weapons", *War on the Rocks*, 31. Januar 2020: https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons/ (abgerufen am 31. Mai 2022)

248 Garfinkel and Allan Dafoe, „Artificial Intelligence, Foresight, and the Offense-Defense Balance", *War on the Rocks*, 19. Dezember 2019: https://warontherocks.com/2019/12/artificial-intelligence-foresight-and-the-offense-defense-balance/ (abgerufen am 31. Mai 2022).

249 Deutscher Bundestag, „Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung, WD2-3000-038/15, (Februar 2015), S. 12–13: https://www.bundestag.de/resource/blob/406028/de1946480e133cf38bbee41d8d3d6898/WD-2-038-15-pdf-data.pdf (abgerufen am 31. Mai 2022).

250 James M. Action, „Cyber Warfare & Inadvertent Escalation", *Daedalus* Nr. 149, Ausgabe 2 (April 2020), S. 133–149: https://direct.mit.edu/daed/article/149/2/133/27317/Cyber-Warfare-amp-Inadvertent-Escalation (abgerufen am 31. Mai 2022); Diese Ambivalenz ist vor allem dann problematisch, wenn verschiedene militärische Fähigkeiten in cyber-physischen Systemen verwoben sind. Die Entdeckung von Malware in Raketenfrühwarnsystemen könnte beispielsweise als Vorbereitung für einen nuklearen Erstangriff interpretiert werden, auch wenn mit der gegnerischen Intrusion eine Schwächung der konventionellen ballistischen Raketenabwehr beabsichtigt ist. James M. Acton, „Why is Nuclear Entanglement So Dangerous?" Carnegie Endowment for International Peace (23. Januar 2019): https://carnegieendowment.org/2019/01/23/why-is-nuclear-entanglement-so-dangerous-pub-78136 (abgerufen am 31. Mai 2022).

251 Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw), „GhostPlay – Simulation für KI-basierte Entscheidungsverfahren": https://dtecbw.de/home/forschung/hsu/projekt-ghostplay (abgerufen am 31. Mai 2022).

Aktueller politischer Ansatz

Mit der Ankündigung einer sicherheits- und verteidigungspolitischen Zeitenwende durch den Bundeskanzler im Februar 2022[252] soll der jahrelange Sparkurs des deutschen Militärs umgekehrt werden. Doch das zugewiesene Sondervermögen in Höhe von 100 Milliarden Euro deckt kaum den Grundbedarf der Bundeswehr. Deutschland ist auf einen weitaus systematischeren haushaltspolitischen – und ethisch-kulturellen – Wandel angewiesen, wenn es über diesen Grundbedarf hinausgehen und sich auf zukünftige Anforderungen einstellen möchte. Zunächst muss die Bundesregierung eine einheitliche Vision für den Einsatz von EDTs in der Bundeswehr entwickeln.

Im 20. Jahrhundert wurden die Kernkraft und die Tarnkappentechnik, ja sogar das Internet, für militärische Zwecke entwickelt. Zivile Nutzungsmöglichkeiten folgten dem. Inzwischen hat sich dieser Trend umgekehrt: Zivile Technologien entwickeln sich zu einer zentralen Dimension militärischer Leistungsfähigkeit. Das Weißbuch (2016) zur Sicherheitspolitik und Zukunft der Bundeswehr[253] und das jüngste Positionspapier (2021) zur Zukunft der Bundeswehr[254] gehen jedoch kaum auf das disruptive Potenzial von Technologien ein, die in erster Linie von zivilen Innovationen angetrieben werden, darunter KI, Quantencomputing und 5G/6G-Konnektivität.[255]

Zudem zeigen Deutschlands wichtigste technologiepolitischen Papiere, dass die Bundesregierung selbst bei Technologien mit eindeutigem Dual-Use-Potenzial weiterhin eine künstliche Trennung zwischen ziviler und militärischer Sphäre beibehält, sowohl hinsichtlich Entwicklung als auch Regulierung. Die deutsche Hightech-Strategie 2025 (2018)[256] und die Industriestrategie 2030 (2019)[257] befassen sich mit volkswirtschaftlichen Dimensionen, verteidigungspolitische Aspekte kommen in der Hightech-Strategie jedoch überhaupt nicht und in der Industriestrategie nur am Rande vor. Das trifft auch auf die deutsche KI-Strategie (2017, 2020)[258] und 5G-Strategie (2017) zu.[259] In der deutschen Cyberstrategie (2021)[260] wird die Cybersicherheit in erster Linie aus der zivilen Perspektive der Strafverfolgung und der Justiz betrachtet.[261]

Die isolierte Betrachtung dieser Technologien im militärischen Kontext spiegelt die Dynamik schwieriger ethischer Debatten in Deutschland wider. Die politische Haltung des Landes zu militärischen Technologien war bislang überwiegend reaktiv, risikoscheu und von gesellschaftlichen Kontroversen geprägt. Mit der Entscheidung für die Bewaffnung der Heron-Drohne im April 2022[262] beendete die Bundesregierung eine fast zehnjährige Diskussion,[263] in der Begriffe wie unbemannte und autonome Systeme häufig fälschlicherweise als Substitute verwendet

252 Die Bundesregierung, „Regierungserklärung von Bundeskanzler Scholz am 27. Februar 2022“: https://www.bundesregierung.de/breg-de/suche/regierungserklaerung-von-bundeskanzler-olaf-scholz-am-27-februar-2022-2008356 (abgerufen am 31. Mai 2022).

253 Die Bundesregierung, „Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr“, (13. Juli 2016): https://www.bundeswehr.de/resource/blob/4800140/fe103a80d8576b2cd7a135a5a8a86dde/download-white-paper-2016-data.pdf (abgerufen am 31. Mai 2022).

254 Bundesministerium der Verteidigung, „Positionspapier – Gedanken zur Bundeswehr der Zukunft (9. Februar 2021): https://augengeradeaus.net/wp-content/uploads/2021/02/20210209_AKK_GI_Bundeswehr_der_Zukunft.pdf (abgerufen am 31. Mai 2022).

255 Dies spiegelt sich auch darin wider, dass in dem 143-seitigen Weißbuch fast keine direkten Verweise auf EDTs mit doppeltem Verwendungszweck enthalten sind (künstliche Intelligenz: 1 Verweis; 5G oder 6G: 0 Verweise; Quantentechnologie: 0 Verweise).

256 Verweise auf Sicherheitsherausforderungen beschränken sich auf die zivile (IT-)Sicherheit. Bundesregierung, „Forschung und Innovation für die Menschen: Die High-Tech Strategie 2025“, (September 2018): https://www.hightech-strategie.de/SharedDocs/Publikationen/de/hightech/pdf/forschung-und-innovation-fuer-die-menschen.pdf?__blob=publicationFile&v=4 (abgerufen am 19. Juni 2022).

257 Bundesministerium für Wirtschaft und Energie (BMWi), „Made in Germany: Die Industriestrategie 2030“ (November 2019): https://www.bmwi.de/Redaktion/DE/Dossier/industriestrategie-2030.html (abgerufen am 31. Mai 2022).

258 Die Bundesregierung, „Nationale Strategie für Künstliche Intelligenz“: https://www.ki-strategie-deutschland.de/home.html (abgerufen am 31. Mai 2022).

259 Bundesregierung, „5G-Strategie für Deutschland“ (Juli 2017): https://www.bmvi.de/blaetterkatalog/catalogs/350336/pdf/complete.pdf (abgerufen am 31. Mai 2022).

260 Bundesministerium des Innern und für Heimat, „Cybersicherheitsstrategie für Deutschland 2021“, (August 2021): https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=1ABEA4EB553C692E35A59577B182FCC4.2_cid287?__blob=publicationFile&v=1 (abgerufen am 31. Mai 2022).

261 Themen wie Desinformationskampagnen und Cyberkriminalität stehen im Vordergrund.

262 Bundesministerium der Verteidigung, „Weg frei zur Bewaffnung der Drohne Heron TP mit Präzisionsmunition“, (6. April 2022): https://www.bmvg.de/de/aktuelles/bewaffnung-der-heron-tp-drohnen-mit-praezisionsmunition-5389376 (abgerufen am 31. Mai 2022).

263 Nina Werkhäuser, „No armed drones for the German army — for now“, Deutsche Welle, 4. Dezember 2020: https://www.dw.com/en/no-armed-drones-for-the-german-army-for-now/a-55936615 (abgerufen am 31. Mai 2022).

12 – DIE TRENNUNG ZIVILER UND MILITÄRISCHER SPHÄREN IN DEUTSCHLANDS WACHSENDEM ÖKOSYSTEM VON INNOVATIONS-INSTITUTIONEN

INSTITUTION	GRÜNDUNG	FÖRDERUNG	BEREICH	PRIORITÄTEN
INNOVATIONS-INSTITUTIONEN IM SICHERHEITS- UND VERTEIDIGUNGSBEREICH				
Cyber Innovation Hub (CyberHub)	2017	€ 200 Mio. 2019–2023	Verteidigung (BMVg)	Förderung Soldatinnen- und Soldaten-zentrierter digitaler Innovationen, einschließlich KI- und Virtual Reality-Anwendungen; Funktion als Schnittstelle zwischen der Bundes-wehr und dem Start-up-Ökosystem
Agentur für Innovation in der Cybersicherheit (Cyberagentur)	2020	€ 350 Mio. 2020–2023	Sicherheit/ Verteidigung (BMVg und BMI)	Unterstützung ehrgeiziger und innovativer FuE auf dem Gebiet der Cybersicherheit, auch in angrenzenden Bereichen wie Mensch-Technik-Interaktion und KI
Zentrum für Digitalisierungs- & Technologieforschung der Bundeswehr (dtec.bw)	2020	€ 500 Mio. 2020–2024	Verteidigung (BMVg)	Bündelung von Forschung der Bundeswehr zu kritischen und neuen Technologien; Förderung der Forschungskooperation mit Wirt-schaft, Verwaltung und Gesellschaft
INNOVATIONS-INSTITUTIONEN IM ZIVILEN BEREICH				
Bundesagentur für Sprunginnovation (SPRIND)	2019	≈€ 1 Mrd. 2019–2029	Zivil (BMBF und BMWK)	Unterstützung disruptiver Innovationen, u.a. in den Bereichen optische Prozessoren, Mikrooptik und Augmented Reality
Deutsche Agentur für Transfer und Innovation (DATI)	2022 (geplant)	€ 15 Mio. Startfinan-zierung	Zivil (BMBF)	Förderung technischer Innovationen, insbesondere an Fachhochschulen; Verstärkung der Zusammenarbeit mit Start-ups, KMUs sowie öffentlichen Einrichtungen
Sovereign Tech Fund (STF)	2022 (geplant)	€ 3,5 Mio. jährlich	Zivil (BMWK, Open Knowledge Foundation)	Unterstützung des Open-Source-Software-Ökosystems; Erhöhung der Sicherheit von grundlegenden Inter-nettechnologien; Verbesserung von Interoperabilität und Stärkung der digitalen Souveränität

Quelle: Eigene Darstellung

wurden.[264] Gleichzeitig schließt Deutschland den Einsatz von vollautonomen Drohnen weiterhin aus und gehört zu den entschiedensten Befürwortern eines völkerrechtlichen Verbots solcher Systeme.[265]

Die jüngsten Bemühungen, die Wettbewerbsfähigkeit in der Verteidigungstechnologie zu stärken, bedeuten einen Bruch mit der üblichen Praxis, künstliche Grenzen zwischen militärischer und ziviler Sphäre zu ziehen. Das Strategiepapier der Bundesregierung aus dem Jahr 2020 zur Stärkung der Sicherheits- und Verteidigungsindustrie[266] verdeutlicht die zunehmende Bedeutung von ziviler Forschung und Entwicklung (FuE) als treibende Kraft für militärische EDT-Anwendungen.[267] Deutschland hat in den vergangenen fünf Jahren auch beträchtliche Summen in neue Institutionen investiert, deren Aufgabe es ist, Forschung und Innovation im Verteidigungsbereich zu fördern (siehe Tabelle).

Dennoch ist die Kluft zwischen ziviler und militärischer FuE in Deutschland nach wie vor größer als in verbündeten Staaten wie Frankreich, dem Vereinigten Königreich und den USA. Obwohl die US-amerikanische Defense Advanced Research Projects Agency im deutschen politischen Diskurs häufig erwähnt wird, hält die deutsche Regierung an einer klaren Trennung zwischen ihren eigenen neuen Innovationsinstitutionen im Sicherheits- und Verteidigungsbereich und der zivilen Innovationsagentur SPRIND fest.[268] Außerdem ist es vielsagend, dass die Unterstützung des Bundesministeriums für Verteidigung für Hochschulforschung bei derzeit rund 50 Millionen Euro jährlich stagniert.[269]

Schwierigkeit, seine umfangreichen FuE-Tätigkeiten zu EDTs für das Verteidigungswesen zu nutzen, untergräbt seine Bemühungen, zu einem zukunftsfähigen europäischen Verteidigungssektor beizutragen. Die Debatte über die militärische Nutzung von EDTs auf EU-Ebene ist zukunftsorientiert, aber es besteht dennoch weiterhin eine Umsetzungslücke. Der von der deutschen EU-Ratspräsidentschaft 2020 initiierte Strategische Kompass der EU (2022)[270] unterstreicht die zentrale Bedeutung einer starken gemeinsamen technologisch-industriellen Basis Europas. Die industrielle Fragmentierung entlang nationaler Grenzen behindert jedoch weiterhin die stärkere Skalierung von Verteidigungstechnologie und damit verbundene Vorteile.

Auch gelingt es den EU-Mitgliedstaaten nicht, ausreichende Ressourcen zu mobilisieren. Der „Koordinierte Jahresbericht zur Verteidigung“ (CARD, Coordinated Annual Review on Defence) der EU aus dem Jahr 2020 warnt davor, dass der Verteidigungstechnologie unzureichende Mittel zugewiesen werden.[271] Initiativen wie der Europäische Verteidigungsfonds (European Defence Fund, EDF), die disruptive Technologien fördern, sind wichtige Schritte zur Stärkung verteidigungsbezogener Forschung.[272] Der ursprünglich für den Zeitraum 2021 bis 2027 vorgesehene EDF-Haushalt in Höhe von 13 Milliarden Euro wurde jedoch um fast die Hälfte auf 8 Milliarden Euro gekürzt.[273] Zudem halten sich lediglich zwei EU-Mitgliedstaaten an die Vereinbarung, zwei Prozent ihres Verteidigungshaushalts in Forschung und Technologie zu investieren.[274]

Angesichts dieser Einschränkungen bleibt die Koordinierung der EU mit der umfangreichen Arbeit der NATO im Bereich der EDTs ein zentraler Bestandteil der deutschen Politik. Im Mittelpunkt des Strategischen Konzepts 2030 der NATO stehen EDTs

264 Während autonome Systeme in der Lage sind, bis zu einem gewissen Grad unabhängig von menschlichen Bedienenden zu agieren, bezieht sich der Begriff „unbemannte Systeme“ lediglich auf die fehlende physische Präsenz menschlicher Bedienenden (z. B. Fernsteuerung).

265 Bundesregierung „Rede der Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, in der Aktuellen Stunde zum Beschaffungsprogramm von Drohnen für die Bundeswehr vor dem Deutschen Bundestag am 2. Juli 2014 in Berlin“, (2. Juli 2014): https://www.bundesregierung.de/breg-de/service/bulletin/rede-der-bundesministerin-der-verteidigung-dr-ursula-von-der-leyen--793046 (abgerufen am 31. Mai 2022).

266 Bundesregierung, „Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie“ (Februar 2020): https://www.bmwk.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-und-verteidigungsindustrie.pdf?__blob=publicationFile&v=4 (abgerufen am 31. Mai 2022).

267 Das Strategiepapier hebt die strategische Bedeutung von Sicherheit und Verteidigung in der allgemeinen Technologie- und Industriepolitik hervor und bezeichnet den Transfer von (grundlegenden) Forschungs- und Entwicklungsergebnissen in beschaffungsfähige Sicherheits- und Verteidigungsprodukte und -dienstleistungen als eine zentrale Herausforderung.

268 SPRIND, „Lernen Sie SPRIND kennen“: https://www.sprind.org/en/we/ (abgerufen am 31. Mai 2022).

269 Die Finanzierung belief sich 2017 auf 42 Mio. Euro, 2018 auf 63 Mio. Euro und 2019 auf 53 Mio. Euro. Armin Himmelrath, „Unis erhalten weniger Geld vom Verteidigungsministerium“, *Spiegel Online*, 15. Juni 2021: https://www.spiegel.de/panorama/bildung/ruestungsforschung-unis-erhalten-weniger-geld-vom-verteidigungsministerium-a-0bec8b22-6269-4224-b620-a689b085fd43 (abgerufen am 31. Mai 2022).

270 European Union External Action Service (EEAS), „A Strategic Compass for Security and Defence“: https://eeas.europa.eu/headquarters/headquarters-homepage/106337/towards-strategic-compass_en (abgerufen am 31. Mai 2022).

271 European Defense Agency, „2020 CARD Report Executive Summary“ (2020), S. 7: https://eda.europa.eu/docs/default-source/reports/card-2020-executive-summary-report.pdf (abgerufen am 31. Mai 2022).

272 European Defence Fund, „Research on disruptive technologies for defence“, Europäische Kommission (2021): https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2021-open-rdis-open (abgerufen am 18. Juli 2022).

273 Europäische Kommission, „The EU budget powering the recovery plan for Europe. Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions“, COM(2020) 44 final (27. Mai 2020): https://ec.europa.eu/info/sites/default/files/about_the_european_commission/eu_budget/1_en_act_part1_v9.pdf (abgerufen am 31. Mai 2022).

274 European Defence Agency, „Defence Data 2019-2020. Key findings and analysis“ (2021), S. 12–13: https://eda.europa.eu/docs/default-source/brochures/eda---defence-data-report-2019-2020.pdf (abgerufen am 31. Mai 2022).

und die Widerstandsfähigkeit gegen Cyber-, weltraumbasierte und hybride Bedrohungen.[275] Die NATO-Verteidigungsminister haben im vergangenen Jahr zudem einen Strategieplan verabschiedet, der die Entwicklung von EDTs durch das Bündnis in sieben Kernbereichen leiten soll, darunter KI, Autonomie und Quantentechnologie.[276] Ferner treiben Deutschland und andere Mitgliedstaaten im Rahmen der NATO-Agenda 2030 ein transatlantisches Ökosystem für Verteidigungstechnologie und -industrie voran. Sie haben vereinbart, einen Defence Innovation Accelerator for the North Atlantic (DIANA)[277] zu etablieren und einen NATO-Innovationsfonds (NIF)[278] einzurichten, über den in den nächsten 15 Jahren mindestens eine Milliarde Euro investiert werden soll.[279]

Handlungs-empfehlungen

Die vom Bundeskanzler angekündigte Zeitenwende muss einen Ausgleich zwischen den ethischen Bedenken und militärischen Erfordernissen in Bezug auf EDTs in der Bundeswehr vorantreiben, wenn diese ein starker Pfeiler der europäischen Sicherheit sein soll. Um dies zu erreichen, sollte die Bundesregierung:

Zwei Prozent des 100-Milliarden-Euro-Sondervermögens für die Förderung disruptiver Verteidigungstechnologien bereitstellen. Die Bundesregierung sollte die Möglichkeit nutzen, mit dem Sondervermögen einen zukunftsfähigen verteidigungstechnologischen Sektor aufzubauen. Obwohl künftige Kampfsysteme wie das FCAS einen beträchtlichen Teil des 100-Milliarden-Euro-Budgets ausmachen, sind derzeit nur 422 Millionen Euro direkt für FuE im Bereich der EDTs, insbesondere für KI-Fähigkeiten, veranschlagt.[280] Die Bundesregierung sollte mindestens 2 Prozent des Sondervermögens für die Förderung disruptiver Verteidigungstechnologien bereitstellen, um Anreize für den Zufluss von Risikokapital in neue Start-ups im Verteidigungssektor und höhere FuE-Ausgaben etablierter deutscher Verteidigungsunternehmen zu setzen.

Die ethische Debatte über militärische Anwendungen von EDTs mit Einsatzrealitäten verbinden. In Deutschland werden Diskussionen rund um das Thema Ethik häufig stark abstrahiert von der Realität militärischer Einsätze geführt. Dabei sollten sich Diskussionen auf die Bestimmung eines angemessenen Maßes an maschineller Autonomie und die Festlegung von vertretbaren Zwecken für den Einsatz von EDTs konzentrieren. Denkbar wären interaktive Workshops, bei denen sich politische Entscheidungsträgerinnen und Entscheidungsträger und/oder Bürgerinnen und Bürger mit wahrscheinlichen Szenarien – zum Beispiel dem Einsatz von Drohnenschwärmen – befassen. Dies könnte die Diskussion über mögliche Gegenmaßnahmen fördern, einschließlich Methoden zur Auswahl von Zielobjekten, wenn die menschliche Reaktionszeit zu langsam ist.

Dual-Use Implikationen von EDTs mit innovationsorientierter Industriepolitik verknüpfen. Ministerien, die Innovations- und Industriepolitik gestalten, insbesondere das Bundesministerium für Digitales und Verkehr (BMDV), das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) und das Bundesministerium für Bildung und Forschung (BMBF), sollten mit dem Bundesministerium der Verteidigung (BMVg) zusammenarbeiten, um das Dual-Use-Potenzial von EDTs wie KI und Quantum in ihren Strategien zu berücksichtigen. neue Nationale Sicherheitsstrategie sollte einen Abschnitt enthalten, der die technologie- und innovationsbezogene Industriepolitik, einschließlich ihrer für die Verteidigung relevanten Aspekte, zusammenführt – und zwar im Rahmen einer regierungsübergreifenden Bewertung zentraler Bedrohungen für die nationale Sicherheit.

275 NATO, „Strategic Concepts" (29. November 2021): https://www.nato.int/cps/en/natohq/topics_56626.htm (abgerufen am 31. Mai 2022).

276 NATO, „Emerging and disruptive technologies", (7. April, 2022): https://www.nato.int/cps/en/natohq/topics_184303.htm (abgerufen am 31. Mai 2022).

277 Ziel des DIANA ist es, die Zusammenarbeit der Allianz im Bereich der EDTs zu fördern und weiterhin Interoperabilität zu gewährleisten. Er wird ein Accelerator-Programm für Start-ups anbieten, das Zugang zu vorqualifizierten Investoren bietet, und Testzentren in Europa und Nordamerika verbinden, um gemeinsam militärische EDT-Anwendungen zu entwickeln, zu validieren und zu testen. NATO, „Emerging and disruptive technologies", (7. April, 2022): https://www.nato.int/cps/en/natohq/topics_184303.htm (abgerufen am 31. Mai 2022).

278 NATO, „NATO Allies take the lead on the development of NATO's Innovation Fund", (22. Oktober 2021): https://www.nato.int/cps/en/natohq/news_187607.htm (abgerufen am 31. Mai 2022).

279 Vivienne Machi, „NATO hopes to launch new defense tech accelerator by 2023", Defense News, 22. Juni 2021: https://www.defensenews.com/global/europe/2021/06/22/nato-hopes-to-launch-new-defense-tech-accelerator-by-2023/ (abgerufen am 31. Mai 2022).

280 Bundesministerium der Verteidigung, „Ministerin: Wir sorgen für eine voll einsatzbereite Bundeswehr", (3. Juli 2022): https://www.bmvg.de/de/aktuelles/ministerin-wir-sorgen-fuer-voll-einsatzbereite-bundeswehr-5438596 (abgerufen am 14. August 2022).

Wissenstransfer zwischen militärischer und ziviler FuE verbessern. Zivile Forschung und Entwicklung im technologischen Bereich bestimmt zunehmend den militärischen Vorsprung. Dem sollte die Bundesregierung Rechnung tragen, indem sie das Münchner Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw) stärker mit den bayerischen Hightech-Start-ups vernetzt. Die Regierung sollte eine separate Track-II-Plattform einrichten, die Innovatoren bei der Entdeckung von Dual-Use-Anwendungen von EDTs unterstützt, welche mit der Förderung von Innovationsagenturen wie SPRIND und dem Cyber Innovation Hub entwickelt werden. Außerdem sollte sie Anreize für deutsche und europäische Risikokapitalinvestitionen in Start-ups im Bereich der Verteidigungstechnologie setzen, etwa durch Ko-Finanzierungen.

Die Beschaffung von Verteidigungsgütern an technologische Innovationszyklen anpassen. Schwankungen im Verteidigungshaushalt erschweren die Unterstützung längerer EDT-Innovationszyklen. Die Regierung sollte einen bis 2030 laufenden Spezial-Fonds für disruptive Verteidigungstechnologien mit jährlichen Mindestbudgetgarantien einrichten. Der Verteidigungsausschuss des Bundestages sollte außerdem ein Mitglied benennen, das über die Projektergebnisse berichtet, die Debatte über Ausgaben für Verteidigungsinnovationen fördert und Möglichkeiten der Zusammenarbeit mit anderen Ausschüssen, einschließlich des Auswärtigen Ausschusses und des Ausschusses für Digitales, ermittelt.[281]

Die Interoperabilität mit Verbündeten durch gemeinsame Grundsätze und militärische Formationen aufrechterhalten. Die Bundesregierung muss sicherstellen, dass die EDT-bezogene Transformation der Bundeswehr nicht die Interoperabilität mit verbündeten Streitkräften untergräbt. Sie sollte die Entwicklung gemeinsamer ethischer Grundsätze und Verhaltenskodizes fördern, wie etwa in der KI-Strategie der NATO geschehen. Deutschland sollte auch die Einführung experimenteller Technologien in binationalen Verbänden und Einheiten (z. B. im Rahmen der Deutsch-Französischen Brigade oder des Deutsch-Niederländischen Korps) fördern und seine Rolle als Teilnehmer am Rahmennationenkonzept der NATO nutzen, um Testumgebungen für militärische Innovationen in multinationalen Formationen zu schaffen.

281 Für ein ähnliches Argument für einen „Defense Innovation and Experimentation Ambassador", siehe: Torben Schütz et al., "Beware of Potemkin: Germany's Defense Rethink Risks Reinforcing Old Habits", War on the Rocks, 11. April 2022: https://warontherocks.com/2022/04/beware-of-potemkin-germanys-defense-rethink-risks-reinforcing-old-habits (abgerufen am 31. Mai 2022).

ÜBER DIESES PROJEKT

Der vorliegende Bericht stellt einen integrierten Politikansatz für Deutschlands digitale Kapazitäten und Zielsetzungen vor. Eine solche Strategie sollte die industriellen Stärken und Digital Governance-Prioritäten des Landes mit seinen geopolitischen Interessen verknüpfen.

Dieser Bericht skizziert einen integrierten Ansatz, welcher auf sieben miteinander verbundenen Teilen eines „Technologiepolitik-Stacks" basiert. Für dieses Projekt hat die DGAP 38 Fachleute dazu eingeladen, einer Arbeitsgruppe beizutreten und zwischen Juli und Oktober 2021 an sieben vertraulichen Workshops über die entscheidenden strategischen Dimensionen von Deutschlands internationaler Digitalpolitik teilzunehmen. Zu den Mitgliedern der Arbeitsgruppe gehörten: politische Mandatsträgerinnen und -träger sowie Kandidatinnen und Kandidaten, hochrangige deutsche Regierungsvertreterinnen und -vertreter, Parteimitarbeiterinnen und -mitarbeiter, die für digitale Plattformen und die Ausarbeitung von Koalitionsverträgen zuständig sind, Expertinnen und Experten für Technologie und Außenpolitik, Vordenkerinnen und Vordenker im Digitalbereich, Managerinnen und Manager von Technologieunternehmen, Akademikerinnen und Akademiker aus den Technik-, Wirtschafts- und Politikwissenschaften sowie Vertreterinnen und Vertreter der Zivilgesellschaft und von Organisationen, die sich für digitale Rechte einsetzen. Außerdem luden wir weitere Expertinnen und Experten dazu ein, an einzelnen Workshops teilzunehmen. Jeder Workshop befasste sich mit jeweils einem Teil von Deutschlands „Technologiepolitik-Stack". Darüber hinaus wurden während der Entstehung dieser Reihe von Berichten Mitglieder der Arbeitsgruppe periodisch konsultiert.

Wir bedanken uns bei der Open Society Initiative for Europe für ihre großzügige Unterstützung, die dieses Projekt ermöglicht hat.

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 Kathrin Hadeler (Einleitung); executive english (Kapitel)

Redaktion Jana Idris

Layout Lara Bührer, Luise Rombach

Design Konzept WeDo

Fotos Autorinnen und Autoren © DGAP

Photos:
Titel © iStock/NicoElNino;
S. 25 © Giu Vicente/Unsplash;
S. 39 © Michael Fousert/Unsplash;
S. 51 © IMAGO/aal.photo;
S. 67 © IMAGO/Kosecki;
S. 81 © iStock/piranka;
S. 93 © IMAGO/photothek