Digitale Souveränität: Anforderungen an Technologie- und Kompetenzfelder mit Schlüsselfunktion

Stellungnahme

www.bitkom.org

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Teresa Ritter | Bereichsleiterin Sicherheitspolitik
T 030 27576-203 | t.ritter@bitkom.org

Satz & Layout

Katrin Krause | Bitkom

Titelbild

© Kim Swain – stocksy united

Digitale Souveränität: Anforderungen an Technologie- und Kompetenzfelder mit Schlüsselfunktion

Stellungnahme

Zusammenfassung

Digitale Souveränität

Über die Digitale Souveränität Deutschlands und Europas wird derzeit viel diskutiert. Oft stehen dabei industrie- und sicherheitspolitische Aspekte im Vordergrund. Dabei wird der Begriff sehr unterschiedlich verwendet.

Die Debatten sind zum Teil missverständlich. Wir wollen deshalb den Begriff der Digitalen Souveränität aufarbeiten und einen fundierten Beitrag zu den jüngsten politischen Debatten z. B. zu Gaia-X oder um den Ausbau des 5G-Netzes leisten. Dieses Papier legt dar, welche Handlungsfelder Digitale Souveränität aus Sicht der Digitalwirtschaft adressiert und welche unterschiedlichen Interessen dabei bestehen. Bereits im Jahr 2015 hat der Bitkom eine Position zur Digitalen Souveränität veröffentlicht, die in weiten Teilen noch heute Relevanz hat. Die Definition von 2015 wird aufgegriffen und weiterentwickelt.

Das Wichtigste

Im Kern ist die Digitale Souveränität die Möglichkeit zur unabhängigen digitalen Selbstbestimmung. Im internationalen Zusammenhang bedeutet das vor allem, eigene Gestaltungs- und Innovationsspielräume zu erhalten und einseitige Abhängigkeiten zu vermeiden. Die Wahrung dieser Handlungs- und Gestaltungsfreiheit umfasst aus Sicht der Digitalwirtschaft folgende Punkte:

- Die Fähigkeit international auf Augenhöhe Schlüsseltechnologien, Geschäftsmodelle und Ökosysteme mitzugestalten, durch Forschung und Entwicklung oder in der Ausarbeitung internationaler Standards.
- Die Fähigkeit neue und bestehende Technologien auf ihre Vertrauenswürdigkeit hin zu bewerten und in die eigenen Produkte, Prozesse, Organisationen und in die Gesellschaft zu integrieren.
- Die Fähigkeit globale Liefer- und Wertschöpfungsketten intelligent zu nutzen und ggf. zu beeinflussen.
- Dabei gilt es zu beachten, dass eine vollständige Digitale Souveränität in einer vernetzten Welt weder realistisch noch zielführend ist. In besonders kritischen Bereichen muss dennoch immer eine Risikoabwägung stattfinden. Eine vollständige Neuentwicklung von bereits auf dem globalen Markt verfügbaren Lösungen kann nach einer umfangreichen Risikoabschätzung u. U. einen Mehrwert haben, wenn es um Kernkomponenten im Bereich der nationalen Sicherheit geht.
- Vor diesem Hintergrund gilt es die dafür notwendigen Kompetenzen zu erhalten, anzuwenden und auszubauen.

Bitkom-Zahl

58 Prozent

der Geschäftsführer und Vorstände quer durch alle Branchen geben an, dass ihr Unternehmen bei der Digitalisierung ein Nachzügler ist. (lt. ↗ einer Studie von Bitkom Research).

Inhaltsverzeichnis

1 Überblick und Zielsetzung

1 Überblick und Zielsetzung

Eine kohärente europäische Digitalstrategie ist eine wichtige Grundlage, um den Wohlstand unseres Kontinents zu sichern, unsere Gesellschaft voranzubringen und unsere politische Handlungsfähigkeit im digitalen Zeitalter zu sichern. Die Digitale Souveränität Europas muss elementarer Bestandteil einer solchen Digitalstrategie sein. Mehr noch, sie ist Grundlage für deren erfolgreiche Umsetzung. Um ein relevanter politischer und wirtschaftlicher Akteur auf globaler Ebene zu bleiben, muss Europa bewusst politische Schritte unternehmen. Gerade in Zeiten sich stark ändernder geostrategischer Verhältnisse, die sich in zunehmenden globalen Handels- und Technologiekonflikten äußern, braucht es klare Antworten Europas auf die damit verbundenen Implikationen für den europäischen Wirtschafts- und Technologiestandort. Europa muss eine weltweite Drehscheibe für innovative Technologien und Dienstleistungen werden, damit leistungsfähige und sichere digitale Technologien hier entwickelt und weltweit gehandelt werden können. Dieses Ziel sollte sich Europa setzen, um seine politische und wirtschaftliche Selbstbestimmung auch im digitalen Zeitalter zu erhalten und seinem sicherheitspolitischen Anspruch jederzeit gerecht zu werden.

Bereits im Jahr 2015 hat Bitkom eine Position zur Digitalen Souveränität Deutschlands veröffentlicht. In weiten Teilen haben die Inhalte noch heute Relevanz. Weiterhin weist Bitkom weitreichende protektionistische Bestrebungen, die sich in der Debatte um Digitale Souveränität auch zeigen, zurück. Der Standort Deutschland im Zentrum Europas profitiert von seiner Einbettung in globale Zusammenhänge, muss und kann auch unter Rückgriff auf globale Technologieressourcen seine Digitale Souveränität stärken. Über Jahrzehnte bewährte und vertrauensvolle Wirtschaftsallianzen dürfen nicht vernachlässigt oder gar gefährdet werden. Eine Zusammenarbeit mit vertrauenswürdigen Partnern über die EU-Grenzen hinaus muss auch weiterhin möglich sein, denn Digitale Souveränität ist nur in starken, zuverlässigen Partnerschaften möglich.[1]

Dennoch will Bitkom seine Antwort auf die jüngsten politischen Debatten um z. B. GAIA-X und den Ausbau des 5G-Netzes geben und dies in den Kontext der Digitalen Souveränität einordnen. Dieses Papier legt die Sichtweise der Digitalwirtschaft dar, welche Handlungsfelder Digitale Souveränität adressiert und welche unterschiedlichen Interessen dabei bestehen. Hierfür wird die Definition von 2015 aufgegriffen und wo nötig weiterentwickelt. Nachfolgend gehen wir im Detail darauf ein, welche unterschiedlichen Dimensionen die Digitale Souveränität umfasst und wie man sie mit kontextabhängigen Maßnahmen und Instrumenten wahren kann. Unabhängig von den Dimensionen Digitaler Souveränität darf Europa gerade bei der Entwicklung neuer Technologien, damit verbundener Geschäftsmodelle und entsprechender Ökosysteme, den Anschluss nicht verlieren. Deshalb beschreiben wir in einem nächsten Schritt, welche Technologie- und Kompetenzfelder aus wirtschaftlicher Sicht eine Schlüsselfunktion haben und durch ihre Nutzung und Anwendung bestehende wirtschaftliche und gesellschaftliche Strukturen disruptiv verändern werden. Außerdem adressieren wir die Frage, welche politische Flankierung notwendig ist, um diese Schlüsseltechnologien ausreichend beherrschen zu können.

1 ↗https://www.bitkom.org/sites/default/files/pdf/Presse/Anhaenge-an-PIs/2015/05-Mai/BITKOM-Position-Digitale-Souveraenitaet1.pdf

2 Stand der Definition

2 Stand der Definition

2.1 Begriffsbestimmung: Das versteht Bitkom unter Digitaler Souveränität

Der Begriff der Digitalen Souveränität ist kein fest umrissener Terminus, sondern zunächst eine politische Zielbestimmung, die verschiedene Aspekte bei der Erarbeitung einer europäischen Digitalstrategie zu vereinen versucht. Unter diesem Begriff werden in der Öffentlichkeit aktuell unter anderem industriepolitische Aspekte, sicherheitspolitische Fragestellungen aber auch verbraucherpolitisch und individualrechtlich geprägte Herausforderungen, etwa im Bereich des Datenschutzes, diskutiert. Wer den Begriff nutzt, bezieht sich auf ein aktuelles oder mögliches zukünftiges Defizit, welches er in der technischen und ökonomischen Leistungsfähigkeit digitaler Unternehmen in einem Betrachtungsraum sieht. Damit ist meist eine Zielvorstellung verbunden, diese Lücke zu anderen Playern mithilfe von vertrauenswürdigen Partnern und eigenen politischen Maßnahmen im Betrachtungsraum zu schließen. Somit kann sie als eine kontextbezogene politische Zielbestimmung gesehen werden, die eine Richtung vorgibt und als Kompass dienen kann. Es gilt deshalb festzuhalten, dass es aufgrund einer besonders heterogenen Landschaft an Akteuren keine abschließende Definition »Digitaler Souveränität« gibt und geben kann. Auch die Schlussfolgerungen und Maßnahmen können divergieren, da auch sie immer kontextgebunden gezogen werden.

Die Digitale Souveränität hat unterschiedliche kontextabhängige Ausprägungen und betrifft sowohl Staat und Wirtschaft als auch Individuen und damit die ganze Gesellschaft. Die Kontrolle über die Speicherung, Weitergabe und Nutzung von Daten und Informationen gehört ebenso dazu, wie die Fähigkeit einer Volkswirtschaft, eigenständig innovative Technologien und wettbewerbsfähige Lösungen hervorzubringen. Darüber hinaus geht es aber auch um Kompetenzen, die dazu befähigen, die Vertrauenswürdigkeit und Integrität von globalen Technologien und Systemen zu bewerten und gegebenenfalls zu steigern, um sich nicht ausschließlich auf eigene Ressourcen verlassen zu müssen, aber im Zweifel eben doch darauf zurückgreifen zu können.

Ein Teilaspekt der Digitalen Souveränität ist das Konzept der Datensouveränität. Datensouveränität hat verschiedene Dimensionen: Die nutzerzentrierte Definition beschäftigt sich mit Fragen der Nutzung und Datenhoheit von personenbezogenen Daten. Eine Geschäftsperspektive beschäftigt sich mit Fragen der Nutzung und Datenhoheit von personenbezogenen und nichtpersonenbezogenen Daten von Unternehmen. Sowie eine politische Perspektive die sich mit Fragen von Zugriffen und Zugriffsrechten von Staaten und Sicherheitsbehörden beschäftigt. Die Datenschutzgrundverordnung hat auf europäischer Ebene bereits für eine Stärkung der Datensouveränität von Verbraucher, Wirtschaft und Staat gesorgt.

Die Selbstbestimmtheit als Ausdruck Digitaler Souveränität ist umso bedeutender, je kritischer der Einsatzbereich digitaler Technologien für eine Gesellschaft ist. Dies kann zum einen bedeuten, dass der Einsatz der digitalen Technologie systemrelevant ist und ein Ausfall mit erheblichen Folgen für die öffentliche Sicherheit und Ordnung verbunden wäre. Zum anderen kann es sich aber auch um Technologien handeln, deren Mangel an europäischen Angeboten, die Wettbewerbsfähigkeit im globalen Wettbewerb, die Innovationsfähigkeit oder das Wirtschaftswachs-

tum ernsthaft beeinträchtigen würde. Das Schaffen eines erfolgreichen, digitalen EU-Wirtschaftsraums bedarf insbesondere souveräner Bürger und Bürgerinnen als Co-Produzenten digitaler Wertschöpfungsketten.[2]

In diesem Sinne müssen Deutschland und Europa Kapazitäten und Kompetenzen in Schlüsseltechnologien und -kompetenzen, Dienstleistungen und Plattformen auf- und ausbauen, um in der Lage zu sein, weltweit führende Technologien einzusetzen, diese als Kunden und Partner mitzugestalten und im Bedarfsfall auch eigenständig zu entwickeln.

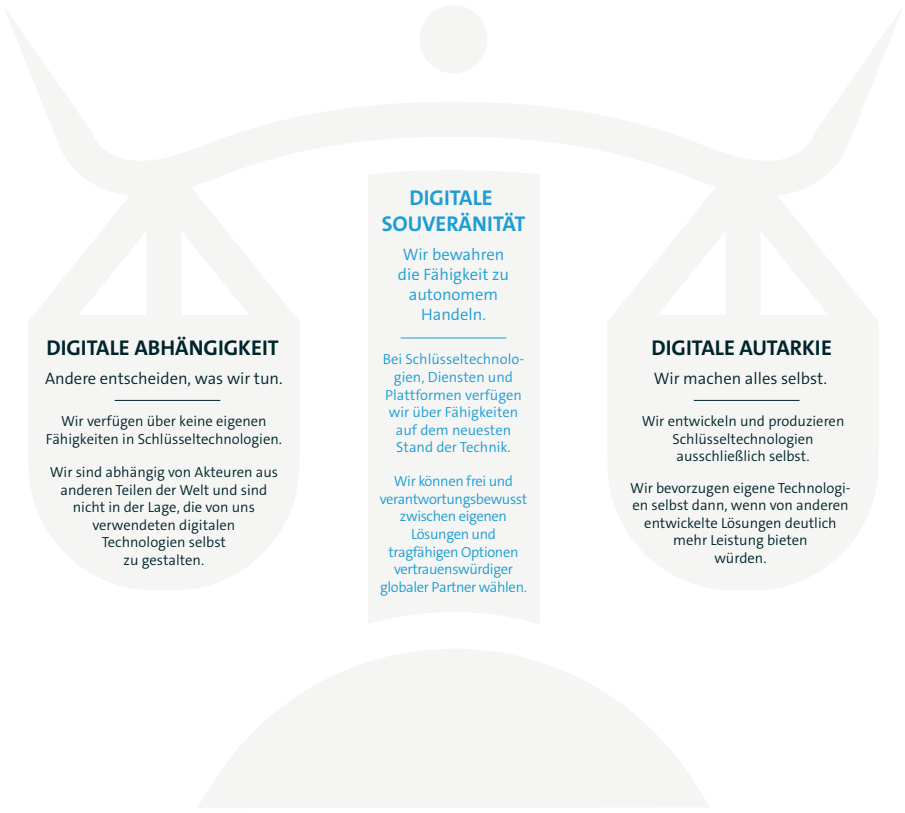

Abbildung 1: Digitale Souveränität

2 MEISTER, S. and B. OTTO, 2019. Digital Life Journey. Framework für ein selbstbestimmtes Leben eines Bürgers in einer sich digitalisierenden Welt (Grundlagenpapier). Dortmund. ISST-Bericht. DOI: 10.24406/ISST-N-559091. Available from: http://publica.fraunhofer.de/documents/N-559091.html

2.2 Konsequenz für Deutschland und Europa

Digitale Souveränität ist somit Ausdruck einer Axiomatik nach der politische Strategien entwickelt werden können. Sie ermöglicht es Staaten, in bestimmten hoch kritischen Bereichen autark zu sein, während es in anderen unkritischen Bereichen nur geringe eigene Handlungskompetenz braucht. Eine vollständige Autarkie jeglicher digitaler Technologien ist in der Breite nicht erwünscht, weil wir damit Wettbewerbsvorteile aufgeben würden, die durch das Nutzen aller weltweit verfügbaren Technologien entstehen. Aufgrund der hohen Kosten, des langsameren Innovationstempos und der Komplexität bestehender globaler Lieferketten in vielen Bereichen, wäre eine vollständige Autarkie außerdem unrealistisch. Digitale Souveränität braucht ein praktikables Gleichgewicht, das unsere politische und wirtschaftliche Handlungs- und Leistungsfähigkeit in einer globalisierten, digitalisierten Wirtschaft erhält und ausbaut.

Die Wahrung der Handlungs- und Gestaltungsfähigkeit für Digitale Souveränität umfasst somit aus der Perspektive der Digitalwirtschaft folgende Aspekte:

- Die Fähigkeit international auf Augenhöhe Schlüsseltechnologien, Geschäftsmodelle und Ökosysteme mitzugestalten, sowohl durch Forschung als auch durch Entwicklung, in der Mitgestaltung internationaler Standards und als Kunde und Partner.

- Die Fähigkeit die weltweit bereits bestehenden und neu entstehenden Technologien auf ihre Vertrauenswürdigkeit hin zu bewerten und in die eigenen Produkte, Prozesse, Organisationen und in die Gesellschaft zu integrieren, um dadurch Wertschöpfung zu erzielen und die Wachstums- und Wettbewerbsfähigkeit der deutschen und europäischen Wirtschaft in Kernfeldern abzusichern und auszubauen.

- Global verteilte Liefer- und Wertschöpfungsketten kreativ und intelligent durch Risikoabschätzungen zu nutzen und ggf. zu beeinflussen.

- Aus sicherheitspolitischer Perspektive gilt weiterhin: Auch wenn eine vollständige digitale Souveränität in einer vernetzten Welt im Normalfall weder realistisch noch zielführend ist, muss in besonders kritischen Bereichen immer eine Risikoabwägung stattfinden. So ist eine vollständige Neuentwicklung von bereits auf dem globalen Markt verfügbaren Lösungen zwar sehr kosten- und zeitintensiv, kann aber nach einer umfangreichen Risikoabschätzung u. U. einen Mehrwert haben, wenn es um Kernkomponenten im Bereich der nationalen Sicherheit geht.

- Entsprechend gilt es vor diesem Hintergrund vorhandene Kompetenzen bestmöglich zur Schaffung und Aufrechterhaltung hinreichend verlässlicher Kommunikations- und Informationssysteme zu erhalten, anzuwenden und auszubauen.

3 Die drei Dimensionen der strategischen Digitalen Souveränität

3 Die drei Dimensionen der strategischen Digitalen Souveränität

Unter der Begriffsdefinition wurden die verschiedenen Dimensionen der strategischen Digitalen Souveränität bereits angerissen. Es wurde dargestellt, dass es zwar um technologische Unabhängigkeit von anderen Staaten geht, aber Gesellschaften durch wichtige Kompetenzen eben auch in der Lage sein müssen, sich selbstbestimmt an Lösungen auf dem globalen Markt zu bedienen. Darüber hinaus kann es Bereiche der Inneren und Äußeren Sicherheit geben, die eine vollständige Neuentwicklung von Lösungen erzwingt.

Die nachfolgende Grafik stellt die drei Dimensionen der Digitalen Souveränität dar.

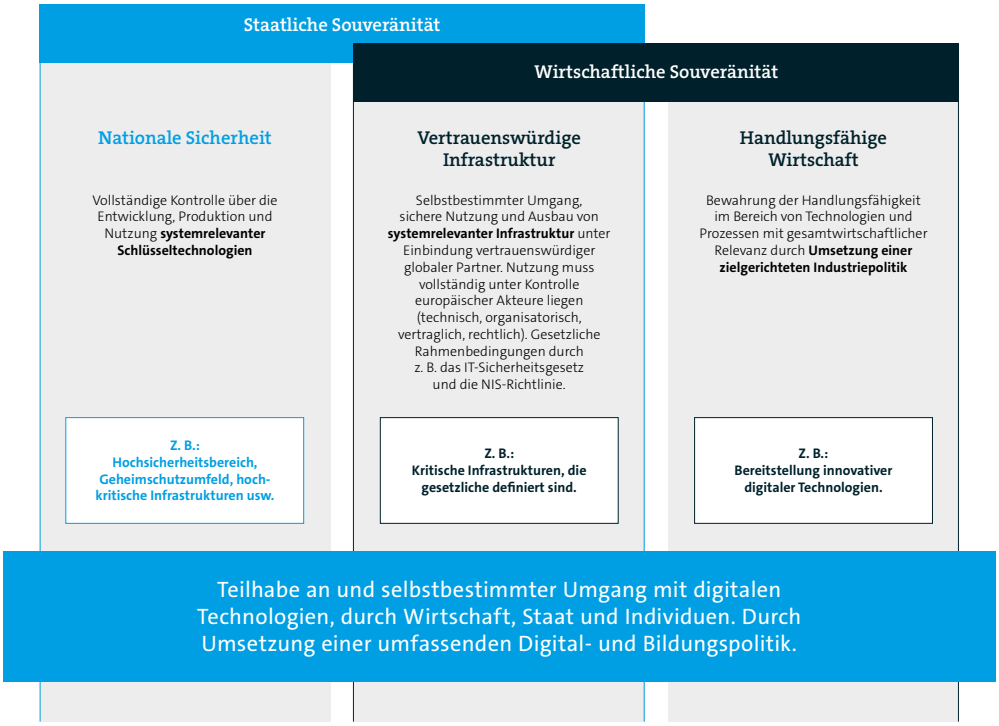

Abbildung 2: Die drei Dimensionen der Digitalen Souveränität

Die Dimensionen sind unterschiedlich zu betrachten und bei der Diskussion um digitale Transformation stets auseinander zu halten. Sie betreffen unterschiedliche Bereiche unserer Gesellschaft und bedürfen grundsätzlich unterschiedlicher Maßnahmen. Bitkom beschäftigt sich in verschiedenen Fachbereichen mit den Dimensionen der Digitalen Souveränität. Während dieses Papier einen Einstieg in die Diskussion liefern soll, wird die Dimension »Nationale Sicherheit« sehr detailliert durch ein gemeinsames Papier des Bitkom mit dem Bundesministerium der Verteidigung (BMVg) und dem Bundesverband Deutschen Sicherheits- und Verteidigungsindustrie (BDSV) aufgegriffen.[3]

3 ↗https://www.bmvg.de/resource/blob/140202/5f48d9a452805e7c3f2e61395682d7a9/ideenpapier-vertrauenswuerdige-it-data.pdf

Auch der Arbeitskreis Verteidigung des Bitkom beschäftigt sich mit der Bedeutung des Themas im militärischen Umfeld. Die Einbindung der Bundeswehr in multinationale Strukturen muss daher in der Gesamtbetrachtung der Digitalen Souveränität berücksichtigt werden. Im Rahmen der Kooperation zwischen dem Bitkom und dem Kommando Cyber- und Informationsraum (KdoCIR) wird das Thema in einer eigenen Arbeitsgruppe aus Vertretern der Industrie und der Bundeswehr behandelt.

Allen drei Dimensionen liegen die Teilhabe an und der selbstbestimmte Umgang mit digitalen Technologien durch Staat, Wirtschaft und Gesellschaft zugrunde. Wir sprechen uns deshalb für eine frühe Förderung dieser individuellen Selbstbestimmtheit im digitalen Raum aus. Eine umfassende Digital- und Bildungspolitik die den selbstbestimmten Umgang mit Daten und Produkten in jeder Lebensphase fördert, fehlt bis heute und muss deshalb dringend auf den Weg gebracht werden.[4]

3.1 Nationale Sicherheit

Hier geht es um Bereiche, die für die Wahrung unserer nationalen Sicherheit von hoher Bedeutung sind. Da die Gewährleistung der Äußeren Sicherheit den Kernbereich staatlicher Souveränität betrifft, handelt es sich hierbei um einen besonders sensiblen Bereich, der sich mit sicherheitspolitischen Grundsatzentscheidungen decken muss – auch für digitale Technologien. Eine vollständige Kontrolle über die Entwicklung, Produktion und Nutzung systemkritischer Schlüsseltechnologien ist hier zwingend notwendig. Dies bedeutet, dass die vollständige Souveränität der gesamten Technologie und Nutzung garantiert sein muss. Anwendungsszenarien betreffen in der Regel den Staat im Geheimschutzumfeld, hochkritische Infrastrukturen oder Systeme, die bei einem Ausfall die Souveränität eines Staates beeinträchtigen.

Heutige Hard-Software-Systeme weisen eine hohe Komplexität auf. Derartig komplexe Systeme von Grund auf mit eigenen Ressourcen selbst aufzubauen, um die Technologie souverän kontrollieren zu können, wäre in mehreren Ressourcendimensionen nicht ökonomisch sinnvoll darstellbar. Die Zertifizierung von Gesamtsystemen und Plattformen stellt ebenfalls eine Herausforderung dar, da in regelmäßigen und immer kürzeren Abständen neue Softwareversionen eingespielt werden, nicht zuletzt um Sicherheitsverwundbarkeiten zu beseitigen. Aufwendige Re-Zertifizierungen möchte man vermeiden, das Einfrieren von Versionsständen wird allerdings auch zum Risiko, und zwar nicht nur aus Sicherheitssicht. Um Digitale Souveränität im Sinne von eigener Kontrolle über die Technologie zu erlangen, bedarf es daher Lösungen, welche die o.g. Problemstellungen der Komplexität und Größe von Systemen sowie der häufigen Aktualisierungen berücksichtigen.

Ein vielversprechender Ansatz besteht darin, die technischen Kernfunktionen und -komponenten zu identifizieren, die für die Sicherstellung der eigenen Kontrolle über die Systeme benötigt

4 ↗https://www.bitkom.org/sites/default/files/file/import/FirstSpirit-1515141793223180103-Positionspapier-Digitale-Bildung-Neuauflage.pdf

werden und diese im Gesamtsystem modular und ersetzbar zu gestalten. Naheliegende Beispiele sind kryptographische Funktionen und das zugehörige Schlüsselmanagement. Es bedarf weiterer und teils auch heute noch unbekannter Lösungen, um die Kontrolle über ein System sicherzustellen.

Wir benötigen dafür eine Architektur, die eine modulare Einbindung und Ersetzbarkeit dieser Kernfunktionalitäten so ermöglicht, dass nachweisbar durchsetzbar ist, wer das System und die Datenflüsse kontrollieren kann. Diese Architektur und Schnittstellen können nur zusammen mit der Industrie entwickelt werden.

Durch die Kapselung erhält man kleinere, weniger komplexe Komponenten, die unter eigener Hoheit hergestellt und zertifiziert werden können, was durchaus ökonomisch darstellbar ist. Es kann hierfür ein Markt für vertrauenswürdige Komponenten entstehen, der eine Chance für europäische, auch kleinere Unternehmen darstellt.

Auch wenn die Technologie nicht im einzusetzenden Land entwickelt wird, ist somit sichergestellt, dass sie selbstbestimmt eingesetzt werden kann (ggf. durch Unterstützung weiterer analytischer oder schützender Technologien, Verträge, Standardisierungen, offene Schnittstellen, Transparenz etc.). Gesetzliche Grundlage hierfür ist das IT-Sicherheitsgesetz auf nationaler Ebene, sowie die NIS-Richtlinie auf europäischer Ebene. Die erforderlichen Standards sollten unbedingt gemeinsam mit der Industrie formuliert werden, um nicht nur das erforderliche Schutzniveau zu erreichen, sondern auch eine reibungslose Implementierung sicherstellen zu können.

Handlungsempfehlungen an die Politik:

- Förderung von innovativen Technologien im Kontext der Sicherheit von Geräten, Infrastrukturen und Systemen, wie z. B. Verschlüsselungsalternativen zur Post-Quanten-Kryptographie sowie der künstlichen Intelligenz zum Schutz von Netzwerken.

- Sicherstellung vertrauenswürdiger Wertschöpfungsketten für Kritische Infrastrukturen, die nach dem IT-Sicherheitsgesetz in Deutschland bzw. der NIS-Richtlinie oder dem Cybersecurity Act auf europäischer Ebene definiert sind.

- Sicherstellung vertrauenswürdiger Elektronik in Europa und Deutschland, um beispielsweise mögliche Backdoor-Funktionen in Importen auszuschalten.

- Bereitstellung der Kompetenz zur Identifikation, Spezifikation und Standardisierung der Architektur, der austauschbaren Kernkomponenten (Hard-/Software-Module), und der Schnittstellen zur Sicherstellung der technischen Kontrollhoheit über das System. Sowie Bereitstellung der Kompetenzen zur Zertifizierung sowohl auf Systemebene, als auch auf Chipebene.

- Methoden für die Entwicklung und Analyse der vorbenannten Kernkomponenten sowie Vermeidung von Exporthürden für Kernkomponenten.

- Kompetenzen bestmöglich zur Schaffung und Aufrechterhaltung hinreichend verlässlicher Systeme und Technologien erhalten, anwenden und ausbauen.

- Unterstützt werden sollten die zuvor aufgeführten Punkte überdies durch die Bedarfsanforderung und Pilotprojekte von und mit der öffentlichen Hand sowie europäische Leuchtturmprojekte wie AIRBUS für den Flugzeugbau und GALILEO für ein Satelliten-Navigationssystem.

- Die die wesentlichen nationalen Sicherheitsinteressen betreffenden Anteile von Cyber/IT sollten im Rahmen der nationalen Schlüsseltechnologien angemessen Berücksichtigung finden. Der Begriff der Schlüsselfähigkeiten[5] sollte zusätzlich eingeführt, übergreifend abgestimmt und definiert sowie detailliert werden.[6]

3.2 Sichere und vertrauenswürdige Kritische Infrastruktur

Eine weitere Dimension der Digitalen Souveränität sind sichere und vertrauenswürdige Kritische Infrastrukturen. Ein selbstbestimmter Umgang sowie eine sichere Nutzung der systemrelevanten Infrastrukturen unter Einbindung vertrauenswürdiger globaler Partner sind für die Erhaltung Digitaler Souveränität unbedingt notwendig. Ein fairer und innovationsstimulierender Wettbewerb mit gleichen Regeln für gleiche Dienste und Angebote sowie die Vielfalt von Technologien und Anbietern ist dabei essenziell. Rahmenbedingungen muss die Politik dabei so gestalten, dass die notwendige Markterschließungsgeschwindigkeit ermöglicht wird. Daneben müssen der Rechtsrahmen und seine Umsetzung so gesetzt werden, dass Kritische Infrastrukturen jederzeit ein Höchstmaß an Sicherheit einschließlich der Verfügbarkeit gewährleisten und nicht kompromittiert werden können. Grundsätzlich gilt, dass für alle Hersteller – ganz gleich welcher Produkte und Angebote sowie unabhängig ihrer Herkunft – idealerweise mindestens europaweit die gleichen produkt- und angebotsspezifischen Prüfkriterien, Regeln und Verfahren gelten müssen.

Auch muss der Gesetzgeber eindeutig adressieren, welche Anforderungen er zur Gewährleistung eines entsprechenden Maßes an IT-Sicherheit stellt. Auch hier ist dem europäischen Cybersecurity Act, dem IT-Sicherheitsgesetz, dem New Legislative Framework sowie der NIS-Richtlinie als horizontaler Regulierung eine bedeutende Rolle zuzuschreiben. In diesem Kontext sollten alle künftigen Regulierungsvorhaben diskutiert werden.

5 Unter Schlüsselfähigkeiten im Kontext Cyber/IT werden die Fähigkeiten verstanden, welche unter Nutzung von Technologieelementen (sowohl Schlüsseltechnologien als auch Nicht-Schlüsseltechnologien) elementar für die Konzeption, Realisierung und Nutzung sowie Lebenszyklusunterstützung von vertrauenswürdigen Informationssystemen, einzelnen Systemkomponenten oder Systemfunktionalitäten sind. (Arbeitshypothese bis zur Bereitstellung einer umfänglichen und formal abgestimmten Definition

6 ↗https://www.bmvg.de/de/aktuelles/vertrauenswuerdige-it-bundeswehr-140710

Bereits in der Debatte um die Aktualisierung des Katalogs von Sicherheitsanforderungen nach § 109 TKG durch die Bundesnetzagentur hat Bitkom Handlungsempfehlungen[7] an den Gesetzgeber formuliert. Die darin aufgeführten Aspekte haben Relevanz weit über die 5G-Infrastruktur hinaus, weshalb wir sie leicht abgeändert im Folgenden auch im Kontext der Digitalen Souveränität für notwendige Voraussetzung halten.

Handlungsempfehlungen an die Politik:

- Transparenz ist die Grundlage für Vertrauen. Dies setzt einen kooperativen Ansatz mit klar definierten Regeln für alle Seiten voraus. So wird die Grundlage gelegt, nicht nur das jeweilige Produkt zu sichern, sondern auch die Erkenntnisse im sicheren Entwicklungslebenszyklus für zukünftige Produkte zu stärken. Alle Beteiligten sollten sicherstellen, dass sie frei von unangemessenem staatlichem Einfluss sind und ihr Handeln mit den Standards und Zielen der OECD-Grundsätze für Corporate Governance übereinstimmt.

- Innovation sichert den Wohlstand von morgen. Innovationen im IKT-Bereich werden zunehmend zur Triebfeder der Entwicklung von Wirtschaft und Gesellschaft. Dafür ist eine innovationsfreundliche Regulierung entscheidend. Staatlicherseits sollten vor allem die Zielsetzung und die Anforderungen der vorgeschlagenen Maßnahmen definiert werden. Dabei ist ein risikobasierter Ansatz zu wählen. Im Rahmen einer Zertifizierung ist die gegenseitige Anerkennung zumindest auf europäischer Ebene zu schaffen. Hier sollte immer auf bereits international anerkannte Standards, Normen und Zertifikate zurückgegriffen werden.

- Staatliche Stellen und in staatlichem Auftrag Handelnde, Betreiber Kritischer Infrastrukturen und Hersteller tragen jeweils ihren Teil zur Verantwortung für sichere KRITIS bei und müssen hierfür entsprechend ihrer jeweiligen Rollen und Zuständigkeiten alle erforderlichen Maßnahmen treffen. Gleichzeitig sind auch die Nutzer dafür zu sensibilisieren, ihren Beitrag für Sicherheit, Integrität und Verfügbarkeit von Daten zu leisten und beispielsweise bei kritischen Daten konsequent Verschlüsselungen einzusetzen.

- Der Europäische Binnenmarkt ist eine Erfolgsgeschichte für die wirtschaftliche Entwicklung in Deutschland. Eine wichtige Zielsetzung für Staat und Wirtschaft in Deutschland ist es, diesen Binnenmarkt zu stärken und an seiner Innovationskraft teilzuhaben. Im Kontext der Digitalisierung gilt dies mehr denn je, wie die europäische Kommission mit ihrer Strategie für den europäischen digitalen Binnenmarkt bereits 2015 bekräftigte[8]. Daher muss jedwede Festlegung von Sicherheitsanforderungen, auch die Zertifizierung von als »kritisch« zu bewertenden Kernkomponenten im europäischen Rahmen erfolgen und die darauf basierende Zertifizierung durch nationale Prüfstellen europaweit anerkannt werden. Nationale Alleingänge schwächen die wirtschaftliche Entwicklung und bremsen die Innovationsfähigkeit. Durch den Cybersecurity Act wurde auf europäischer Ebene bereits ein möglicher Rahmen dafür gesetzt.

7 ↗https://www.bitkom.org/sites/default/files/2019-11/20191118_bitkom-stellungnahme_katalog-sicherheitsanforderungen.pdf

8 ↗https://ec.europa.eu/info/strategy/priorities-2019-2024

- Die Anwendungsfälle vertrauenswürdiger IT, die derzeit noch nicht hinreichend verlässlich regulatorisch abgebildet sind, sollten präzisiert werden, um Handlungssicherheit zu gewährleisten.

- Die Fähigkeit zur quantitativen und qualitativen Bemessung des Bedarfes an Sicherheit inklusive der Berücksichtigung des Aufwandes sollte sowohl im Hinblick auf das benötigte Maß an Vertrauenswürdigkeit als auch an Verfahrensstärke und Wirksamkeit verbessert werden.

3.3 Handlungsfähige Wirtschaft

Eine weitere Dimension der Digitalen Souveränität ist die Handlungsfähigkeit der deutschen und europäischen Wirtschaft im Bereich neuer und innovativer Technologien. Es geht dabei um den Erhalt und die Schaffung von Fähigkeiten in der nationalen bzw. internationalen Wirtschaft, um die staatliche Souveränität zuerst zu ermöglichen bzw. zu stärken. Die derzeitige Situation ist verbesserungswürdig. Gegenseitige Abhängigkeiten scheinen zum Nachteil von Europa aus dem Gleichgewicht zu geraten. Priorität hat deshalb die Sicherstellung einer Digitalen Souveränität für Zukunftsthemen. Ein digitaler Binnenmarkt zur Schaffung eines weltweit größenordnungsmäßig vergleichbaren, technisch-regulativ homogenen Nachfragepools, der europäischen Firmen ein für Innovationsfinanzierung ausreichendes Wachstum innerhalb der EU ermöglicht und auf dessen Basis internationale Wettbewerbsfähigkeit und Exportstärke erzielt werden können, muss das Ziel sein.

Nachfolgend werden Maßnahmen aufgeführt, die nötig sind, um die Wettbewerbsfähigkeit der europäischen Wirtschaft im Bereich digitaler Technologien zurückzugewinnen und damit ein gewisses Maß an technologischer Unabhängigkeit zu gewährleisten.

Handlungsempfehlungen an die Politik:

- Die erfolgreiche digitale Transformation der Industrie in Deutschland und der EU entscheidet sich mithin weder allein auf der Anbieterseite noch ausschließlich auf der Anwenderseite. Beide Aspekte hängen vor allem insoweit zusammen, als Anwender von IT-Dienstleistungen und Nutzer erfolgskritischer digitaler Technologien auf einen hinreichenden Wettbewerb auf der Anbieterseite angewiesen sind. Wirksamer Wettbewerb in einem europäischen Binnenmarkt verhindert am ehesten einseitige Pfadabhängigkeiten und verspricht die größte Innovationsdynamik. Die Sicherstellung und Förderung des dafür notwendigen Wettbewerbs ist eine wesentliche Aufgabe der Politik. Dazu braucht es vor allem das Durchhaltevermögen, kurzfristigen Gewinnen auf Basis protektionistischer Entscheidungen zu widerstehen und stattdessen zu einer wettbewerbsorientierten, offenen internationalen Wirtschaftsordnung zu stehen.

- Einer der wichtigsten externen Faktoren für die digitale Transformation, vom Kleinunternehmen über den Mittelstand bis hin zu großen Konzernen und dem Staat selbst, ist der Faktor

Zeit. Da die Digitalisierung die Dauer von Innovationszyklen radikal verkürzt, wird die rasche Implementierung von technologiegetriebenen Innovationen zu einer kritischen Anforderung und erfordert deshalb einen innovationsfreundlichen Regulierungsrahmen sowie geeignete Forschungs- und Innovationsförderung auf europäischer Ebene. Gerade Startups brauchen eine passende Förderung, z. B. durch die Vergabe von Venture Capital anhand von Bewertungsstandards, die einem agilen Startup-Ökosystem gerecht werden.

- Zur Erhaltung der Wettbewerbsfähigkeit dürfen die Kosten für Einhaltung regulatorischer Standards auf dem EU-Markt nicht allein für EU-ansässige Marktteilnehmer entstehen, vielmehr müssen die Standards für alle Teilnehmer im EU-Markt verpflichtend gelten und effektiv durchgesetzt werden. Dies bedeutet, dass auch EU-Unternehmen nur von außereuropäischen Unternehmen Komponenten und Dienstleistungen beziehen können, welche die EU-Standards erfüllen – auch im Hinblick auf Corporate Social Responsibility (CSR) wie etwa Umweltschutz. In Erweiterung zur CSR sollten zudem klare Verhaltensregeln für ein verantwortungsvolles Miteinander in sich digitalisierenden Geschäftssystemen – Corporate Digital Responsibility – messbar vorgegeben werden. Dies erfordert geeignete Nachweise und Zertifizierung entlang der Wertschöpfungskette. Diese Standards sollten die EU aktiv mitgestalten und international durchsetzen.

- Gerade die deutsche Wirtschaft ist mittelständisch geprägt, mit hoch innovativen, aber oftmals sehr eng begrenzten Lösungen. Test- und Experimentierfelder für den Aufbau digitaler Infrastrukturen, die internationale Beachtung erlangen, ziehen globale Unternehmen, Startups und Wissen an. Dies bietet die beste Voraussetzung, um Lösungspartnerschaften zu schmieden und als Ökosystem gemeinsam den Weltmarkt zu beliefern. GAIA-X ist ein Projekt, das die Chance erkennt und solche Ökosysteme besonders fördert, eine Ausweitung auf weitere Technologiefelder ist möglich.

- Für eine nachhaltig erfolgreiche Digitalisierung müssen neben ausreichenden Investitionen in Digitalisierung und Cyber-Sicherheit immer auch die Mitarbeiter und deren Qualifizierung berücksichtigt werden. Gerade im Hinblick auf Fachkräfte, bedeutet das u.a. eine Umstellung des Bildungswesens mit Schwerpunkten und Fokussierung in STEM Kurrikulum.

- Die öffentliche Hand ebenso wie Unternehmen, insbesondere im Mittelstand, benötigen Entscheidungskompetenz, um Angebote am Markt und Maßnahmen für mehr Cyber-Sicherheit bewerten zu können. Entscheidungskompetenz muss in allen Bereichen aufgebaut werden.

4 Technologie- und Kompetenzfelder mit Schlüsselfunktion

4 Technologie- und Kompetenzfelder mit Schlüsselfunktion

Unabhängig der drei Dimensionen Digitaler Souveränität, wurde zu Beginn des Papiers beschrieben, dass Europa gerade bei der Entwicklung neuer Technologien nicht den Anschluss verlieren darf. Denn unabhängig, ob es um eine handlungsfähige Wirtschaft, Kritische Infrastrukturen oder die nationale Sicherheit geht, Grundvoraussetzung zur Erlangung Digitaler Souveränität ist ein Gleichgewicht technologischer Abhängigkeiten. Hierzu gehört, dass Staaten durch eigene Kompetenzen in der Lage sind wesentliche digitale Technologien selbstständig zu verstehen, zu nutzen, zu modifizieren und herzustellen. Im Folgenden stellen wir Technologie- und Kompetenzfelder vor, die eine Schlüsselfunktion haben, da ihre Nutzung und Anwendung bestehende wirtschaftliche und gesellschaftliche Strukturen disruptiv verändern wird.[9] Aus wirtschaftlicher Sicht sind sie dadurch gekennzeichnet, dass ganze Geschäftsmodelle und Wirtschaftszweige auf ihnen basieren. Unternehmen erlangen durch die Nutzung dieser Technologien und Kompetenzen entscheidende Wettbewerbsvorteile und treiben so die digitale Transformation der Wirtschaft voran. Die nachfolgende Definition ist aus dem Jahr 2015 und hat noch heute ihre Gültigkeit.

4.1 Begriffsbestimmung: Schlüsseltechnologie und Schlüsselkompetenz

Nationale Schlüsseltechnologien sind Technologien, die aus den außen-, sicherheits- und europapolitischen Interessen Deutschlands, dem militärischen Bedarf der Bundeswehr[10], den Bündnisverpflichtungen sowie der Verantwortung Deutschlands abgeleitet und regelmäßig überprüft werden.

1. Entwicklungs- und Produktionskompetenzen rund um IT-, Netzwerk- und Plattformsicherheit, Infrastrukturen und Verschlüsselungstechnologien sowie

2. Kompetenzen, digitale Technologien, Lösungen und Plattformen zu verstehen, zu prüfen, verantwortungsvoll einzusetzen und im Bedarfsfall so weitgehend zu veredeln und zu härten, dass sie den jeweils angestrebten Sicherheitsanforderungen entsprechen.

Hieraus leiten wir die folgenden neun Technologie- und Kompetenzfelder mit Schlüsselfunktion ab (siehe Schaubild 2). Sie lassen sich in drei Gruppen einteilen. Künstliche Intelligenz, Sicherheitstechnologien und Blockchain sind dem Bereich »Anwendungen & Software« zuzuordnen. Durch diese Gruppe von Technologie- und Kompetenzfeldern werden Prozesse und Anreizme-

9 Ergänzend sei auf die Studie **↗Kompetenzen für eine Digitale Souveränität** aus dem Jahr 2017 verwiesen, die die Relevanz einzelner Technologien für eine Digitale Souveränität anhand der Kriterien Zukunftsfähigkeit, Interoperabilität, Substituierbarkeit sowie strategische Bedeutung bewertet. Insgesamt wurden 121 Technologien bewertet.

10 Siehe hierzu die Definition aus dem Papier aus dem Ideenpapier »Sichere IT« von BMVg, BDSV und Bitkom: **↗https://www.bmvg.de/de/aktuelles/vertrauenswuerdige-it-bundeswehr-140710**

chanismen in der Wirtschaft vollkommen neu organisiert. Es ist damit nicht von einem engen Technologiebegriff auszugehen. Vielmehr sind auch Kompetenzen und Anwendungen als erforderliche Grundlagen mit in den Blick zu nehmen. Die Bedeutung der Anwendungsfelder zeigt sich an querschnittlichen Schlüsselfaktoren für die europäische Wirtschaft, wie z. B. digitale Identitäten.

Die weiteren Technologie- und Kompetenzfelder Rechenzentren & Cloud-Infrastruktur, Kommunikationssysteme & Netze, Hochleistungsrechner & Quantencomputer und Mikro- und Nanoelektronik sind die Infrastruktur- und Hardwaregrundlagen der digitalen Transformation. Eine mittlere Position zwischen den beiden Bereichen nehmen Digitale Plattformen ein. Sie können je nach Art bzw. Einsatz der betreffenden Plattform sowohl Infrastruktur als auch Anwendung sein, mitunter sogar beides gleichzeitig.

Abbildung 3: Schlüsseltechnologien

4.2 Infrastruktur & Hardware

4.2.1 Kommunikationssysteme & Netze

Digitale Infrastrukturen im Festnetz und im Mobilfunk bilden das Rückgrat einer vernetzten und digitalen Wirtschaft und Gesellschaft. Sie selbst sind eine kritische Infrastruktur[11]. Neben Video-, Augmented- und Virtual-Reality-Anwendungen, die das Datenvolumen vorantreiben, nutzen immer mehr vertikale Branchen digitale Infrastrukturen zur Vernetzung ihrer Prozesse. Viele

11 ↗https://www.kritis.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/Aufgabenbereiche/ITundTK/informationstechnikundtelekommunikation_node.html

dieser vertikalen Sektoren sind ebenfalls Kritische Infrastrukturen wie etwa Energie, Wasser und Gas. Hinzu treten intelligente Stadtanwendungen, Verkehr einschließlich automatisierter Fahrzeuge und Anwendungen im Gesundheitsbereich.

Der Datenverkehr in Kommunikationsnetzen wächst exponentiell. Dadurch steigen die Anforderungen der Anwender an die Kommunikationsnetze, z.B. hinsichtlich Mobilität, Bandbreite, Verfügbarkeit, Sicherheit und perspektivisch an Echtzeit-Fähigkeit. Die konvergenten Netze von Festnetz und Mobilfunk erfordern daher eine hoch flexible und skalierbare Architektur, in der die Netzfunktionen virtualisiert sind (Network Function Virtualisation, NFV) und gemäß den Anforderungen bezüglich Leistungsfähigkeit und operativer Effizienz verteilt (wie Multi-Access Edge Computing, MEC / Distributed Cloud Computing) oder zentral implementiert werden können. Software wird ein immer wichtigerer Bestandteil moderner Kommunikationsstruktur. Der weitere Ausbau der Glasfasernetze und der Einsatz der Schlüsseltechnologie 5G sind wesentliche Träger dieser Netzarchitektur. Zukünftige Netze werden zunehmend künstliche Intelligenz, Machine Learning und Softwaretechnologien einsetzen. Cybersecurity wird ein integraler Teil dieser Netze sein. In diesem Sinne sind die einzelnen Schlüsseltechnologien nicht mehr getrennt zu sehen sondern sie wachsen zunehmend zusammen.

Forschung, Entwicklung und Herstellung von Kommunikationssystemen und -netzen sind eine wesentliche Voraussetzung und der Garant für den Markterfolg und das Wachstum im Dienstleistungsbereich. Bereits heute bauen moderne Kommunikationsnetze weltweit auf europäischer Technologie auf. So hat Europa beispielsweise eine ausgeprägte Landschaft an kleinen und mittelständischen Unternehmen, die Telekommunikationslösungen entwickeln und fertigen. Und auch die zukünftigen 5G-Leitmärkte setzen auf innovative Netzwerktechnik aus Europa. Im Hinblick auf die Anforderungen an eine sichere, hochverfügbare, zuverlässige und unabhängige Infrastruktur muss Europa seine technologische Souveränität nutzen, bei Forschung und Entwicklung vorantreiben und am Ende Investitionen in dieses Know-how sicherstellen. Hierbei geht es weniger um einen Ausschluss bestimmter Technologien und Hersteller, sondern um das Einführen gezielter Redundanzen, um im Bedarfsfall souverän entscheiden und auswählen zu können.

Handlungsempfehlungen an die Politik:

- Es muss so viel privatwirtschaftliches Engagement wie möglich generiert und incentiviert werden. Gleichzeitig muss die Entwertung bereits getätigter Investitionen verhindert werden. Die Umsetzung des Europäischen Kodex für elektronische Kommunikation setzt den Rahmen für die Entwicklung des Telekommunikationssektors der nächsten Dekade. Sie bietet die Chance, die Digitalisierung und Vernetzung Deutschlands zu gestalten und zu beschleunigen.

- Die staatliche finanzielle Förderung des Netzausbaus muss weiterhin das letzte Mittel bleiben und darf den eigenfinanzierten Ausbau der Unternehmen nicht verdrängen, verzerren oder gar entwerten. Um flächendeckend schnelle Internetverbindungen im ländlichen Raum sicherzustellen, ist die öffentliche Hand aber dort gefragt, wo ein wirtschaftlicher Ausbau perspektivisch nicht machbar ist. Für diese unterversorgten Gebiete braucht es unter Berück-

sichtigung eines ausreichenden Investitionsschutzes auch künftig öffentliche Mittel zur Förderung des Ausbaus von Glasfasernetzen. Hierbei müssen auch weiterhin Anbindungsbedarfe für bestehende oder künftige Mobilfunkstandorte in die Glasfasernetzplanungen einbezogen werden.

- 5G ist eine zentrale Technologie der Gigabit-Gesellschaft. Für den Auf- und Ausbau der entsprechenden Infrastruktur ist eine vorausschauende und europaweit koordinierte Frequenzstrategie, inklusive der Zuweisung weiterer Frequenzen für Mobilfunk, nötig. Zusätzlich ist auch für WLAN weiteres Spektrum erforderlich.

- Die zukünftige Ausrichtung der Frequenzregulierung muss mehr Rechts- und Planungssicherheit schaffen, um die Bedingungen des Mobilfunkausbaus zu verbessern. Eine etwaige Förderung von Mobilfunkstandorten muss wettbewerbsneutral erfolgen, um verbleibende weiße Flecken zu schließen und den Roll-Out von 5G zu beschleunigen.

- Schnellerer Glasfaser- und Mobilfunk-Ausbau braucht einfachere, standardisierte Antrags- und Genehmigungsverfahren. Ziel muss u.a. die vollständige Digitalisierung aller wegerechtlichen Genehmigungsprozesse für Fest- und Mobilnetze sein. Zudem sollte das Potenzial alternativer Verlegetechniken deutlich stärker ausgeschöpft werden, um Kostensenkungs- und Beschleunigungspotenziale beim Glasfaserausbau zu heben.

- Die Akzeptanz des Ausbaus von Festnetz und neuen Mobilfunkstandorten in der Bevölkerung muss deutlich verbessert werden. Das ist eine gemeinsame Aufgabe von Politik und Wirtschaft. Zudem braucht es einen Rechtsrahmen und eine entsprechende Anwendungspraxis, die es ermöglichen, die differenzierten Anforderungen von Wirtschaft und Nutzern an sichere Netze und Konnektivität zu erfüllen. Vor dem Hintergrund von 5G bedeutet dies, dass insbesondere mittels Network Slicing erbrachte Dienste nicht von vornherein durch restriktive Regulierung behindert werden dürfen, sondern durch einen Light Touch Approach die Chance erhalten, sich nachfragegerecht zu entwickeln.

- Die im Rahmen des 5-Punkte-Plans in der vom BMVI vorgelegten Mobilfunkstrategie greifen viele Forderungen der Branche auf, müssen nun aber in enger Kooperation von Branche, Politik und Aufsichtsbehörden konkretisiert und ungesetzt werden. Neben dem Bund müssen auch die Länder und Kommunen Verantwortung übernehmen und Investitionshemmnisse beseitigen. Besonders wichtig ist dabei die frühzeitige Diskussion über sinnvolle Vergabeverfahren für Frequenzen ohne teure Auktionen,

- Eine etwaige Mobilfunk-Infrastrukturgesellschaft (MIG) begegnet grundsätzlichen Bedenken, könnte aber bei Beschränkung auf solche Standorte, die sich durch lokale Hindernisse nicht durch Netzbetreiber ausbauen lassen, einen sinnvollen Beitrag auch ohne Anschluss- und Benutzungszwang leisten.

- Die Bereitstellung von Infrastrukturen, Grundstücken und Liegenschaften des Bundes sollte ausgeweitet werden auf sämtliche geeigneten Liegenschaften der öffentlichen Hand (Bund, Länder, Kommunen) und dabei ein Verzicht auf Mietzahlungen erfolgen.

4.2.2 Rechenzentren & Cloud-Infrastruktur

Leistungen und Services, denen Rechenzentren zugrunde liegen, werden nahezu rund um die Uhr in Anspruch genommen. Das beginnt im Kleinen beim Upload von Handyfotos oder Nachrichten aus dem Messenger in die Cloud, bei E-Mails und Einkaufslisten, Kalendereinträgen und Suchmaschinenanfragen. Vor allem aber im Großen werden heute zahlreiche Dinge in unserer Umgebung direkt oder indirekt von Rechenzentren kontrolliert, seien es Energie, Telekommunikation, Internet, Verkehr, Industrie 4.0, Banken oder Sicherheitssysteme. In der Verordnung des Bundesministeriums des Innern zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz heißt es, dass die Funktionsfähigkeit von Rechenzentren für die Erbringung der kritischer Dienstleistungen zwingend erforderlich ist.[12] Sie sind zudem die infrastrukturelle Basis für Cloud Computing, welches den Zugriff auf Server, Datenbankensysteme und Speicherkapazitäten radikal vereinfacht und eine große Bandbreite an Anwendungen, sogenannte Microservices bietet. Cloud Computing ist keine Technologieinnovation der letzten Jahre, sondern war bereits Teil der Grundkonzeption des Internet im Sinne einer Client-Server-Logik. Die Bedeutung des Cloud Computing in seiner heutigen Form liegt in der Zugänglichmachung und »Demokratisierung« immenser Speicher- und Rechenkapazitäten sowie der darauf aufsetzenden intelligenten Services für nahezu alle Anwenderklassen, vom Individualnutzer, über Kleinstbetriebe, den Mittelstand bis zur Großindustrie und staatlichen Verwaltungen.

Die Diskussion um 5G hat gezeigt, welche Bedeutung ein sicheres Telekommunikationsnetz für unsere Gesellschaft hat. Zur Gewährleistung eines Mindestmaßes an IT-Sicherheit hat der Gesetzgeber Kriterien formuliert, die von den Herstellern erfüllt werden müssen. So kann die Vertrauenswürdigkeit der Elemente sichergestellt werden, ohne einzelne Anbieter vom Markt auszuschließen.

Cloud Computing verändert den Aufbau von IT-Infrastrukturen in Unternehmen. Kosten können reduziert und eine höhere Flexibilität kann erreicht werden, da Dienste im tatsächlich notwendigen Umfang eingekauft und keine eigenen IT-Infrastrukturen mehr vorgehalten werden müssen. Auch das IT-Sicherheitsmanagement muss nicht länger vollständig inhouse beim Anwender angesiedelt werden, sondern ist Teil der via Cloud erbrachten Serviceleistung. Der IT-Sicherheits-Managementaufwand beim Anwender reduziert sich hierdurch erheblich. In Unternehmen und Organisationen bilden sich digitale Ökosysteme, in welchen Menschen, Unternehmen und Komponenten miteinander agieren. Viele dieser Ökosysteme von ihnen werden auch aus diesem Grund schon heute als kritische Infrastruktur eingestuft[13].

12 ↗https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/BSI_Kritisverordnung_Final.pdf

13 ↗https://creditreform-magazin.de/technik/kommentar-cloud-schluesseltechnologie-der-digitalisierung/

Im Zuge der digitalen Transformation sind in allen Sektoren der Wirtschaft und im öffentlichen Sektor Cloud-Infrastrukturen und Cloud-Anwendungen Grundlage neuer digitaler Geschäftsmodelle und digitaler Prozesse. Eigene europäische Cloud- und Dateninfrastrukturlösungen, die sowohl von den Funktionalitäten als auch von den Skalierungsmöglichkeiten her mit den Angeboten der aktuell verfügbaren Cloud- und Dateninfrastrukturen vergleichbar sind, existieren derzeit nicht. Marktanteile hochskalierbarer Infrastrukturen werden gegenwärtig fast ausschließlich von nicht-europäischen Anbietern gehalten. Diese Systeme werden oft als Hyperscaler[14] bezeichnet. Fragen der digitalen Souveränität und Datensouveränität in Bezug auf Cloud-Infrastrukturen in Deutschland und Europa müssen diesen Sachverhalt berücksichtigen.

Cloud-Infrastrukturen bilden außerdem die Grundlage für Dateninfrastrukturen und Datenmanagement. Dies zeigt wie eng verzahnt Cloud- und Dateninfrastrukturen mittlerweile sind und in Zukunft vermehrt sein werden. Digitale Geschäftsmodelle und digitale Prozesse basieren auf eben diesen Infrastrukturen.

Politik und Wirtschaft diskutieren derzeit unter dem Stichwort GAIA-X über die Schaffung einer europäischen Cloud und Dateninfrastruktur, die der Stärkung der digitalen Souveränität und Datensouveränität von Deutschland und Europa dienen soll. Dabei soll, unter Berücksichtigung der dezentralen Struktur der deutschen und europäischen IT-Landschaft, ein »virtueller Hyperscaler« geschaffen werden. Dabei sollen Anbieter von Cloud-Infrastrukturen und Cloud-Anwendungen sich auf freiwilliger Basis in einem gemeinsamen Netzwerk ein Ökosystem GAIA-X bilden. Kern von GAIA-X soll ein Regelwerk und eine Referenzarchitektur sein, die Datensouveränität für Anwender der aus dem GAIA-X Ökosystem angebotenen Anwendungen garantiert.

Handlungsempfehlungen an die Politik:

- Es müssen Rahmenbedingungen geschaffen werden, in denen die Entwicklung und Skalierung von Cloud- und Dateninfrastrukturen der Zukunft und darauf basierenden Geschäftsmodellen in Europa ermöglicht und erleichtert werden. Dies umfasst die leichtere Wachstumsfinanzierung von jungen und dynamischen Unternehmen, die weitere Stärkung des digitalen Binnenmarktes sowie den Abbau von regulatorischen Hürden.

- Deutschland hat mit Abstand die höchsten Strompreise für Industriekunden in Europa. Grund dafür sind vor allem die im Vergleich mit den Nachbarstaaten deutlich höheren Steuern, Abgaben und Netzentgelte. In den Niederlanden oder den nordischen Ländern betragen diese Kosten gerade einmal rund 15% des deutschen Wertes. Um die Chancengleichheit im europäischen Umfeld zu verbessern sollten Rechenzentren bei Netzentgelten, Steuern und Abgaben entlastet werden. Insbesondere eine Aufnahme von Rechenzentren in die Liste der Stromkos-

14 Als Hyperscaler werden in der Regel Architekturen und Systeme bezeichnet, die skalierbare und hochleistungsfähige Infrastrukturen für Cloud-Computing Anwendungen und zur Analyse von großen Datenmengen bereitstellen können. Dies geschieht auf der technischen Ebene durch eine effiziente Orchestrierung von großen Rechen-, Speicher- und Netzwerkressourcen. Im allgemeinen Sprachgebrauch werden auch die Anbieter, die diese Services anbieten, als Hyperscaler bezeichnet.

ten- oder handelsintensiven Branchen im Erneuerbare-Energien-Gesetz würde hier zu ausgewogeneren Verhältnissen führen.

- Es sollte für die Betreiber von Fernwärmenetzen regulatorische Anreize geben um Wärme aus Rechenzentren abzunehmen, solange dies wirtschaftlich und technisch sinnvoll ist. Dadurch würde erreicht, dass z. B. Hotels, Schwimmbäder oder andere Nutzer Abwärme aus Rechenzentren beziehen, anstatt wie bisher Primärenergie für Heizung und Warmwasser zu verwenden. Die gesetzlichen Rahmenbedingungen sollten so gestaltet werden, dass die Nutzung von Abwärme günstiger als die Nutzung der Primärenergie ist. Damit könnten Rechenzentren einen deutlichen Beitrag zur Verbesserung der CO_2-Bilanz bei der Wärmeversorgung leisten.

4.2.3 Hochleistungsrechner & Quantencomputer

Hoch- und Höchstleistungsrechnen (engl. High Performance Computing – HPC) ist für die Wettbewerbsfähigkeit von Wissenschaft und Wirtschaft unerlässlich. Ohne detaillierte Simulationen ist moderne Grundlagenforschung in der Energieforschung, den Material- und Lebenswissenschaften oder auch der Klimaforschung undenkbar. Das gilt auch für Schlüsselbereiche der deutschen und europäischen Wirtschaft.[15] Es herrscht deshalb bereits ein breites Verständnis darüber, dass Hoch- und Höchstleistungsrechner (HPC) eine Schlüsseltechnologie sind[16]. Ob elektronische Geräte, Autos, Flugzeuge, moderne Medikamente oder neuartige Operationsverfahren – sie alle basieren auf Erkenntnissen aus Simulationen. Ebenfalls relevant ist HPC für die Analyse großer Datenmengen (Big Data). Und auch für kleine und mittelständische Unternehmen wird HPC in Zukunft immer mehr an Bedeutung gewinnen. Im Sinne digitaler Souveränität sollten HPC-Systeme auch in Deutschland und Europa entworfen und hergestellt werden können und der Mittelstand sollte durch Informations- und Förderprogramme bei der Nutzung von HPC-Leistungen unterstützt werden.

Das Thema Quanten-Computing (QC) rückt von der Grundlagenforschung zunehmend in den Fokus tatsächlicher Anwendungen und wirtschaftlicher Relevanz. Neben der deutlich erhöhten Geschwindigkeit für Berechnungen in der Wissenschaft (z.B. für effizientere chemische Katalysatoren oder zur Entwicklung neuer Medikamente) werden Quantencomputer ihren disruptiven Charakter vor allem in solchen Industriebereichen ausspielen, in denen stark parallelisierte Probleme zu berechnen sind. Die Anwendungsbereiche reichen von einer Beschleunigung des Investmentbankings über großes Optimierungspotenzial im Bereich der Logistik bis hin zur Fähigkeit, die kryptographischen Schlüssel etablierter Verschlüsselungssysteme eklatant schneller zu brechen. Um einen frühzeitigen Zugang der deutschen und europäischen Industrie in diesem Zukunftsfeld zu gewährleisten und einen entsprechenden Wissens- und Erfahrungsschatz aufzubauen, sollte neben der bisher vor allem auf die Physik konzentrierten Förderung im

15 ↗https://www.bundesbericht-forschung-innovation.de/de/Digitalisierung-Schlusseltechnologien-1692.html

16 ↗https://www.bmbf.de/upload_filestore/pub/Quantentechnologien.pdf und ↗http://dipbt.bundestag.de/dip21/btd/19/070/1907036.pdf und ↗https://gauss-allianz.de/de/article/hpc_explained

Bereich Quantencomputing verstärkt auch Forschung und Entwicklung zu Anwendungen und Software gefördert werden.

Handlungsempfehlungen an die Politik:

- Die Nutzung von HPC-Ressourcen für die Industrie fördern: Die großen Potenziale für HPC-Anwendungen in der Wirtschaft werden noch nicht vollumfänglich ausgeschöpft. Große wie auch kleine und mittlere Unternehmen sollten daher gezielt bei der Nutzbarmachung von HPC-Ressourcen für ihre Zwecke unterstützt werden, um die Wettbewerbsfähigkeit der deutschen Wirtschaft zu sichern.

- Hard- und Software-Entwicklung gleichermaßen im Blick behalten: Im Bereich Entwicklung sollte neben der Hardware (vor allem Mikroelektronik) auch die Entwicklung von Softwaretechnologien sowohl für HPC als auch für QC unterstützt werden, mit gleich starkem Fokus auf beide Aspekte.

- Ausbildung von Fachkräften stärken: Neben der rein technologischen Entwicklung in den Bereichen HPC und QC wird auch die Ausbildung von Fachkräften im Bereich Programmierung, Algorithmen und Software zunehmend wichtiger. Insbesondere die Ausbildung von Programmierern und Software-Experten in neuen HPC-Bereichen wie dem Neuromorphen Computing sowie im QC-Bereich sollte entsprechend gefördert werden.

4.2.4 Mikro- und Nanoelektronik

Mikroelektronik ist die dominante Schlüsseltechnologie der Gegenwart, auf der alle anderen Entwicklungen, Systeme und Technologien im Bereich Digitalisierung basieren[17]. Nahezu sämtliche mit Strom betriebenen Geräte hängen heute von leistungsfähigen elektronischen Bauteilen auf Basis moderner Halbleiter ab. Viele Industriezweige sind durch die Halbleiterindustrie überhaupt erst entstanden (Computer, Internetwirtschaft, Mobiltelefonie, Kommunikationstechnik, ...), andere haben sich schon heute grundlegend verändert (Maschinen- und Fahrzeugbau, Logistik, medizinische Diagnostik, Energieerzeugung, ...). Auch Zukunftstechnologien wie z.B. Künstliche Intelligenz, Distributed Ledger Technologie und Quantencomputing sind ohne hochleistungsfähige Mikroelektronik nicht möglich. Der Erfolg am Markt basiert – vor allem für Systemindustrien und für die Servicebetreiber – sehr stark auf funktionierenden Wertschöpfungsketten bzw. -netzwerken, an deren Anfang oft Komponenten der Mikroelektronik stehen. Aber auch ständig leistungsfähigere Mikro- und Nanoelektronik und immer kleinere Strukturen und damit kostengünstigere Komponentenpreise ermöglichen immer mehr Anwendungen in der Breite. Die Hebelwirkung der Mikroelektronik für die Wertschöpfung in Systemindustrien darf nicht unterschätzt werden.

17 ↗http://dip21.bundestag.de/dip21/btd/18/077/1807729.pdf und ↗https://www.bmbf.de/de/elektroniksysteme-made-in-germany-850.html und ↗https://ec.europa.eu/programmes/horizon2020/en/area/key-enabling-technologies und ↗https://www.acatech.de/projekt/nanoelektronik-als-kuenftige-schluesseltechnologie-der-informations-und-kommunikationstechnik-in-deutschland/

Leider haben Deutschland und Europa in den vergangenen Jahrzehnten einige Kompetenzen in solchen Bereichen verloren, in denen Unternehmen in Asien und den USA die Marktführerschaft erlangt haben. Zu den Komponenten, die heute fast ausschließlich in Asien oder den USA entwickelt und produziert werden, gehören z.B. Prozessoren, Komponenten für Mobiltelefone und für 5G. Diese technologische Abhängigkeit auf dem Gebiet der Mikroelektronik führt zu Nachteilen für Wirtschaft und Wissenschaft, wenn hohe Zölle, Handelssanktionen oder gar Lieferstopps die Verfügbarkeit wichtiger Komponenten einschränken. Im Extremfall drohen hierzulande Produktionsstopps z.B. für Maschinen, Fahrzeuge und Flugzeuge, weil elektronische Komponenten nicht verfügbar sind. Und darüber hinaus stellt diese Abhängigkeit zunehmend ein großes Sicherheitsrisiko für Staat und Gesellschaft dar, wenn allgegenwärtige Kritische Infrastrukturen hiervon betroffen sind. Dennoch kann die Antwort Deutschlands und Europas darauf nicht sein, in Zukunft vollständig technologische Autonomie erlangen zu wollen. Vielmehr muss die Befähigung zu souveränem Handeln erhalten oder ggf. wieder hergestellt werden. Dazu gehört, dass alle Komponenten, die für das Funktionieren von wichtigen Infrastrukturen (z.B. für Wasser, Energie und Verkehr) kritisch sind, auf Sicherheit und Vertrauenswürdigkeit geprüft werden müssen – unabhängig von deren Herkunft. Wachsender Protektionismus und die Erhebung von Zöllen behindern zunehmend den Welthandel. Daher kann es ebenfalls sinnvoll sein, die deutsche und europäische Mikroelektronik gezielt da zu stärken, wo die zuverlässige Lieferung systemkritischer Komponenten zukünftig infrage gestellt ist.

Auch für die zukünftige Entwicklung z.B. des Quantencomputing und der Post-Quantum-Kryptografie kommt der Mikroelektronik eine wichtige Rolle zu. Sie wird diesen Technologien ebenso zum Durchbruch verhelfen, wie sie es kürzlich bei der Künstlichen Intelligenz getan hat (u.a. wegen verbesserter Sensorik zur Erhebung von Daten und großer Rechenpower). Neue Verschlüsselungstechnologien für Quantencomputer können nur mithilfe der Mikroelektronik entwickelt werden. Deutsche Unternehmen nehmen hier aktuelle eine führende Rolle ein. Diese sollte gesichert und ausgebaut werden.

Handlungsempfehlungen an die Politik:

- Die gerade gestartete Leitinitiative »Vertrauenswürdige Elektronik« des BMBF geht in die richtige Richtung und sollte unter Einbeziehung aller relevanten Stakeholder aus Wirtschaft und Wissenschaft konsequent fortgesetzt werden.

- Die Verfügbarkeit und Vertrauenswürdigkeit mikroelektronischer Komponenten, Systeme und Wertschöpfungsketten sollte zudem eine wichtige Säule aktueller Förderbekanntmachungen sowie des zukünftigen Rahmenprogrammes für Mikroelektronik ab 2021 werden.

4.3 Digitale Plattformen und Ökosysteme als Verbindung zwischen Infrastruktur und Anwendungen

Digitale Plattformen sind das Herzstück der digitalen Wirtschaft.[18] Aus und auf ihnen können ganze digitale Ökosysteme entwickelt werden. Sie fungieren dann als Schnittstellen in allen Märkten und Branchen: Digitale Produkte, Dienstleistungen und (industrielle) Produktion wachsen zusammen und werden über sogenannte Intermediäre (technisch durch Plattformen) zugänglich gemacht. Diese Intermediäre, z.B. Marktplätze, gab es in verschiedenen Formen auch in der Vergangenheit, doch seit einigen Jahren entstehen neue, vollkommen ortsungebundene Marktformen mit enormen Skalierungspotenzialen, großen Mehrwerten für ihre Teilnehmer, mehr Transparenz über das Marktangebot, bessere Auswahlmöglichkeiten, mehr Zugängen zu Kunden und insgesamt geringeren Such- und Transaktionskosten. Um seinen (industriellen) Wohlstand in Zukunft zu sichern, muss man daher in der Lage sein, neue industrienahe digitale Plattformen zu entwickeln und weltweit zu vermarkten. Knappe Ressourcen, politische Aufmerksamkeit und Förderinstrumente müssen konsequent da eingesetzt werden, wo zukünftige Wachstumsfelder entstehen, rückwärtsgerichtete Strategien helfen in diesem Kontext nicht weiter. In diesem Zusammenhang muss der Förderfokus auf diejenigen Technologiefelder gerichtet sein, die von strategischer Bedeutung sind und in denen Deutschland und Europa bereits über führende Kompetenzen und signifikante Kapazitäten verfügen. Außerdem wird eine chancenorientierte Regulierung auf deutscher und europäischer Ebene benötigt, um die Fähigkeit auch mittelständischer Unternehmen, digitale Plattformen zu entwickeln und möglichst weltweit zu vermarkten, zu stärken. Nur so kann Europa im internationalen Wettbewerb mithalten.[19]

Eine der führenden Referenzarchitekturen stellt die Initiative International Data Spaces (vormals Industrial Data Space). Sie zielt darauf ab, einen sicheren Datenraum zu schaffen, der Unternehmen verschiedener Branchen und aller Größen die souveräne Bewirtschaftung ihrer Datengüter ermöglicht. Die Vorarbeiten der IDS zur Datensouveränität sind deshalb auch Teil des Projekts GAIA-X und bieten eine Lösungsvariante für »data in use«.[20]

Angesichts der sich rapide verändernden Marktstrukturen, sowie schnellen technologischen Entwicklungen und Produkterneuerungen sind Teile der bisher angemessenen Regulierung nicht mehr zeitgemäß. Sie sind von statischen Betrachtungen, Snap-Shot Untersuchungen, sowie Miniaturvergleichen von Einzeldiensten und Produktsegmenten geprägt. Oft scheinen sich regulatorische Vorhaben gegenseitig zu blockieren oder gar zu widersprechen. In vielen Politikbereichen reflektiert die Gesetzgebung noch nicht ausreichend die Beschaffenheit, Komplexität und Besonderheiten der Plattformökonomie. Die Rahmenbedingungen entsprechen dadurch

18 ↗https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/new-evidence-for-the-power-of-digital-platforms

19 ↗https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digitale-souveraenitaet.pdf?__blob=publicationFile&v=3

20 ↗https://www.fraunhofer.de/de/forschung/fraunhofer-initiativen/international-data-spaces.html

nicht den Dynamiken und Anforderungen der wirtschaftlichen Entwicklung und bremsen Innovation in Geschäftsmodellen. Es bestehen zudem Rechtsunsicherheiten, die gerade für kleine und mittelständische Unternehmen geschäftsschädigende Folgen haben können. Rechts- und Planungssicherheit ist jedoch essentiell, um rechtskonformes Wirtschaften ohne unverhältnismäßigen Aufwand zu ermöglichen. Regulatorische Rahmenbedingungen müssen mit Veränderungen nicht nur Schritt halten, sondern diese vorantreiben um Innovation, Wohlstand und Wertschöpfung in Deutschland und Europa zu fördern.

Handlungsempfehlungen an die Politik:

- Ein institutionalisierter Mechanismus in Gesetzgebungsprozessen, z.B. ein Innovationscheck oder die Einbindung von Digitalexperten, kann Regulierung effektiver und angemessener machen. Die regulatorische Kompetenz sollte generell durch Heranziehen von sachkundigen Experten aus Wirtschaft und Wissenschaft gestärkt werden. Zusätzlich ist eine mindestens bundesweite Innovationsstrategie notwendig, die die Leitplanken für neue Regulierung festlegt.

- Grundsätzlich sollte der Fokus auf einer optimierten Anwendung bestehender Regulierung liegen. Bereits das Grünbuch Digitale Plattformen des Bundesministeriums für Wirtschaft und Energie stellte fest, dass der Beitrag Digitaler Plattformen zu Wirtschaftswachstum, Beschäftigung und Innovation beträchtlich ist und warnte vor unverhältnismäßiger Regulierung. Die Erfahrung der letzten Jahre zeigt jedoch, dass Deutschland nach wie vor durch derartige unflexible Regulierungsansätze digitale Wachstumspotenziale vergeben hat. Bevor also neue Regulierungen Innovationen ausbremsen, sollten bestehende Regulierungen regelmäßig überprüft werden. Diese Überprüfung sollte feststellen, in welchen Bereichen zusätzliche Regulierung überhaupt benötigt wird, in welchen Bereichen Deregulierungspotenziale entstanden sind und in welchen Bereichen bestehende Regulierung angepasst oder die Durchsetzung verbessert werden muss.

- Bei der regulativen Ausgestaltung darf es keinen »one size fits all« Ansatz geben – auch in der Plattformökonomie gilt das Fundamentalprinzip, gleiches gleich und ungleiches ungleich zu behandeln. Der Begriff digitale Plattform ist sehr weit und umfasst eine große Bandbreite an verschiedensten Geschäftsmodellen – aus Sicht des Bitkom lässt der politische Diskurs derzeit jedoch an Unterscheidungsgrad und differenzierter Wahrnehmung dieser Modelle vermissen.

- Dynamische Innovations-Anreizsysteme müssen aktiv gesetzt werden, beispielsweise als Pilotprojekte der öffentlichen Hand. Förderprogramme können Entwicklung, Aufbau und Betrieb digitaler Plattformen »made in Germany« vorantreiben, damit diese weltweit eingesetzt werden können. Es sollten daher mehr gezielte Anreize für die Zusammenarbeit öffentlicher und privater Stellen, sowie Kooperationserleichterungen im Allgemeinen, z.B. zur Schaffung von Datenplattformen, geboten werden.

- Um digitale Innovationen wie die Plattformökonomie zu ermöglichen, bedarf es einer stringenten bundespolitischen und europaweiten Innovationsstrategie. Harmonisierte Regulie-

rung auf EU-Ebene beschleunigt die Entwicklung, Einführung und Verbesserung innovativer Angebote in den europäischen Märkten. Damit diese harmonisierten Vorschriften vollumfassend greifen und funktionieren können, ist die Realisierung des digitalen Binnenmarkts essentiell.

4.4 Anwendungen & Software

4.4.1 Künstliche Intelligenz

Als Schlüsseltechnologie trägt Künstliche Intelligenz maßgeblich zum ökonomischen und gesamtgesellschaftlichen Fortschritt bei[21]. Nicht nur in Unternehmen, sondern auch im Öffentlichen Sektor und im Verbraucheralltag gewinnen KI-Anwendungen zunehmend an Relevanz. Aufgrund ihrer bereichsübergreifenden Einsatzmöglichkeiten spielen KI-Technologien in einer Vielzahl von Anwendungsbereichen eine signifikante Rolle und führen so zu einer breitgefächerten Innovationsdiffusion: Cyber- und IT-Security, Edge Computing, Cloud-Dienste, Telekommunikation, IoT-Anwendungen, Smart-City- und Mobilitätsdienste sowie der Gesundheitsbereich profitieren bereits heute von KI-Technologien. Um deren Potenziale zukünftig noch weiter skalieren zu können, sollte die Entwicklung und Anwendung von Künstlicher Intelligenz als Schlüsseltechnologie in signifikantem Umfang gefördert werden.

Die Absichtserklärung der Bundesrepublik Deutschland und der europäischen Union im globalen Wettstreit nicht den Anschluss zu verlieren, muss nun dringend operationalisiert werden. Insbesondere im Vergleich zu China und den USA, wo (daten-)ethische Aspekte anders gewichtet werden, wird die internationale Wettbewerbsfähigkeit Deutschlands und Europas als enorm wichtig erachtet. Jedoch ist es weder empfehlenswert noch sinnvoll, dem chinesischen oder US-amerikanischen Weg zu folgen – Deutschland muss und kann insbesondere im Verbund mit Europa souveräne Wege gehen.

Handlungsempfehlungen an die Politik:

- Es wird eine gezielte finanzielle Förderung von Forschungsprojekten sowie entsprechend notwendiger Forschungsinfrastruktur empfohlen.

- Daneben sind Investitionen in den kulturellen Wandel in Organisationen und Unternehmen sowie die Modernisierung von Aus- und Weiterbildung und das Anwerben und Halten von Fachkräften unumgänglich, um die Wettbewerbsfähigkeit zu halten.

21 ↗https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economy-September-2018.ashx

- Die Wahrung von Grundrechten der Bürgerinnen und Bürger, die Verbesserung ihrer Lebensumstände und die Erweiterung ihrer Handlungsoptionen sollen als unumstößliches Leitmotiv, die Entwicklung einer vertrauensvollen robusten (daten-)ethischen Standards als Ziel bei der Förderung von KI-Technologien gelten.

4.4.2 Sicherheitstechnologien

Die Verfügbarkeit digitaler Technologien wird immer mehr zum Rückgrat unserer Wirtschaft und Gesellschaft. Kritische Infrastrukturen wie Wasser-, Strom- und Transportsysteme sind auf die ununterbrochene Verfügbarkeit von miteinander verbundenen digitalen Komponenten und Systemen angewiesen. E-Payment, Cloud Computing, Machine-to-Machine-Kommunikation und viele andere Technologien können nur durch sichere Komponenten, Systeme und Lösungen zum Leben erweckt und ihr volles Potenzial ausschöpfen. IT-Sicherheit ist ein wesentliches und unverzichtbares Element für die erfolgreiche Implementierung und Akzeptanz neuer digitaler Technologien und Geschäftsmodelle. Fortschrittliche IT-Sicherheitstechnologien können außerdem Abhängigkeiten von menschlicher Expertise reduzieren.

Die europäische IT-Sicherheitswirtschaft ist technologisch innovativ, im internationalen Vergleich jedoch eher kleinteilig. Damit IT-Sicherheit »Made in Europe« auch mittel- und langfristig bestehen kann, brauchen die heimischen Anbieter eine stärkere Nachfrage in Europa, dazu können öffentlich geförderte Leuchtturmprojekte und die öffentliche Beschaffung genauso gehören, wie kundenseitige Steueranreize beim Einsatz solcher Produkte[22].

In diesem Segment sind auch die vertrauenswürdigen Kernkomponenten und zugehörigen Maßnahmen zu sehen, die benötigt werden, um die Kontrollhoheit über IT-Systeme zu erlangen. Einige dieser Kernkomponenten werden keine reinen Software-Lösungen sein, sondern eine vertrauenswürdige Abstützung auf Hardwareelementen mit überschaubarer Komplexität benötigen. Dementsprechend muss dieses Thema auch in der Schlüsseltechnologie der Mikro- und Nanoelektronik berücksichtigt werden.

Handlungsempfehlungen an die Politik:

- Für die Sicherheitstechnologien ist die öffentliche Hand ein wichtiger Kunde mit entsprechender Signalwirkung und entsprechenden Auswirkungen auf Entscheidungen bei Beschaffungen aus dem privaten und privatwirtschaftlichen Umfeld. So haben große Beschaffungsvorhaben im Bereich der zivilen Sicherheitsindustrie nicht nur Auswirkungen auf den nationalen Markt sondern unterstützen auch die Wettbewerbsfähigkeit der nationalen Sicherheitsindustrie, um im europäischen und internationalen Wettbewerb bestehen zu können. Sie sind somit auch Teil einer Wettbewerbs- und Innovationspolitik.

22 ↗https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheitsmarkt-in-deutschland-studie-2019.pdf?__blob=publicationFile&v=8

- Um die richtigen Schlüsse zu einer weiteren Verbesserung der Wettbewerbsfähigkeit ziehen zu können, ist es wichtig, die Großvorhaben im Bereich der Sicherheitstechnologien genau zu kennen, nationale Stärken im Bereich der Sicherheitstechnologien, der Sicherheitsdienstleister aber auch von IT-Sicherheit zu kennen und nach nationalen Stärken zu analysieren. U.E. liegt bisher keine umfassende Analyse vor, die diese Aspekte ausreichend würdigt. Die notwendigen Informationen sind auch nicht in Wissens- oder Informationssystemen gebündelt.

- Im Forschungsprogramm für zivile Sicherheit des BMBF werden weiterhin erhebliche Investitionen in Forschungs- und anwendungsnahe Innovationsvorhaben getätigt. Die Programme werden ebenso weiterhin intensiv von Forschungseinrichtungen, Universitäten und Hochschulen (u.a. wegen Förderquoten) genutzt. Der Output in Form von fertig entwickelten und somit einführbaren Produktinnovationen (und nicht nur Demoprojekten oder Prototypen) ist weiterhin zu verbessern und ggfs. mit Förderinstrumenten zu einer weitergehenden Markteinführung zu unterstützen.

4.4.3 Digitale Identitäten

Ob natürliche Person, Mobiltelefon, vernetzter Kühlschrank oder Fertigungsroboter in der Industrie 4.0 – alle haben eine oder sogar mehrere digitale Identitäten. Und je vernetzter die Welt, desto mehr Identitäten entstehen. In diesem Zusammenhang wird das verlässliche und sichere Management von Identitäten zur notwendigen Bedingung für die Digitale Souveränität.[23]

Den Markt für digitale Identitätslösungen dominieren bisher aber vor allem nicht-europäische Unternehmen, die durch Skalen- und Lock-in-Effekte die Nutzer an ihre Plattformen binden können. Bestehende staatliche Lösungen stoßen dagegen auf wenig Akzeptanz der Nutzer.[24] Das Ziel muss es daher sein, bestehende staatliche Lösungen sehr zeitnah zu optimieren. Der neue Personalausweis verfügt bereits über die notwendigen technischen Voraussetzungen. Aufgabe der Politik ist es, die fehlende Anwenderfreundlichkeit herzustellen und darüber hinaus die digitale Identität des hoheitlichen Dokuments weiterzuentwickeln und deren einfache Nutzung in mobilen Endgeräten, Apps und Plattformen möglich zu machen.

Die Verabschiedung der Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS) für elektronische Transaktionen im Binnenmarkt der Europäischen Union im Jahr 2014 war ein Meilenstein für die Regulierung elektronischer Vertrauensdienste und die Schaffung digitaler Souveränität in Europa. Die Verordnung liefert u.a. europaweit geltende Regelungen und Tools für die Bereiche elektronischer Identifizierung und elektronischer Vertrauensdienste. Der nächste Schritt muss es nun sein, mehr Verbindlichkeit in die Akzeptanz und Nutzung dieser

23 ↗https://identity.utexas.edu/research-projects/identity-threat-and-assessment-prediction-itap

24 ↗https://www.digitale-technologien.de/DT/Navigation/DE/Foerderaufrufe/Sichere_Digitale_Identitaeten/sichere_digitale_identitaeten.html

Dienste rund um sichere digitale Identitäten zu bringen, um europaweit Standards zu setzen, die wiederum Digitale Souveränität fördern.[25]

Handlungsempfehlungen an die Politik:

- Im Sinne der digitalen Souveränität ist der Staat aufgefordert, seinen Bürger parallel zum physischen Personalausweis auch im Digitalen einen modernen, nutzerfreundlichen Identitätsnachweis (Digitale ID) bereitzustellen, mit dem sich Bürger in möglichst vielen Anwendungen von Wirtschaft und Verwaltung sicher online ausweisen und rechtsverbindlich agieren können.

- Um die digitale Selbstbestimmung der Bürger zu ermöglichen, sollte der Staat im Rahmen der digitalen Daseinsvorsorge eine Basisinfrastruktur bereitstellen, die dem Bürger eine einfache Nutzung dieser staatlichen digitalen ID in Alltagsanwendungen ermöglicht.

- Die in der eIDAS-Verordnung enthaltenden und europaweit standardisierten Tools müssen im deutschen Recht und in Verordnungen verbindlich verankert werden. Nur wenn diese eIDAS-Standards gesetzlich vorgeschrieben sind, wird eine breite Anwendung in Wirtschaft und Verwaltung erfolgen.

4.4.4 Blockchain / Distributed Ledger Technologien

Blockchain ist eine Technologie zur gesicherten Verarbeitung und Prüfung von Datentransaktionen auf Basis eines verteilten Peer-To-Peer-Netzwerks. Blockchain ist Teil der Distributed Ledger Technologie-Familie. Sie nutzt kryptographische Verfahren, Konsensalgorithmen und rückwärtsverlinkte Blöcke, um Transaktionen praktisch unveränderbar zu machen. Die Anwendungsmöglichkeiten der Blockchain sind vielfältig – von den Bereichen Buchhaltung, Finanzen und Controlling über Logistik- und Lagerprozesse in der Lieferkette bis hin zu neuen Finanzierungsoptionen mit Kryptowährungen oder Token. Die Blockchain-Technologie hat das Potenzial, ganze Industriesektoren – insbesondere das Finanz-, Energie-, Logistik-, und Gesundheitswesen – zu revolutionieren. So sagen inzwischen 53% der befragten Unternehmen einer Deloitte-Studie, dass die Blockchain Technologie eine kritische Priorität für ihre Organisation darstellt. Branchenübergreifend sehen 83% sinnvolle Use Cases für den Einsatz der Technologie.[26] Auch in der öffentlichen Verwaltung, etwa für öffentliche Register, können Blockchain- und Distributed Ledger Technologien dazu beitragen, den Informationsaustausch zu verbessern und Prozesse zu beschleunigen.

Handlungsempfehlungen an die Politik:

25 ↗https://www.egovernment-computing.de/eidas-muss-gesetzlich-staerker-beruecksichtigt-werden-a-863442/

26 Vgl. Deloitte's 2019 Global Blockchain Survey, S.3. ↗https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf

- Technische wie rechtliche Herausforderungen verlangsamen bisher einen breiten Einsatz der Blockchain-Technologie. Insbesondere deshalb sollte die Entwicklung und Förderung von Forschungsprojekten, vor allem zu anwendungsbezogenen Geschäftsmodellen, politisch vorangetrieben werden. Ein niederschwelliger Zugang zu Fördermitteln für Blockchain Projekte ist eine sinnvolle Zukunftsinvestition.

- Zudem brauchen Blockchain-Geschäftsmodelle und -Startups staatliche Akzeptanz und Rechtssicherheit bei den regulatorischen Rahmenbedingungen. Die Bedingungen für Lösungen auf Blockchain-Basis im Zivil-, Steuer-, und Kapitalmarktrecht müssen klar sein, und Blockchain-Geschäftsmodelle, etwa die öffentliche Ausgabe von Kryptotoken zur Finanzierung und die Digitalisierung von Wertpapieren, müssen zügig ermöglicht werden.

- Zudem sollte der Staat mit eigenen Blockchain-Pilotprojekten in der Verwaltung, z.B. mit verteilten Registern für Stiftungen oder Hochschulzeugnisse, selbst vorangehen, dadurch Expertise aufbauen und Effizienzen schaffen.

- Auch die hiesige Aus- und Weiterbildung von Blockchain Experten ist für die Zukunft entscheidend. Die Technologie muss Teil von Studienangeboten mit informationstechnischem und wirtschaftlichem Bezug werden. Dazu braucht es die Schaffung und Förderung von entsprechenden Professuren.

- Durch rechtliche Klarstellungen und politische Flankierung könnte Deutschland seine gute Ausgangsposition im Bereich der Blockchain- und DLT-Technologien ausbauen und sich zu einem weltweit angesehenen »Blockchain-Hotspot« etablieren, der nicht nur Talente und Unternehmen anzieht, sondern globale Standards bei rechtlichen, technischen, und politischen Fragen setzt.

5 Fazit

5 Fazit

Digitale Souveränität ist die Möglichkeit zur digitalen Handlungs- und Gestaltungsfreiheit. Das bedeutet Mitgestaltungs- und Innovationsspielräume zu erhalten. Das heißt: Europa und Deutschland als starkes Mitgliedsland müssen dort technologische Kernkompetenzen weiter ausbauen, wo Expertise, Marktanteile und Innovationskraft vorhanden sind bzw. in der Zukunft entwickelt werden können. Gleichzeitig sollten sie in der Lage sein, Technologien und Dienstleistungen von vertrauenswürdigen internationalen Partnern erwerben zu können. Gerade durch diese komplementäre Stärke der Wirtschaftsräume können Innovations- und Effizienzgewinne entstehen, wenn die grenzüberschreitende Zusammenarbeit auf Augenhöhe und regelbasiert stattfindet. Um dies sicherzustellen, braucht es daher zum einen eine Initiative der Bundesregierung und der EU-Kommission zur fortlaufenden Bewertung der digitalen Souveränität Deutschlands und Europas unter Einbindung der unterschiedlichsten Perspektiven in der Form eines Multistakeholder Observatoriums. Nur so können Lücken identifiziert und gezielt geschlossen werden.

Deutschland und Europa müssen zum Erhalt ihrer digitalen Souveränität sicherstellen, dass Schlüsseltechnologien wie Mikroeletronik, 5G, KI, Blockchain und Quantencomputing nicht aus Europa abwandern oder durch Unternehmenszukäufe perspektivisch aus Europa verschwinden. Ein praktisch wirksamer digitaler Binnenmarkt muss daher unverändert intensiv politisch und regulativ vorangetrieben werden, um die europäische Nachfrage nach Schlüsseltechnologien zu aggregieren. Die Förderung von Technologien und Kompetenzfeldern mit Schlüsselfunktion muss sich dabei auf Felder konzentrieren, die für Europa und Deutschland die größte Hebelwirkung erzeugen. Ebenso müssen Deutschland und Europa dafür sorgen, dass Marktverzerrungen in Drittstaaten nicht dazu führen, dass die Wettbewerbsfähigkeit europäischer Unternehmen unterminiert wird. Dies würde die Digitale Souveränität Europas schwächen. Digitale Souveränität ist eine Facette der Sicherheitspolitik und muss als solche wahrgenommen werden, von Staat, Wirtschaft und Gesellschaft.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 1.900 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org