Bundesministerium
für Wirtschaft
und Energie

DE.DIGITAL

Schwerpunktstudie Digitale Souveränität

Bestandsaufnahme und Handlungsfelder

2021

bmwi.de

Impressum

Herausgeber
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Text und Redaktion
ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung
Dr. Mareike Seifried*, Prof. Dr. Irene Bertschek
*verantwortliche Autorin

unter Mitarbeit von
Patrick Breithaupt, Dr. Daniel Erdsiek, Manuel Lauer,
Dr. Thomas Niebel, Dr. Christian Rammer, Vincent Rost, Tim Schieber

Stand
Oktober 2021

Diese Publikation wird ausschließlich als Download angeboten.

Gestaltung
ZEW Mannheim

Bildnachweis
zf L / Gettyimages / Titel

Zentraler Bestellservice für Publikationen der Bundesregierung:
E-Mail: publikationen@bundesregierung.de
Telefon: 030 182722721
Bestellfax: 030 18102722721

Diese Publikation wird vom Bundesministerium für Wirtschaft und Energie im Rahmen der Öffentlichkeitsarbeit herausgegeben. Die Publikation wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Sie darf nicht zur Wahlwerbung politischer Parteien oder Gruppen eingesetzt werden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung, Ziele und zentrale Ergebnisse

Schon vor Ausbruch der Corona-Pandemie wurden die Rufe nach digitaler Souveränität im Sinne von mehr Unabhängigkeit und Selbstbestimmung in Bezug auf digitale Technologien in Deutschland und Europa lauter. Prominente Beispiele sind die Regulierung von Plattformmärkten aufgrund der monopolartigen Stellung großer Digitalunternehmen aus den USA und die Diskussion um eine Beteiligung des chinesischen Telekommunikationsausrüsters Huawei am deutschen 5G-Mobilfunknetz aufgrund von Sicherheitsbedenken. Während der Pandemie zeigte sich dann, dass der Zugang zu bestimmten Technologien in Krisenzeiten eingeschränkt ist und zu einer handlungsunfähigen Wirtschaft führen kann. So haben Lieferengpässe bei Halbleitern zu Kurzarbeit und Produktionsschwierigkeiten in der deutschen Industrie geführt (ntv.de 2021). Gleichzeitig wachsen geopolitische Handelskonflikte und der globale Wettbewerb um die Technologieführerschaft in Schlüsseltechnologien, wie etwa der Künstlichen Intelligenz oder der Quantentechnologie, intensiviert sich. So konkretisierte die chinesische Regierung jüngst ihr Ziel, dass die Volksrepublik bis 2049 eine weltweite Technologie- und Innovationsführerschaft einnehmen soll (Wietholtz 2021). Diese und viele weitere Beispiele zeigen, dass dem Erhalt und der Stärkung digitaler Souveränität in Zukunft eine Schlüsselrolle zukommt, um die Handlungsfähigkeit sowie Innovations- und Wettbewerbsfähigkeit der deutschen Wirtschaft sicherzustellen.

Trotz dieser vielen Debatten bleibt insgesamt unklar, was digitale Souveränität im Kern eigentlich bedeutet, wie die digitale Souveränität Deutschlands und Europas aktuell einzuschätzen ist und wie die deutsche Wirtschaft das Thema wahrnimmt und adressiert. Vor diesem Hintergrund untersucht die vorliegende Schwerpunktstudie das Konzept der „Digitalen Souveränität“ aus der Perspektive der Wirtschaft. Basierend auf einer umfassenden Literaturübersicht und einer repräsentativen Unternehmensbefragung ergeben sich interessante Einblicke aus Forschung und Praxis zum aktuellen Stand sowie zu möglichen Stellhebeln, die die digitale Souveränität der deutschen Wirtschaft erhalten und stärken können.

Auf Basis bestehender Literatur zeigt sich, dass für eine digital souveräne Wirtschaft zwei Aspekte von zentraler Bedeutung sind: Zum einen bedarf es der Verfügbarkeit von bzw. dem Zugang zu geeigneten digitalen Technologien und Daten. Dies wird sichergestellt, indem digitale Technologien entweder im eigenen Land produziert werden oder indem der Zugang zu diesen, auch in Krisenzeiten, abgesichert ist. Dafür sind Herstellungs- und Entwicklungskompetenzen von deutschen und europäischen Unternehmen in relevanten Technologiefeldern und Schlüsseltechnologien (Anbieterkompetenzen) von zentraler Bedeutung, um zum einen die Verfügbarkeit von Technologien zu gewährleisten und zum anderen die Digitalisierung der Wirtschaft im Sinne europäischer Rechts- und Wertevorstellungen mitzugestalten. Nichtsdestotrotz wird explizit keine vollständige Unabhängigkeit im Sinne einer Autarkie in allen (Technologie-)Bereichen und ausschließlich im eigenen Land produzierter Lösungen (d.h. Protektionismus) angestrebt. Vielmehr bedeutet digitale Souveränität, die digitale Transformation selbstbestimmt und frei zu gestalten, also die Möglichkeit dort mehr Unabhängigkeit zu erzielen, wo sie erwünscht ist. Zum anderen ist der souveräne – d.h. selbstbestimmte, sichere und reflektierte – Umgang mit digitalen Technologien und Daten eine Voraussetzung für eine digital souveräne Wirtschaft. Diese Handlungs- und Entscheidungskompetenzen im digitalen Raum

(Anwendungskompetenzen) beziehen sich auf die Fähigkeit, die Digitalisierung des eigenen Unternehmens selbstbestimmt, verantwortungsvoll und sicher zu gestalten, die Potenziale digitaler Technologien zu heben und Risiken zu reduzieren, demnach die unternehmenseigene Handlungs- und Wettbewerbsfähigkeit beizubehalten.

Um zu untersuchen, inwiefern dies in Europa und insbesondere in Deutschland gegeben ist, wurde basierend auf bestehenden Studien eine Bestandsaufnahme der gegenwärtigen Abhängigkeitsstrukturen und Anbieter- und Anwenderkompetenzen innerhalb von sechs zentralen Technologiefeldern durchgeführt[1]. Insgesamt zeigen sich in allen Technologiefeldern – (1) Hardware/Infrastruktur, (2) Software/Anwendungen, (3) Künstliche Intelligenz, (4) IT-Sicherheit, (5) Digitale Plattformen, (6) Daten[2] – teils erhebliche Abhängigkeiten zu nicht-europäischen Staaten, insbesondere den USA und China, aber auch bestehende Stärken in Bezug auf Anbieterkompetenzen, die es nun gilt zu erhalten und zu stärken. Auch anwenderseitig, d.h. bezogen auf den Umgang mit digitalen Technologien und Daten, zeigt sich Entwicklungspotenzial. Zwar wird deutlich, dass ein Teil der deutschen Unternehmen die wirtschaftlichen Chancen digitaler Technologien sowie deren Risiken erkannt hat, es aber noch an flächendeckenden Maßnahmen zur Reduzierung von Abhängigkeiten mangelt.

Eine repräsentative Unternehmensbefragung des ZEW Mannheim in der Informationswirtschaft und im Verarbeitenden Gewerbe bestätigt und erweitert dieses Bild. Zwar kennt nur jedes zweite Unternehmen den Begriff der digitalen Souveränität, jedoch messen die Unternehmen dem Thema langfristig eine hohe Bedeutung bei, sowohl für das eigene Unternehmen als auch für die deutsche Wirtschaft insgesamt. Insbesondere der Aspekt der Datenhoheit bzw. Datensouveränität wird von nahezu allen Unternehmen als besonders wichtig für das eigene Unternehmen angesehen. Zudem werden teils erhebliche Abhängigkeiten zu Nicht-EU-Anbietern wahrgenommen: Über 80 Prozent der Unternehmen fühlen sich in mindestens einem vorgegebenen Technologiefeld etwas oder stark abhängig von nicht-europäischen Anbietern. Dies gilt insbesondere für die Bereiche Hardware/Infrastruktur und Software/Anwendungen. Insgesamt 16 Prozent der Unternehmen in der Informationswirtschaft und 19 Prozent im Verarbeitenden Gewerbe geben sogar an, in allen vorgegebenen Technologiefeldern etwas oder stark abhängig von nicht-europäischen Anbietern zu sein. Als Gründe für bestehende Abhängigkeiten werden insbesondere die mangelnde Auswahl an Alternativen aus der Europäischen Union sowie die technologische Überlegenheit des aktuellen Anbieters benannt. Trotz der Bedeutung des Themas für Unternehmen plant derzeit nur ein geringer Anteil Maßnahmen durchzuführen, um bestehende Abhängigkeiten abzubauen. Eine Erklärung dafür wäre der Mangel an EU-Alternativen, so dass Unternehmen nicht wissen, wie Abhängigkeiten abgebaut werden können. Wenn allerdings Maßnahmen geplant sind, werden diese als „Chefsache“ behandelt, was erneut den hohen Stellenwert verdeutlicht.

Auf Basis der Literaturrecherche und der Unternehmensbefragung wurden fünf Handlungsfelder für Politik und Wirtschaft identifiziert:

1. Abbau von Informationsdefiziten und Sensibilisierung: Aufgrund der nicht flächendeckenden Bekanntheit des Konzepts der digitalen Souveränität und der geringen Verbreitung von gezielten Maßnahmen zur Reduzierung bestehender Abhängigkeiten ist es wichtig, z. B. über die Zentren im Netzwerk Mittelstand-Digital, die Informationslage zur digitalen Souveränität sowie zu möglichen Lösungsstrategien (z. B. Open-

[1] Aufgrund der Dynamik und der Breite des Themas kann der Bericht keinen Anspruch auf einen vollumfänglichen und tagesaktuellen Überblick leisten. Das Ziel ist vielmehr, Akzente zu setzen und interessierten Leserinnen und Lesern einen Einstieg in und Überblick über das Thema zu bieten.
[2] Obwohl Daten kein Technologiefeld im eigentlichen Sinne darstellen, wird der Zugriff auf und die Verarbeitung von Daten zur Vereinfachung unter den Technologiefeldern geführt.

Source-Software, GAIA-X) zu verbessern und für mögliche Risiken (z. B. IT-Sicherheit) zu sensibilisieren. Darüber hinaus sind die Stärkung des Vertrauens in und die Akzeptanz von digitalen Technologien seitens der Unternehmen und der Endnutzer essenziell, beispielsweise durch Gütesiegel.

2. Kontinuierliches Monitoring und Risikoanalyse: Aufgrund der Dynamik der Situation durch sich stetig verändernde Technologien und neue Anbieter sowie aufgrund wachsender geopolitischer Unsicherheiten sind das systematische Monitoring bestehender Kompetenzen und Abhängigkeiten sowie die Bewertung der Risiken von zentraler Bedeutung. Dies gilt sowohl auf staatlicher bzw. gesamtwirtschaftlicher Ebene als auch für Unternehmen.

3. Stärkung der Technologie- und Datensouveränität: Bestehende technologische Abhängigkeiten müssen abgebaut werden. Dafür gilt es auf bestehenden Stärken aufzubauen und insbesondere in Zukunftstechnologien wie Quantencomputer, Künstliche Intelligenz und in die IT-Sicherheit zu investieren. Ebenso sollten Projekte wie die europäische Cloud-und Daten-Infrastruktur (GAIA-X) zeitnah umgesetzt werden. Darüber hinaus wird es nicht gelingen, digitale Souveränität zu erhalten und zu stärken, wenn bestimmte Rahmenbedingungen – Innovationsumfeld, regulatorischer Rahmen und gesellschaftliche Faktoren – nicht gegeben sind.

4. Aufbau von digitalen Kompetenzen: Die Verfügbarkeit von und der Zugang zu grundlegenden und fortgeschrittenen digitalen Kompetenzen in einer Gesellschaft sind essenziell für den Erhalt und die Stärkung der digitalen Souveränität. Auch wenn der Ruf nach einer intensiveren Förderung von digitalen Kompetenzen und Maßnahmen zur Reduzierung des Fachkräftemangels seit einigen Jahren besteht, zeigt sich in diversen Studien, dass weiter enormer Handlungsbedarf besteht. Hier gilt es, digitale Technologien auch als Chance zu begreifen, etwa kreative digitale Weiterbildungsformate zu entwickeln.

5. Agiles und kooperatives Handeln: Digitale Souveränität ist kein statischer Zustand, der erreicht werden kann, sondern einer fortwährenden Dynamik unterworfen, weshalb die Situation stetig neu bewertet und der Kurs gegebenenfalls angepasst werden muss. Dies impliziert, dass agiles Handeln auf allen Ebenen wichtig und zu fördern ist. Gleichzeitig hat das kooperative Vorgehen und Bündeln von Kompetenzen, etwa auf europäischer Ebene oder über Unternehmensgrenzen hinweg, einen hohen Stellenwert im Kontext der digitalen Souveränität.

Insgesamt zeigt sich, dass der Erhalt und die Stärkung digitaler Souveränität eine gesamtgesellschaftliche Aufgabe darstellt und durch die Handlungen einer Vielzahl an Akteuren beeinflusst wird, welche es zu koordinieren und harmonisieren gilt. Des Weiteren wird deutlich, dass digitale Souveränität ein heterogenes und dynamisches Konstrukt ist und somit einer kontinuierlichen Beobachtung und Anpassung von Maßnahmen bedarf.

2. Aktueller Stand der Forschung

2.1 Stand der Begriffsdefinition

2.1.1 Definition und Abgrenzung von „Souveränität“

Souveränität bedeutet wörtlich ‚darüber befindlich‘ oder ‚überlegen‘ (aus dem Französischen: souveraineté; mittellateinisch superanus) und kann verschiedenen Handlungsebenen zugeschrieben werden. Bezogen auf Individuen bedeutet souverän zu sein, aufgrund eigener Fähigkeiten sicher und überlegen auftreten und handeln zu können. Ein Staat oder dessen Regierung ist souverän, wenn es die staatlichen Hoheitsrechte ausübt oder anders gesagt, die Staatsgewalt innehält (Duden 2021). Auf staatlicher Ebene unterscheidet man weiter zwischen *innerer* und *äußerer* Souveränität (Schiefdecker und March 2021). Die grundsätzliche Unabhängigkeit eines Staates von anderen Staaten markiert die Souveränität nach außen und die Selbstbestimmtheit in Fragen der eigenen staatlichen Gestaltung wie etwa Art der Regierung, das Rechtssystem und die Gesellschaftsordnung die Souveränität nach innen (Zandonella 2005). Im politikwissenschaftlichen Diskurs wird der Souveränitätsbegriff teilweise noch differenzierter betrachtet und zwischen vier Deutungsmöglichkeiten unterschieden (Krasner 2001): Neben der zuvor genannten inneren und äußeren Souveränität besteht die *Interdependenz-Souveränität*. Sie beschreibt eine effektive Kontrolle über grenzüberschreitende Austauschprozesse. Die *international rechtliche Souveränität* als vierte Möglichkeit weist auf die wechselseitige rechtliche Anerkennung als souveräner Staat durch andere Staaten hin.

Der Begriff Souveränität beinhaltet somit verschiedene Aspekte und Blickrichtungen, die nicht notwendigerweise miteinander einhergehen müssen (Thomson 1997). Demnach kann ein Staat durchaus rechtlich international anerkannt und in diesem Sinne souverän sein, aber gleichzeitig eine mangelnde innere Souveränität aufweisen. Zudem kann die Souveränität eines Staates zwar rechtlich und formell vorhanden, aber wegen Abhängigkeiten zu anderen Staaten faktisch begrenzt sein. Es zeigt sich zum einen die Vielschichtigkeit und Ambiguität des Souveränitätsbegriffs und zum anderen die Schwierigkeit, Souveränität empirisch zu erfassen. Denn die „vollständige“ Souveränität eines Akteurs lässt sich erst in einer Gesamtbetrachtung einzelner Faktoren bestimmen. Das bedeutet auch, dass Souveränität keiner Eins-Null-Logik folgt, sondern graduelle Ausprägungen zulässt (VDE 2020; BMWi 2017). So kann ein Akteur in Teilbereichen bzw. nur in bestimmten Aspekten oder aber über alle Dimensionen hinweg souverän sein, demnach wird auch von einer niedrigen bis hoch ausgeprägten digitalen Souveränität gesprochen (vgl. BMWi 2017).

Des Weiteren wird in der gegenwärtigen Diskussion oftmals darauf verwiesen, dass sich Souveränität einerseits von *Autarkie* und andererseits von Fremdbestimmung (als Gegenteil von *Autonomie*) abgrenzt (Bitkom 2015). Obwohl staatliche Souveränität also mit wirtschaftlicher und politischer Unabhängigkeit verbunden ist, ist sie nicht mit Autarkie und Autonomie gleichzusetzen.

Autarkie ist die *wirtschaftliche* Unabhängigkeit einer Einheit, wie etwa einer Region oder eines Staates, durch die vollständige oder teilweise Selbstversorgung mit Gütern und Dienstleistungen. Autarkie beschreibt demnach einen Zustand, in dem ein Staat nicht mehr auf die Einfuhr oder die Ausfuhr von Waren angewiesen

ist und komplett auf auswärtige finanzielle Transaktionen verzichten kann, in diesem Sinne also vollständige wirtschaftliche Selbständigkeit erlangt hat. Jedoch ist Autarkie im Sinne einer (vollständigen) Unabhängigkeit nicht zwingend mit Souveränität gleichzusetzen. Denn die Souveränität eines Staates leidet bei gleichzeitiger Autarkie, wenn das Gemeinwohl oder die Funktionsfähigkeit im Inneren dadurch eingeschränkt wird (Draghi 2019). Im Umkehrschluss kann ein Staat bzw. ein Akteur auch bei unvollständiger Unabhängigkeit souverän sein. So geht es im Kontext der Souveränität immer auch um ein Abwägen, ein „Abhängigkeitsmanagement", und die *bewusste* Entscheidung für oder gegen etwas sowie die kontinuierliche Neubewertung gegenwärtiger Abhängigkeitsbeziehungen. In diesem Sinne ist der Entscheidungsträger „überlegen", weil er über der Entscheidung steht und diese selber bewusst trifft, also im eigentlichen Wortsinn souverän.

Autonomie (auch Eigengesetzlichkeit, Selbstständigkeit) bezieht sich auf die *politische* Unabhängigkeit und bezeichnet den Zustand der Selbstbestimmung, Selbstverwaltung oder Entscheidungs- bzw. Handlungsfreiheit. Ihr Gegenteil ist die Heteronomie, die Fremdbestimmung. Der Unterschied zur Souveränität zeigt sich bei der Betrachtung autonomer Gebiete. Diese können sich nach innen selbst verwalten und besitzen eigene Gesetzgebungsorgane und politische Strukturen. Sie unterliegen aber auch der Gesetzgebung des übergeordneten Staates und werden außen- und sicherheitspolitisch von diesem vertreten. In diesem Sinne sind sie nicht souverän. So ist Autonomie zwar ein Teilaspekt der Souveränität, jedoch bedarf es für eine „vollständige" Souveränität auch die Vertretung, Durchsetzungsfähigkeit und Anerkennung bzw. Gleichstellung nach außen. Nichtsdestotrotz ist sowohl Autonomie als auch Souveränität als Gegenteil von Fremdbestimmung zu verstehen. Autonomie und Heteronomie sind zudem verwandt mit dem Begriff der **Hegemonie**, der Vorherrschaft oder Vormachtstellung, die ein Staat gegenüber einem oder mehreren anderen Staaten besitzt. In diesem Sinne ist die Souveränität anderer Staaten eingeschränkt, weil sie die Gleichheit der Staaten verletzt. Die Abgrenzung zwischen aktiver Gestaltungsmacht als positiv konnotiertem Begriff und Hegemonie kann dabei als fließend betrachtet werden.

Insgesamt zeigen sich die Vielschichtigkeit und die unterschiedlichen Verwendungsmöglichkeiten des Souveränitätsbegriffs und bedingt dadurch auch die Schwierigkeit, Souveränität zu bestimmen und empirisch zu erfassen.

2.1.2 Digitale Souveränität der Wirtschaft

Aufgrund der dominierenden Stellung der USA bzw. amerikanischer Digitalunternehmen bei der Gestaltung der Digitalisierung im europäischen Raum und zunehmender Abhängigkeiten von nicht-europäischen Anbietern von digitalen Technologien wurde der Ruf nach einem eigenen, europäischen Weg bei der Gestaltung des digitalen Wandels in den vergangenen Jahren lauter. Ansonsten besteht die Gefahr, dass „die Digitalstrategien anderer aufstrebender Wirtschaftsregionen, der Aufbau neuer Internetkonzerne und zunehmende strategische Aufkäufe europäischer Unternehmen die Abhängigkeit Europas verstärken" (BMWi 2018, S. 2). Vor diesem Hintergrund wird auch der Souveränitätsbegriff wieder vermehrt in Wissenschaft und Politik diskutiert (Krasner 2001; Thiel 2019; Brozus 2014) und es entstand eine Debatte um den Erhalt und die Stärkung „digitaler Souveränität", eine „spezifisch digitale Form der Souveränität" (Thiel 2019). Aufgrund der aktuellen Relevanz des Themas bei gleichzeitiger Unschärfe des Begriffs befasst sich eine Vielzahl an Impulspapieren mit der theoretischen Diskussion von digitaler Souveränität. Jedoch bauen diese Studien zu einem Großteil nicht explizit aufeinander auf, so dass bisher noch keine allgemein anerkannte Definition existiert. Häufigere Verwendung finden sowohl eine Definition von Bitkom (2015) als auch den Veröffentlichungen der Fokusgruppen des Digital-Gipfels. Insgesamt wurden 19 Papiere von Ministerien,

Forschungsinstituten, Verbänden und weiteren Institutionen identifiziert, die sich im Kern mit digitaler Souveränität befassen. Im Anhang befindet sich eine Tabelle mit den darin verwendeten Definitionen, die einen Überblick verschaffen soll. Im Rahmen dieser Studie wird digitale Souveränität wie folgt definiert (BMWi 2018):

Souveränität bezeichnet die Möglichkeit zur unabhängigen Selbstbestimmung von Staaten, Organisationen oder Individuen. Digitale Souveränität ist heute ein wichtiger Teilaspekt allgemeiner Souveränität, der die Fähigkeit zur unabhängigen Selbstbestimmung in Bezug auf die Nutzung und Gestaltung digitaler Systeme selbst, der darin erzeugten und gespeicherten Daten sowie der damit abgebildeten Prozesse umfasst.

Das übergeordnete Ziel einer digital souveränen Wirtschaft ist die Sicherstellung ihrer Handlungsfähigkeit und Zukunftsfähigkeit, d.h. Wettbewerbs- und Innovationsfähigkeit. Dafür sind zwei Aspekte von zentraler Bedeutung (vgl. oben genannte Definition und Kagermann et al. 2021): Die Verfügbarkeit von bzw. der Zugang zu Technologien und Daten und der selbstbestimmte, reflektierte, verantwortungsvolle und sichere Umgang mit bzw. die Nutzung von digitalen Technologien und Daten.

Zunächst ist die **Verfügbarkeit von bzw. der Zugang** zu geeigneten digitalen Technologien und Daten von zentraler Bedeutung (Kagermann et al. 2021; Edler et al. 2020; VDE 2020). Dies wird sichergestellt, indem digitale Technologien entweder selbst geschaffen (d.h. im eigenen Land produziert) werden oder indem der Zugang zu diesen, auch in Krisenzeiten, abgesichert ist (Edler et al. 2020; Kagermann et al. 2021). Dabei besteht ein breiter Konsens, dass eine vollständige Unabhängigkeit im Sinne einer Autarkie in allen (Technologie-)Bereichen und ausschließlich im eigenen Land produzierter Lösungen (d.h. Protektionismus) nicht erstrebenswert ist. Vielmehr wird digitale Souveränität als Gestaltungsfreiheit interpretiert, d.h. die Möglichkeit mehr Unabhängigkeit zu erzielen, wo sie erwünscht ist, z. B. in Bereichen, die die nationale Sicherheit und den Schutz von Wirtschafts- und Personendaten betreffen (Kagermann et al. 2021). Dies impliziert gleichzeitig einen Gestaltungswillen, d.h. selbst eine Spitzenposition in Bezug auf digitale Technologien einnehmen zu wollen und die digitale Transformation nach europäischen Wertevorstellungen zu gestalten sowie Innovationen durch freien, regelbasierten Handel zu skalieren und global anzubieten (vgl. Koch et al. 2021). Nichtsdestotrotz beinhaltet digitale Souveränität bis zu einem gewissen Maße auch eine Abkehr vom Globalisierungstrend und internationaler Arbeitsteilung, wenn bestimmte Technologien, wie etwa Mikrochips, zumindest teilweise (wieder) in der Europäischen Union produziert werden.

Eine wesentliche Voraussetzung dafür ist, dass deutsche bzw. europäische Unternehmen **Herstellungs- und Entwicklungskompetenzen** in relevanten Technologiefeldern und Schlüsseltechnologien besitzen (*Anbieterkompetenzen*). Dadurch wird die Wahlfreiheit am Markt erhöht und zugleich ein Angebot geschaffen, welches den europäischen Rechts- und Wertevorstellungen entspricht. Gleichzeitig können europäische Angebote als Gegengewicht zu bestehenden nicht-europäischen Anbietern wirken. Dazu zählt im Sinne des oben genannten Gestaltungswillens auch, dass Unternehmen aus Deutschland und der EU im globalen Kontext aktiv auftreten und an der Gestaltung der digitalen Transformation bzw. Gestaltung des digitalen Raums gleichberechtigt und selbstbestimmt mitwirken. Dies bedeutet, selbst eine Vorreiterrolle in Zukunftstechnologien einzunehmen und technologische Standards mitzugestalten, sich aber ebenso für europäischen Datenschutz, Offenheit, Transparenz und ein freies, offenes, globales und sicheres Internet einzusetzen (Gesellschaft für Informatik 2020; BMI 2016).

Beim Zugang zu Technologien, die nicht in Deutschland oder der EU hergestellt werden (können), müssen die Versorgungsrisiken – bedingt durch wirtschaftliche, politische oder sonstige Gründe (z. B. Klimaereignisse, politische Instabilität, Pandemie) – beobachtet und reduziert werden (Edler et al. 2020). Das Versorgungsrisiko kann zum einen durch das Bereitstehen technologischer Alternativen (Substitute) reduziert werden. Substitute wirken zudem disziplinierend auf die Ausübung von Marktmacht im Falle einer Angebotskonzentration. Zum anderen helfen stabile Partnerschaften und die Vermeidung einseitiger Abhängigkeiten zu anderen Ländern auf staatlicher Ebene (Edler et al. 2020). Im Zusammenhang mit der wirtschaftlichen Unabhängigkeit von ausländischen Anbietern wird vermehrt der Begriff **Technologiesouveränität** verwendet, „[...]die Fähigkeit eines Staates oder Staatenbundes, die Technologie, die er für sich als kritisch für Wohlfahrt, Wettbewerbsfähigkeit und staatliche Handlungsfähigkeit definiert, selbst vorzuhalten und weiterentwickeln zu können, oder ohne einseitige strukturelle Abhängigkeiten von anderen Wirtschaftsräumen beziehen zu können“ (Edler et al. 2020, S. 2). Teilweise werden technologische und digitale Souveränität in der Diskussion synonym verwendet (Pohle 2020), teilweise jedoch auch als Teilaspekt des jeweils anderen Begriffs, z. B. technologische Souveränität als Teilaspekt von digitaler Souveränität (Gesellschaft für Informatik 2020) oder andersrum (VDE 2020; Wittpahl 2017). Im Verständnis dieser Studie bezieht sich technologische Souveränität auf einen Teilaspekt einer allgemeinen digitalen Souveränität und verfolgt vor allem das Ziel der Sicherstellung des Zugangs zu und der Verfügbarkeit von digitalen Technologien auf staatlicher Ebene.

Auf Unternehmensebene zeigen sich technologische Abhängigkeiten von einzelnen Anbietern durch **hohe Wechselkosten und sonstige Wechselbarrieren, den sogenannten Lock-in-Effekt**. Nicht mehr von einer technischen Lösung auf eine andere wechseln zu können, schränkt dabei die Handlungsfähigkeit eines Unternehmens stark ein und somit auch die digitale Souveränität. Da dies im Umkehrschluss nicht bedeutet, dass deutsche Unternehmen komplett autark und mit Insellösungen wirtschaften sollten, da auch dies die Handlungsfähigkeit einschränkt, stellt sich die Frage, wie ein erstrebenswerter Soll-Zustand aussieht. Ob der Eigenbetrieb bzw. die Eigenentwicklung („make“, z. B. ein eigenes Rechenzentrum) oder eine bestehende Lösung am Markt („buy“ – z. B. eine bestimmte Cloud-Lösung) eingesetzt wird, kann dabei nur eine Einzelfallentscheidung bleiben. So existiert nicht die eine, für alle Anwender und alle Einsatzfälle optimale Lösung, sondern es bleibt eine individuelle Entscheidung und Abwägen von Aufwand und Risiken (Goldacker 2017).

Auch wenn eine bestehende Lösung am Markt bezogen wird, können bestimmte technische Eigenschaften wie Modularität, Interoperabilität und offene Schnittstellen die Abhängigkeit von einzelnen Anbietern oder Partnern reduzieren (BMWi 2018). Dazu zählt auch die Nutzung von Open-Source-Angeboten, bei denen der Quellcode eingesehen und genutzt werden kann, sowie von etablierten und offenen Standards (Gesellschaft für Informatik 2020). Anwenderseitig kann die Abhängigkeit von einzelnen Anbietern auch durch bestimmte Strategien reduziert werden, z. B. Multi-Sourcing, also den Bezug von Komponenten von mehreren Anbietern, oder etwa in der Vertragsgestaltung, z. B. das Vermeiden von langfristigen Verträgen. Zugleich wäre das Aufsetzen einer hybriden IT, bei der selbst erbrachte Leistungen („make“) und von Dienstleistern in beliebiger Form bereitgestellte Services („buy“) kombiniert werden, eine Möglichkeit, die Unabhängigkeit von einzelnen Anbietern zu erhöhen. Insgesamt geht es für Unternehmen also um ein Bewusstsein über technologische Abhängigkeiten, ein Abwägen der Risiken sowie die Entwicklung und Umsetzung von Lösungsansätzen, um bestimmte Abhängigkeiten zu reduzieren und zu vermeiden.

In der Diskussion um digitale Souveränität hat sich auch der Begriff der **Datensouveränität** als eigenständiges Konzept und Teilgebiet der digitalen Souveränität etabliert. Datensouveränität bezieht sich auf eine

Sicherstellung von Datenbereitstellung und -zugang, eine verantwortungsvolle Datennutzung zur Ausschöpfung von Innovationspotenzialen sowie das Bestehen von Datenkompetenzen und die Etablierung einer Datenkultur (Gesellschaft für Informatik 2020). Nach dem Papier des Digital-Gipfels (BMWi 2019) ist Datensouveränität gewährleistet, „wenn die Verfügungs- und Nutzungsrechte an Daten, das heißt der Zugriff, der Transfer, die Verarbeitung und die Analyse auf jeder Wertschöpfungsebene ein selbstbestimmtes Handeln gewährleisten. Dies schließt etwa die Möglichkeit ein, auf vertraglicher Grundlage Dritte vom Zugriff auf Daten ein- oder auszuschließen, die Verknüpfung unterschiedlicher Daten sowie die Verarbeitung und Analyse von Daten zu ermöglichen oder zu unterbinden“ (S. 11). Des Weiteren findet auch der Begriff **Plattformsouveränität** teilweise Verwendung (BMWi 2017), wodurch sich zeigt, dass Souveränität in unterschiedlichen Teilbereichen (hier Technologiefeldern) untersucht bzw. bestimmt werden kann.

Aus der Beschreibung von Datensouveränität wird auch deutlich, dass nicht nur die uneingeschränkte Verfügbarkeit von digitalen Technologien und Daten durch mehr Unabhängigkeit eine wesentliche Voraussetzung für eine digitale Souveränität darstellt, sondern auch der souveräne – d.h. selbstbestimmte, sichere und reflektierte – **Umgang mit digitalen Technologien** (Goldacker 2017; BMWi 2015). Somit sind **Anwendungskompetenzen** innerhalb von Unternehmen in Bezug auf digitale Technologien – also Fähigkeiten, die Digitalisierung des eigenen Unternehmens souverän zu gestalten – ebenso eine Voraussetzung für eine hohe digitale Souveränität.

Hier wird im Wesentlichen zwischen **Entscheidungs- und Handlungskompetenzen** unterschieden. Unter Entscheidungskompetenzen im Kontext der digitalen Souveränität versteht man die Fähigkeit, die Leistungsfähigkeit und Vertrauenswürdigkeit von Komponenten und Lösungen am Markt verstehen, beurteilen und prüfen zu können (Bitkom 2015). Dies beinhaltet auch, dass Entscheidungsträger in Unternehmen über grundlegende und teilweise auch fortgeschrittene digitale Kompetenzen verfügen müssen. Handlungskompetenzen beziehen sich zunächst auf den effektiven Einsatz von digitalen Technologien zur Steigerung der eigenen Wettbewerbs- und Innovationsfähigkeit (z. B. Datenkompetenz). Auch das Erkennen und die kontinuierliche Neubewertung von technologischen Abhängigkeiten sowie der Planung und Durchführung von Maßnahmen zur Reduzierung dieser Abhängigkeiten zählen zu den notwendigen Kompetenzen. Zuletzt ist der verantwortungsvolle, sichere und reflektierte Einsatz digitaler Technologien Voraussetzung einer digitalen Souveränität, d.h. Risiken erkennen, Folgen abschätzen und IT-Sicherheit gewährleisten können. Dafür werden wiederum Technikkompetenzen benötigt, also ein Verständnis der Funktionsfähigkeit von Technologien, und folglich die Fähigkeit, die Nutzung von Technologien auch kritisch zu hinterfragen (vgl. Strubell et al. 2019). Gleichzeitig bedeutet digitale Souveränität im Unternehmenskontext, eigene unternehmerische Pflichten zum Schutz der digitalen Souveränität von Verbrauchern und Arbeitnehmern wahrzunehmen und in diesem Sinne die digitale Transformation im Sinne der europäischen Werte mitzugestalten (Sachverständigenrats für Verbraucherfragen 2017). Beispiele wären die Sicherstellung von Transparenz und Nachvollziehbarkeit bei der Nutzung von Algorithmen im Recruiting sowie der Einhaltung von Datenschutzvorgaben bei der Verarbeitung von Personaldaten.

Um die digitale Souveränität der deutschen Wirtschaft auf **Anbieter- und Anwenderseite** zu untersuchen, wird im folgenden Kapitel auf Basis bestehender Literatur eine Bestandsaufnahme der zwei Kernelemente einer hohen digitalen Souveränität – des Zugangs zu Technologien und Daten und des Umgangs mit Technologien und Daten – durchgeführt. Im Kern geht es dabei um eine Bestandsaufnahme derzeitiger Abhängigkeitsstrukturen und eine Bewertung, in welchen Technologiefeldern Deutschland und Europa eigene Entwicklungs- und Herstellungskompetenzen (Anbieterkompetenzen) bzw. Anwendungskompetenzen

besitzen oder auf- und ausbauen sollte. Da es zudem gewisser Rahmenbedingungen bedarf, um eine digitale Souveränität zu erreichen bzw. zu erhalten, erfolgt auch hierzu eine Bestandsaufnahme. Der Fokus liegt dabei auf den Bereichen Kompetenzentwicklung, Innovationsumfeld, regulatorischer Rahmen und gesellschaftliche Faktoren.

2.2 Bestandsaufnahme: Digitale Souveränität und Rahmenbedingungen

2.2.1 Identifikation und Bewertung von Technologiefeldern

In der Untersuchung digitaler Souveränität ist es sinnvoll, die Souveränität differenziert, also getrennt nach Technologiefeldern zu betrachten. Dafür müssen zunächst Technologiefelder und Schlüsseltechnologien identifiziert und dahingehend bewertet werden, welche Bedeutung sie zum Erhalt bzw. der Steigerung der digitalen Souveränität der deutschen Wirtschaft haben. In diesem Zusammenhang wird betont, dass nicht pauschal technologische Aktivitäten ausgeweitet werden sollten, d.h. in allen Bereichen, in denen die eigene internationale Wettbewerbsfähigkeit als zu gering oder ausbaufähig wahrgenommen wird. Souveränität sollte vielmehr in ausgewählten Bereichen gesucht werden, die nach zu definierenden Kriterien als besonders zentral angesehen werden (Edler et al. 2020).

Eine Reihe von Studien hat sich bereits mit der Identifikation und Bewertung befasst und diverse Technologien bzw. Technologiefelder identifiziert. Kagermann et al. (2021) entwickeln auf Basis von Experteninterviews ein Schichtenmodell mit acht aufeinander aufbauenden Ebenen der Digitalen Souveränität. Diese acht Ebenen beziehen sich auf die folgenden Technologiefelder: Rohmaterialien und Vorprodukte, Komponenten, Kommunikationsinfrastruktur, Infrastructure-as-a-Service, Platform-as-a-Service, Europäische Datenräume, Softwaretechnologien und Europäisches Rechts- und Wertesystem (u.a. Cybersecurity). Auch eine Studie im Auftrag des BMWi (2017) identifiziert sieben Technologiefelder, die als besonders relevant im Zusammenhang mit der digitalen Souveränität erachtet werden: Software-Architekturen und -Anwendungen, Hardware-Architekturen und Infrastruktur, Umwelt-Technik-Interaktion, Management von Daten, Anwendungen und Diensten, Data Analytics/Machine Learning, IT-Sicherheit und Entwicklung digitaler Technologien. Die Identifikation erfolgt auf Basis einer Literaturrecherche, einer Unternehmensbefragung und der Analyse von weiteren Datenquellen. Die Kriterien für die Bewertung einer Liste an Technologiefeldern erfolgte auf der Basis von vier Kriterien: Zukunftsfähigkeit, Substituierbarkeit, Interoperabilität und strategische Bedeutung des jeweiligen Technologiefeldes. Der Verband der Elektrotechnik (2020) hat wiederum acht Technologiefelder festgelegt, in denen eine Technologiesouveränität erreicht werden sollte: Informations- und Kommunikationstechnik; Mikroelektronik; Software; KI; Digitale Plattformen; Energie; Automation und Medizintechnik. Auch Schmoch et al. (2020) betrachten technologische Souveränität breiter und nicht mit einem Fokus auf digitale Technologien. Die Autoren identifizieren und bewerten konkrete Zukunftstechnologien auf Basis von Patent-, Publikations- und Marktindikatoren, um ihre Bedeutung für Deutschland zu untersuchen. Zur Identifikation von Zukunftstechnologien wurden verschiedene Zukunftsstudien aus dem nationalen und internationalen Raum, Technologien, die im Kontext nationaler und internationaler gesellschaftlicher Herausforderungen diskutiert werden, sowie Fraunhofer-interne und externe Experten herangezogen. Auf dieser Basis wurde eine Liste von 32 Technologien zusammengestellt, die sich auf die Bereiche Informationstechnik, Produktionstechnik, Werkstoffe, Gesundheit, Verkehr, Umwelt/Klima und Energie beziehen und somit ein breites Technologiespektrum abdecken. Zu den Informationstechnologien mit Zukunftspotenzial gehören laut der Recherche Internet der Dinge, Augmented und Virtual Reality, 5G/6G,

Cybersecurity, Authentifizierung, Künstliche Intelligenz, Blockchain, Quantencomputer und abgeleitet auch Roboter, Soft Robotics, Digitale Medizin, Smart Grids und Autonomes Fahren.

Darauf aufbauend wurde für diese Studie die folgende, vereinfachte Abgrenzung vorgenommen: (1) Hardware/Infrastruktur, (2) Software/Anwendungen, (3) Künstliche Intelligenz, (4) IT-Sicherheit, (5) Digitale Plattformen, (6) Daten. Diese Bereiche werden als Basis für die nachfolgende Bestandsaufnahme der Anbieter- und Anwenderkompetenzen in Europa bzw. insbesondere Deutschland und auch für die Unternehmensbefragung genutzt.

2.2.2 Anbieter- und Anwenderkompetenzen in Deutschland und der EU

2.2.2.1 Hardware/Infrastruktur

Hardware und Infrastruktur stellen die Grundvoraussetzungen für die Digitalisierung dar. Zur Hardware zählen die physischen Komponenten (die elektronischen und mechanischen Bestandteile) eines datenverarbeitenden Systems, wie Mikrochips, Sensoren, Aktuatoren, Endgeräte (BMWi 2015), aber auch Rohstoffe und Vorprodukte. Die Infrastruktur bildet wiederum die technologische Basis der Vernetzung (connect), der Bereitstellung von Rechenkapazität (compute) sowie der Speicherung von Daten auf Servern (store) (Kagermann et al. 2021). Dazu zählt die Kommunikations- bzw. Netzinfrastruktur, Rechen- bzw. Datenzentren aber auch die Nutzung von Cloud-Technologien (insbesondere Infrastructure-as-as-Service).

Im Bereich der Hardware und Infrastruktur bestehen insgesamt sehr hohe Abhängigkeiten zu nicht-europäischen Anbietern (Kagermann et al. 2021). Im Bereich der Rohstoffe und Vorprodukte (seltene Erden, Prozesschemikalien) existieren zunehmende Abhängigkeiten europäischer Hersteller von amerikanischen und asiatischen Rohmaterial- und Vorprodukteanbietern. Die Verlagerung der Wertschöpfungsnetzwerke nach Asien aufgrund von Kostenvorteilen und der Nähe zu wichtigen Kunden stellt insbesondere KMU vor große Herausforderungen, die aufgrund ihrer begrenzten Marktmacht nur wenig Einfluss auf Rahmenbedingungen nehmen können. Komponenten (Mikrochips, Sensoren, Aktuatoren) bilden die Grundlage aller weiteren Infrastrukturen, weshalb diesen und den für sie benötigten Basis- und Fertigungstechnologien sowie teilweise auch Entwicklungs-Softwaretools eine besondere Bedeutung zukommt. In der Sensorik, der Aktorik und den Fertigungstechnologien (im Bereich Sensorik und Leistungselektronik) ist Deutschland wiederum gut aufgestellt. Die Corona-Pandemie hat jedoch enorme Abhängigkeiten der deutschen Wirtschaft im Bereich der Mikrochips (insbesondere High-End-Mikrochips) offenbart. So haben Lieferengpässe die Handlungsfähigkeit zahlreicher Branchen, wie etwa der Automobilindustrie, eingeschränkt. Der Aufbau von Kompetenzen und Kapazitäten zur Reduzierung dieser Abhängigkeiten wird insbesondere im Bereich spezialisierter More-than-Moore-Chips[3] und neuartiger Beyond-Moore-Chiptechnologien gesehen, da Kompetenzen im Bereich von High-End-Mikrochips (More-Moore-Chips) nicht mehr ohne Weiteres aufgeholt werden können. Dadurch können wechselseitige Abhängigkeiten aufgebaut und somit der Zugriff auf nicht in Europa produzierte Chips, auch in Krisenzeiten, sichergestellt werden. In diesem Zusammenhang wird auch betont, dass es darum geht Standards zu setzen und innovative Produktkategorien zu definieren, wofür eine entsprechende Nachfrage aus Leitindustrien nötig ist und sich Branchen jenseits des Mobilfunks und der Automobilindustrie aktiv einbringen müssen (Kagermann et al. 2021). Der Handlungsbedarf im Bereich der Mikrochips wurde bereits

[3] Erklärung der Chiptypen: Fertigungsverfahren mit einer Auflösung von fünf Nanometern und weniger werden „More Moore“ genannt. Neben der zunehmenden Minituarisierung haben sich „More than Moore“-Fertigungstechnologien entwickelt. Dies bedeutet, eine dritte Dimension und dadurch weitere Funktionen hinzuzufügen, wodurch Spezialaufgaben gelöst werden können (spezialisierte Chips). Beyond-Moore-Chips beziehen sich auf neuartige und besonders leistungsstarke Chips, die neuronale Strukturen des Gehirns nachbilden und insbesondere im Bereich Künstliche Intelligenz Verwendung finden sollen.

von der Politik erkannt und es wird anvisiert, Europas Marktanteil an der weltweiten Chipproduktion bis 2030 auf 20 Prozent zu verdoppeln. Aufgrund einer gleichzeitig stark steigenden Produktion weltweit entspricht dies effektiv einer Verdreifachung oder Vervierfachung der Produktion in Deutschland. Der Fokus soll hier insbesondere auch auf Spezialchips für KI und autonomes Fahren liegen (BMWi 2021c).

Auch im Bereich der Kommunikationsinfrastruktur bestehen Abhängigkeiten. Diese sind im Bereich der Mobilzugangsnetze (RAN) aufgrund proprietärer Standards und Lock-in-Effekten nicht leicht lösbar. Um dieser Entwicklung entgegenzusteuern, hat die O-RAN-Alliance, bei der sich auch europäische Anbieter beteiligen, das Ziel, offene Schnittstellen zu etablieren. Ein vollständig offener Open-Source-Ansatz würde Innovation (zum Beispiel 6G), Wettbewerb, Resilienz und Transparenz im Bereich Mobilfunk fördern. Zwar wird O-Ran Potenzial bescheinigt, doch ist die Technologie weit davon entfernt, bestehende Abhängigkeiten abzubauen (Sawall 2021). Innerhalb des europäischen Telekommunikationsmarktes ist es daher auch wichtig, über geeignete industriepolitische Maßnahmen und regulatorische Ansätze die Position der europäischen Anbieter zu verbessern (Kagermann et al. 2021).

Im Kontext der Kommunikationsinfrastruktur ist der Mobilfunkstandard 5G ein vieldiskutiertes Thema. Dieser ermöglicht schnellere Verbindungen, weniger Latenzzeit und höhere Datenraten und liefert somit die technologische Basis der Digitalisierung von wirtschaftlichen und behördlichen Prozessen. Jedoch zeigen sich in diesem Bereich eine Reihe technologischer Abhängigkeiten und Risiken (Eckert et al. 2020). Zunächst besteht eine Abhängigkeit von Herstellern der 5G-Netz-Komponenten. Diese Hersteller sind wiederum auf Cutting-Edge-Mikroelektronik-Hardware angewiesen, deren wenige Hersteller überwiegend aus den USA stammen. Zudem sind die in 5G-Netzen sehr wichtigen Software-Komponenten in hohem Maße durch Patente geschützt und werden in einem komplexen Prozess zu einer Gesamtlösung zusammengeführt, so dass Hintertüren und Einfallstore bislang kaum eindeutig einem Urheber zugeordnet werden. Dadurch bestehen hohe Risiken durch staatliche Einflussnahme, insbesondere zum Zweck der Spionage und Sabotage. Diese existieren zwar auch bei konventionellen Systemen, doch das Potenzial wird mit 5G aufgrund der vielfältigen Einsatzmöglichkeiten sowie dem möglichen Einsatz in sicherheitskritischen Bereichen noch beträchtlich höher sein, sofern keine geeigneten Schutzvorkehrungen getroffen werden. Dazu zählt z. B. eine sichere Ende-zu-Ende-Verschlüsselung bei Endgeräten. Ein Verbot einzelner Hersteller kann zwar zur Risikoreduktion beitragen, jedoch nicht vollständig beseitigen. Zudem könnte die damit verbundene Angebotsreduktion kurz- und mittelfristig zu kritischen Engpässen bei der Bereitstellung von 5G führen und die Wettbewerbsfähigkeit Deutschlands als Forschungs- und Innovationsstandort schwächen. Insgesamt zeigt die 5G-Technologie, wie vielschichtig und komplex technologische Abhängigkeitsstrukturen sein können (vgl. Eckert et al. 2020, S. 8-9) und entsprechend auch Lösungsansätze zum Erhalt bzw. zur Stärkung digitaler Souveränität.

Rechenzentren zählen ebenfalls zur Hardware und gelten aufgrund des steigenden Bedarfs an Rechenleistung als das Rückgrat der Digitalisierung. Zahlen aus einer Studie von 2017 zum deutschen Rechenzentrumsmarkt zeigen eine positive Entwicklung und wachsende Bedeutung (Hintemann 2017). Die Investitionen in Rechenzentrumsinfrastruktur stiegen von 2016 auf 2017 um 10 Prozent auf knapp eine Milliarde Euro. Hiesige Rechenzentren beschäftigten 2017 rund 130.000 Vollbeschäftige und es waren zusätzlich noch rund 85.000 Arbeitsplätze direkt von Rechenzentren abhängig (Hintemann 2017). Bedingt durch die Corona-Pandemie und hohe Investitionen der großen Hyperscaler wächst der Markt aktuell stark und auch die Rechenzentrumsstandorte Frankfurt und Berlin profitieren von dem Boom (Rüdiger und Ostler 2021). Insgesamt nimmt die Wettbewerbs- und Handelsintensität im Rechenzentrumsmarkt weiter zu. Durch eine zunehmende Versorgung mit Hochgeschwindigkeitsnetzen und technologische Fortschritte wie z. B. Cloud

Computing und Virtualisierung werden der Betrieb und die Standortwahl von Rechenzentren immer flexibler. Auch die Datenschutz-Grundverordnung (DSGVO) wird den Wettbewerb innerhalb von Europa voraussichtlich weiter intensivieren, weil das Verschieben der Rechenlasten innerhalb von Europa mit angeglichenem Datenschutzniveau einfacher wird. Trotz zahlreicher Vorteile wie sicherer Stromversorgung, einer guten Anbindung an das Internet sowie Datenschutz, Energieeffizienz und Rechtssicherheit hat der deutsche Rechenzentrumsstandort auch zahlreiche Nachteile. Hier werden insbesondere die zu hohen Strompreise und langwierige Genehmigungsprozessebemängelt (Hintemann 2017).

Solange Hardware und Software entkoppelt sind, ist es relativ unproblematisch, dass es im privaten und kommerziellen Bereich insgesamt keine größeren deutschen Hardwareanbieter gibt. Jedoch ist die Entkoppelung durch die Verbreitung von Cloud-Technologien zunehmend aufgelöst (Kagermann et al. 2021). Anwenderunternehmen werden zu Konsumenten technischer Cloud-Dienste, die „as a service“ von spezialisierten Anbietern vertrieben und zur Verfügung gestellt werden. Dadurch entwickeln sich Netzwerk- und Skaleneffekte zugunsten der Cloud-Anbieter als zugrundeliegender Plattform. Die Notwendigkeit einer globalen Präsenz und dadurch bedingte immense Investitionen führen zu oligopolartigen Marktstrukturen mit wenigen marktbeherrschenden Cloud-Infrastruktur-Anbietern (Hyperscalern) wie Microsoft, Amazon Web Services oder Google, die einen Lock-in der Anwender auf diesen Plattformen anvisieren. Dieser entsteht durch die zwingende Verbindung eben dieser wenig differenzierenden Cloud-Infrastruktur mit den Anwendungsplattformen (vgl. Kapitel 3.2.5). Cloud-Anbieter können dadurch wiederum enorme Mengen an Daten sammeln und globale Datenräume aufbauen. Diese Herausforderung wird in Kapitel 3.2.6 ausführlicher diskutiert.

Zuletzt soll die Quantentechnologie als Zukunftstechnologie nicht unerwähnt bleiben, da die Gefahr besteht, dass sich Abhängigkeiten auf der Ebene der Hardware künftig intensivieren. Die Quantentechnologie gilt als Technologiesprung und besitzt viele Vorteile und Anwendungsfälle. So können Quantencomputer u.a. zu einer massiven Beschleunigung der Rechenleistung führen und dort Lösungen liefern, wo klassische Supercomputer an der Komplexität bestimmter Aufgaben scheitern. Laut Bundesregierung sind Deutschland und Europa in der Grundlagenforschung zu Quanten-Phänomenen sehr gut aufgestellt, haben jedoch in der Entwicklung erster Quantencomputer Nachholbedarf. In Europa gibt es zurzeit kein etabliertes Unternehmen, das die Zusammenführung von Hard-, Soft- und Middleware adressiert. Darum können Aufträge zur Entwicklung und zum Bau von Quantencomputern nicht unmittelbar vergeben werden (Deutscher Bundestag 2021). Beim Bau von kompletten Systemen sind andere Regionen, etwa die USA oder China, schon weiter. Jedoch gibt es hier durchaus Ansätze, wie eine künftige Abhängigkeit noch vermieden werden kann, z. B. die modulare Gestaltung von Quantencomputer-Komponenten, so dass sie mit klassischen Computern kombinierbar sind und sich hybride Systeme ergeben (Kühl 2021).

Aus Anwendersicht ist im Infrastrukturbereich vor allem der Einsatz von und der Umgang mit Cloud-Technologien interessant, da dies eine zentrale Entscheidung in der IT-Infrastruktur eines Unternehmens darstellt. Inwiefern Unternehmen Cloud-Technologien einsetzen und mit diesen umgehen, beobachtet der Cloud-Monitor (KPMG 2021). Laut diesem hat die Verbreitung von Cloud-Technologien in Unternehmen durch die Corona-Pandemie noch einmal deutlich zugenommen: 82 Prozent der Unternehmen mit 20 oder mehr Beschäftigten in Deutschland nutzen derzeit Cloud-Technologien. Das Wachstum der Cloud-Nutzung hat sich somit laut der Studie auf hohem Niveau von drei Prozentpunkten (2019/20) auf sechs Prozentpunkte (2020/21) verdoppelt. In der Informations- und Planungsphase bezüglich des Cloud-Einsatzes befinden sich weitere 15 Prozent der Unternehmen.

Die Prognosen zur Cloud-Nutzung weichen jedoch grundsätzlich ab. Laut einer Befragung von Eurostat mit europaweit knapp 150.000 befragten Unternehmen nutzen nur etwa 36 Prozent der Unternehmen ab zehn Beschäftigten Cloud-Dienste. In Deutschland ist es sogar nur ein Drittel der Unternehmen (Eurostat 2021). Diese Ergebnisse zeigen, dass kleinere Rechenzentren und der Eigenbetrieb von Servern trotz des Trends zu Cloud Computing in der Praxis noch eine Rolle spielen (Hintemann 2020). So weisen Stimmen sogar darauf hin, dass einige Unternehmen Anwendungen aus der Cloud zurück in eigene Rechenzentren migrieren (Alffen 2019; Ostler 2019). Zudem deutet sich ein Trend zu sogenannten Hybrid-Cloud-Modellen ab. Darunter versteht man die kombinierte Nutzung von Servern in eigenen Rechenzentren mit Angeboten aus der Cloud. Dies ermöglicht eine Kombination der Vorteile von standardisierten Cloud-Angeboten – Flexibilität und Skalierbarkeit – mit den Vorteilen des Eigenbetriebs. Eine globale Befragung von über 3.000 IT-Verantwortlichen ergab, dass das Hybrid-Cloud-Modell von 86 Prozent der befragten Unternehmen als ideales Betriebsmodell angesehen wird (Vanson Bourne 2020).

Im Umgang mit Cloud-Technologien zeigt sich im Cloud-Monitor (KPMG 2021) dass sechs von zehn Unternehmen, die Cloud-Lösungen nutzen, über eine Cloud-Transformationsstrategie, d.h. eine Strategie, in welchen Bereichen Cloud-Technologien angewendet werden sollten, verfügen. Demgegenüber gibt ein Drittel an, keine spezifische Strategie zu verfolgen. Betrachtet man nur Großunternehmen (ab 2.000 Beschäftigten) gibt es so gut wie kein Unternehmen ohne eine Strategie. Unternehmen scheinen insgesamt bewusst und kompetent mit Cloud-Technologien umzugehen und den Einsatz konkret zu planen, wobei Großunternehmen hier vorne liegen. Ähnliches zeigt sich im Umgang der Unternehmen mit Cloud-Ausfällen. Diese sind grundsätzlich nicht vermeidbar, so dass sich Unternehmen darauf vorbereiten und für den Ernstfall Notfallpläne ableiten sollten, was über 70 Prozent der Cloud-nutzenden Unternehmen bejahen und konkret umsetzen.

Auch der Umgang mit Public-Cloud-Angeboten[4] ist von Bedeutung, da öffentliche Cloud-Angebote Implikationen für die Souveränität haben, insbesondere in Bezug auf den Zugriff und die Verarbeitung von Daten. Das Vorgehen von Unternehmen bei der Nutzung einer öffentlichen Cloud lässt sich laut Cloud-Monitor in drei Stufen darstellen: Jeweils 29 Prozent sammeln Public-Cloud-Erfahrungen bisher ausschließlich mit unkritischen Geschäftsprozessen und -informationen (Stufe 1) oder verlagern kritische Lösungen und Daten zumindest teilweise in die Public-Cloud (Stufe 2). Die meisten Nutzenden (42 Prozent) vertrauen der Public-Cloud bereits nahezu alle kritischen Anwendungen und Informationen an (Stufe 3). Während kleinere und mittlere Unternehmen bei der Public-Cloud-Nutzung für kritische Anwendungen und Informationen noch zurückhaltender sind, gehen Großunternehmen voran. Hier liegt der Anteil derjenigen, die eine No-Public-Cloud-Strategie für kritische Anwendungen und Informationen verfolgen, lediglich bei 12 Prozent. Demzufolge setzen neun von zehn Großunternehmen Public-Cloud-Lösungen für kritische Geschäftsprozesse und informationen ein. Bei den kleinen (70 Prozent) und mittleren Unternehmen (71 Prozent) ist der Anteil vergleichsweise geringer. Trotz dieser verbreiteten Nutzung, befürchten drei Viertel unberechtigte Datenzugriffe bei der Nutzung einer Public-Cloud. Jeweils rund 60 Prozent der Unternehmen haben Bedenken aufgrund von Hardwareschwachstellen wie Spectre oder Meltdown oder fürchten sogar den Verlust von Daten. Ein jeweils vergleichbarer Anteil sieht Unsicherheiten in der der Rechtslage oder rechtliche und regulatorische

[4] Die Public Cloud oder öffentliche Cloud ist ein Angebot eines frei zugänglichen Providers, der seine Dienste offen über das Internet für jedermann zugänglich macht. Webmailer-Dienste oder die bekannten Google-Docs sind ebenso Beispiele für Public Cloud Angebote wie die kostenpflichtigen Services eines Microsoft Office 365 oder eines SAP Business by Design (Fraunhofer-Allianz Cloud Computing 2021.).

Bestimmungen, die gegen die Public-Cloud sprechen. Insgesamt zeigt sich, dass die Public-Cloud-Nutzung trotz Bedenken der Unternehmen und bestehender Risiken verbreitet ist.

Um Abhängigkeiten in diesem Bereich abzubauen, nutzen Unternehmen spezifische Cloud-Lösungen nicht mehr nur einzeln, sondern verwenden mehrere unterschiedliche Private-Cloud- oder mehrere unterschiedliche Public-Cloud-Lösungen parallel (KPMG 2021). Mithilfe des sogenannten Multi-Cloud-Ansatzes können Unternehmen somit von den Vorteilen unterschiedlicher Cloud-Angebote profitieren. Sie buchen Speicherkapazitäten bei einem Cloud-Provider, Rechenkapazitäten bei einem anderen und Entwicklungsumgebungen bei einem weiteren. Jedes dritte Unternehmen ab 20 Beschäftigten in Deutschland setzt im Jahr 2021 auf eine Multi-Cloud-Strategie. Im Vergleich zur vorangegangenen Erhebung ist die Multi-Cloud-Nutzung damit moderat um drei Prozentpunkte gestiegen. Deutlich stärker ist der Anstieg bei Planung und Diskussion. Während 2019 erst jedes sechste Unternehmen (18 Prozent) das Multi-Cloud-Konzept geplant oder diskutiert hat, befindet sich 2021 jedes vierte Unternehmen (26 Prozent) in der Informations- bzw. Planungsphase. Aufgrund der Komplexität von Multi-Cloud-Lösungen und der dafür benötigten Ressourcen zur Planung und Umsetzung kann die Informations- und Planungsphase durchaus langwierig sein. Zudem ist der Schritt zurück oder der Wechsel zwischen den anbietenden Unternehmen häufig aufwendig und kann sehr teuer werden. Der Anstieg der Multi-Cloud-Nutzung ist in erster Linie auf kleinere und mittlere Unternehmen zurückzuführen. In den Unternehmensgrößenklassen 20 bis 99 und 100 bis 1.999 Beschäftigte nimmt Multi-Cloud-Computing wie in der Gesamtheit der Unternehmen jeweils um drei Prozentpunkte zu. Gleichzeitig wächst in beiden Gruppen auch das Nutzungsinteresse auf 27 bzw. 21 Prozent. Unter den Großunternehmen setzen mehr als 80 Prozent der Unternehmen auf die Multi-Cloud. Die Nutzung bleibt damit konstant auf hohem Niveau (KPMG 2021). Insgesamt rät der Cloud-Monitor dazu, dass alle Unternehmen, die mit der Cloud arbeiten oder ihren Einsatz planen, eine mittel- bis langfristige Cloud-Transformationsstrategie benötigen, die den Aspekt der Abhängigkeit bzw. Unabhängigkeit von einzelnen Providern berücksichtigt sowie perspektivisch den Übergang zu einer Multi-Cloud-Strategie offenhält – auch in Hinblick auf die Realisierung von GAIA-X, der europäischen Cloud- und Daten-Infrastruktur (vgl. Kapitel 3.2.6).

Mehr Agilität bietet als alternativer Ansatz zu Multi-Cloud-Lösung auch die Nutzung von Open-Source-Lösungen, wodurch proprietäre Technologien in der Infrastruktur- und Plattform-Schicht bewusst vermieden werden. In diesem Bereich sind z. B. Kubernetes (Container), PostgreSQL (Datenbanken), Tomcat (Application Server) und Hadoop/Spark (Big Data) als Open-Source-Lösungen verfügbar (Regenfuß et al. 2020). Sie können als Basiskomponenten für die Anwendungsentwicklung auf Public Cloud verwendet werden. Jedoch hat auch dieser Ansatz Nachteile: Zum einen eine ebenfalls hohe technische Komplexität und zum anderen verhindert die zusätzliche Schicht den Zugriff auf einen Großteil der differenzierenden Services und Innovationen der Cloud-Anbieter.

Fazit: Insgesamt zeigt sich, dass im Hardware- und Infrastrukturbereich erhebliche Abhängigkeiten zu nicht-europäischen Anbietern bestehen, die als kritisch eingestuft werden. Demnach sollten diese Abhängigkeiten künftig reduziert bzw. vermieden werden, dies gilt insbesondere für Mikrochips, Kommunikationsinfrastruktur und Cloud-Infrastrukturen. Stärken bestehen vor allem im Bereich der Leistungselektronik und Rechenzentren. Bezogen auf Anwenderunternehmen zeigt sich, dass Unternehmen sich den Risiken bestimmter Lösungen durchaus bewusst sind und entsprechend Maßnahmen einleiten, um einen Provider-Lock-in zu vermeiden. Jedoch besteht hier noch Entwicklungspotenzial, insbesondere bei kleineren und mittleren Unternehmen. Im Umgang mit Cloud-Technologien zeigt sich weiteres

Verbesserungspotenzial, so ist ein nicht zu vernachlässigender Anteil an Unternehmen unzureichend auf Cloud-Ausfälle vorbereitet.

2.2.2.2 Software/Anwendungen

Das Technologiefeld Software-Architekturen und Anwendungen bezieht sich auf Software-Architekturen (generische Struktur eines komplexen Softwaresystems), Betriebssysteme oder Anwendungen (Unternehmenssoftware, Spezialapplikationen und -module) (BMWi 2017). Im Folgenden liegt der Fokus auf Betriebssystemen sowie Open-Source-Lösungen, da letztere als Lösung für mehr Unabhängigkeit im Softwarebereich gesehen werden.

Im Bereich der Betriebssysteme bestehen erhebliche Abhängigkeiten zu nicht-europäischen Anbietern (Windows, iOS, Android) sowie Microsoft Office (Kagermann et al. 2021). Aufgrund der verbreiteten Anwendung stellen diese sowohl für Privatpersonen, Unternehmen als auch öffentliche Verwaltungen de facto einen Standard dar. Das gilt besonders für Microsoft, dessen Produkte vielfach eingesetzt werden und eng miteinander verknüpft sind (bspw. Outlook, Exchange und Windows Server). Die Bindung an die Ökosysteme der Anbieter wird durch eine zunehmende Abhängigkeit der Funktionalitäten von Onlinediensten der Anbieter weiter verstärkt, beispielsweise im Rahmen der Umstellung auf das Microsoft-365-Cloud-Servicemodell. Grundsätzlich herrscht hier Einigkeit, dass Abhängigkeiten abgebaut werden sollten, insbesondere weil eingeschränkte Informationssicherheit und (datenschutz-)rechtliche Unsicherheiten als kritisch erachtet werden. Hier wird z. B. die Ergänzung oder Ablösung von eingesetzten Produkten durch weitere proprietäre Software zur Diversifikation vorgeschlagen. Aber auch der Einsatz bzw. Aufbau von Open-Source-Alternativen ist eine vieldiskutierte Lösungsstrategie (PwC 2019). Dies beinhaltet auf Staats- und Unternehmensseite zum einen die Förderung von Open-Source-Software und -Plattformen und zum anderen den Aufbau von Wissen über Open-Source-Entwicklungs- und Lizenzmodelle sowie über die Funktionsweise von Open-Source-Communities (Kagermann et al. 2021).

Eine aktuelle Studie (Blind et al. 2021) zeigt zudem, dass Open Source mittlerweile eine hohe wirtschaftliche Bedeutung zukommt. So trägt Open Source 95 Milliarden Euro zur EU-Wirtschaftskraft bei. Allein die über 30 Millionen Open-Source-Beiträge der EU-Staaten in Communities entsprachen 2018 einer Personalinvestition in Höhe von fast einer Milliarde Euro. Damit dies so bleibt, bedarf es jedoch auch finanzieller Förderung des Open-Source-Ökosystems, um zu verhindern, dass etablierte Digitalunternehmen wie Microsoft, IBM, Google, Amazon oder Facebook auch im Bereich Open-Source dominieren, da diese sich zunehmend in Open-Source-Communities einbringen. In Europa sind es hingegen eher Einzelentwickler und KMU, die zu Open-Source-Projekten beitragen.

Eine wichtige Voraussetzung für den vermehrten Einsatz von Open-Source-Software (OSS) ist wiederum, dass Unternehmen in Deutschland Anwendungskompetenzen in Bezug auf Open-Source-Lösungen besitzen. Der Open-Source-Monitor (Bitkom 2019b) untersucht im Rahmen einer repräsentativen Unternehmensbefragung von Unternehmen ab 100 Mitarbeitern die Einstellung und den Beitrag zu sowie den Einsatz von Open-Source-Software in deutschen Unternehmen. Die Mehrheit der befragten Unternehmen ist Open-Source-Software gegenüber grundsätzlich positiv eingestellt. Drei Viertel aller Unternehmen sind interessiert an Open-Source-Software und zeigen sich dem Thema gegenüber aufgeschlossen. Nur vier Prozent der Unternehmen beurteilen Open-Source-Software kritisch und lehnen diese eher ab. Zwischen diesen Ansichten liegt noch ein Fünftel der Unternehmen (19 Prozent), die gegenüber Open-Source-Software indifferent sind. Des Weiteren zeigt die Studie, dass nur jedes fünfte Unternehmen (21 Prozent) über eine OSS-Strategie verfügt.

In Bezug auf den Einsatz zeigt sich, dass sieben von zehn Unternehmen bewusst OSS in ihrem Unternehmen einsetzen. Demgegenüber steht rund ein Viertel der Unternehmen, die angeben, keinerlei OSS-Lösungen zu verwenden. Der häufigste Anwendungsfall im Unternehmen ist der Einsatz von auf OSS basierenden Lösungen für einen bestimmten Anwenderkreis im eigenen Unternehmen, ohne dass der OSS-Quellcode verändert wird. Über die Hälfte aller Unternehmen (58 Prozent) setzt OSS auf diese Weise ein. Ein Drittel der Unternehmen (32 Prozent) nutzt OSS-Anwendungen im eigenen Unternehmen und nimmt Anpassungen am Quellcode vor. Jeweils ein Fünftel der befragten Unternehmen setzt auf OSS als Teil eigener Produkte oder Dienstleistungen, die mit Quellcode-Anpassungen (20 Prozent) oder ohne (22 Prozent) an die eigenen Kunden weitergegeben werden. Die Entwicklung von eigenständigen OSS-Produkten beziehungsweise -Lösungen ist Bestandteil des Kerngeschäfts von lediglich zwei Prozent der Unternehmen. Demnach nutzen Unternehmen OSS bereits, jedoch bestehen Unterschiede in der Kompetenz der Unternehmen im Umgang mit OSS.

Die Studie offenbart auch Defizite bei der OSS-Nutzung: Von den Unternehmen, die OSS verwenden, in ihre Produkte und Lösungen integrieren, (weiter-)entwickeln oder sich an OSS-Projekten und -Communities beteiligen, verfügt nur etwa jedes sechste Unternehmen (17 Prozent) über schriftlich formulierte Richtlinien und Regeln zum Umgang mit OSS. Fast 80 Prozent der OSS-Anwender haben keinerlei Richtlinien definiert. Auch bei der Beteiligung an der Weiterentwicklung von OSS zeigt sich Nachholbedarf: Nicht einmal jedes dritte Unternehmen beteiligt sich an der Entwicklung bzw. Weiterentwicklung von Open-Source-Software.

Hemmnisse in der Nutzung liegen vor allem im Bereich fehlender Fachkräfte (12 Prozent), also Experten im Unternehmen, um zum Beispiel OSS an den individuellen Bedarf anzupassen und weiterzuentwickeln. In diesem Zusammenhang werden auch fehlende Schulungsangebote (6 Prozent) und ein großer Schulungs- und Einarbeitungsaufwand (5 Prozent) für die entsprechenden Fachkräfte als Nachteil angesehen. Im Hinblick auf das Thema IT-Sicherheit zeigen die Ergebnisse der Studie, wie ambivalent der OSS-Einsatz gesehen wird. Während zwölf Prozent sicherheitsrelevante Aspekte als Vorteile von OSS ins Feld führen, sehen insgesamt sieben Prozent darin eher Nachteile. Vier Prozent nannten Sicherheitslücken als OSS-Nachteil und weitere drei Prozent bemängeln die Fehleranfälligkeit.

Fazit: Insgesamt wird deutlich, dass die Potenziale von Open-Source-Angeboten erkannt wurden und sich sowohl Anbieter- als auch Anwenderunternehmen in diesem Bereich engagieren bzw. OSS einsetzen. Gleichzeitig wird deutlich, dass Unternehmen, die bereits OSS einsetzen, unterschiedlich elaboriert damit umgehen, etwa in Bezug auf die eigenständige Weiterentwicklung der Lösungen oder dem Bestehen von Umgangsrichtlinien. Insbesondere mangelnde Fachkräfte werden dabei als Hemmnis von den Unternehmen benannt.

2.2.2.3 Künstliche Intelligenz

Künstliche Intelligenz (KI) gilt als Schlüsseltechnologie, die großes Potenzial für Wirtschaftswachstum und Produktivitätszuwächse verspricht. Aus diesem Grund strebt die Bundesregierung mit ihrer nationalen KI-Strategie an, Deutschland zu einem führenden Standort für die Entwicklung und Anwendung von KI-Technologien zu machen und die globale Wettbewerbsfähigkeit zu sichern (Plattform Lernende Systeme 2020). Der globale Wettkampf um die KI-Technologieführerschaft wird bereits intensiv betrieben (Savage 2020). Vor allem Digitalunternehmen aus den USA haben sich durch enorme Mengen an Nutzerdaten sowie umfangreiche Investitionen Wettbewerbsvorteile verschafft. Aber auch China strebt an, bis 2030 führend im Bereich KI zu werden und investiert massiv in deren Forschung und Entwicklung (BMWi 2021d). Deshalb stellt sich grundsätzlich die Frage, ob Europa sich trotz seiner Stärken im Wettbewerb behaupten kann, da es in

Bezug auf Investitionen und der Verfügbarkeit und Güte von Daten zurückliegt (Savage 2020; Marcus et al. 2019).

Deutschland ist im Bereich der KI-Forschung, insbesondere bei Themen wie Lernende Systeme und Maschinellem Lernen, auf einem weltweit führenden Niveau. Gemäß dem SCImago-Journal-Ranking war Deutschland im Ländervergleich bei der Anzahl der KI-Publikationen sowohl im Durchschnitt von 1996 bis 2018 als auch 2018 allein auf Rang 6. Bei der Anzahl von Zitierungen lag Deutschland nach den USA und Großbritannien sogar auf dem dritten Platz (Plattform Lernende Systeme 2020). China hat in den letzten Jahren jedoch enorm aufgeholt. In den Jahren 2016 bis 2019 hat China jedes Jahr mehr Forschungspapiere mit KI-Bezug veröffentlicht als jedes andere Land und wuchs über diesen Zeitraum um 120 Prozent, während der Forschungsoutput der USA beispielsweise nur um 70 Prozent anstieg. Bezogen auf die Qualität (gemessen an Zitationen) liegt China jedoch noch hinter den USA (Savage 2020).

Doch trotz sehr guter universitärer Forschung, fällt es Gründern in Deutschland oft schwer, daraus Geschäftsideen zu entwickeln und zu skalieren. Dies zeigt sich z. B. in einer Untersuchung, wo sich die meisten KI-Start-ups ansiedeln (Demary und Goecke 2019). Die meisten Neugründungen auf dem Gebiet der Künstlichen Intelligenz, fast 1400 der 3500 identifizierten jungen Unternehmen, sind in den USA angesiedelt. Das Silicon Valley gilt nach wie vor als der attraktivste Standort, um eine Geschäftsidee möglichst schnell zum Erfolg zu bringen. Die Nummer zwei stellt China mit rund 400 KI-Start-ups dar. Deutschland liegt mit rund 100 Start-ups deutlich dahinter (Rang 9). Selbst wenn man alle Start-ups innerhalb der Europäischen Union aufsummiert und Großbritannien noch mitzählt, kommt Europa nur auf rund 730 Neugründungen. Damit zählt die EU nur etwa halb so viele junge KI-Unternehmen wie die USA, liegt aber immerhin noch vor China. Bezieht man die Zahl der KI-Startups auf die Anzahl an Unternehmen insgesamt zeigt sich ein anderes Bild: Israel liegt dann auf der Spitzenposition, d.h. KI-Start-ups haben in Bezug auf alle Unternehmen des Landes die größte Bedeutung im Ländervergleich. Dahinter liegen die USA (Rang 2). Finnland (Rang 3) und die Schweiz (Rang 4). Deutschland hält gegenüber der Betrachtung der reinen Anzahl der KI-Startups seine Position (Rang 9). Die EU-28 verlieren dagegen deutlich und belegen bei diesem Indikator nur noch Rang 12 und China den vorletzten Platz. Aktuellere Zahlen der German AI Startup Landscape (appliedAI 2021) zeigen zwar eine positive Entwicklung in Bezug auf KI-Start-ups – so werden in Deutschland von der Initiative 278 Start-ups verzeichnet –, jedoch liegt von den 100 vielversprechendsten KI-Start-ups laut CB Insights der Großteil (64 Prozent) immer noch in den USA (CB Insights 2021).

Insgesamt wird deutlich, dass Deutschland im internationalen Start-up-Vergleich nur gut bis mittelmäßig abschneidet und noch viel Entwicklungspotenzial besteht – auch im Vergleich zu anderen europäischen Staaten. Die Gründe dafür sind laut Demary und Goecke (2019) vielfältig: So befindet sich die deutsche KI-Start-up-Landschaft noch immer in den Anfängen, die öffentliche Förderung von KI ist verbesserungswürdig und auch die allgemein schwache Gründungsaktivität in Deutschland wird als ursächlich bezeichnet. Von der Europäischen Kommission wird in diesem Zusammenhang betont, dass es sich um eine gemeinschaftliche Aufgabe des öffentlichen und privaten Sektors der gesamten Europäischen Union handelt, graduell die Investitionen in KI zu erhöhen und Aktivitäten auszubauen (Europäische Kommission 2018). Eine Stärke Europas könnte dabei die Entwicklung von verantwortungsvoller und menschenzentrierter KI sein, die dem Gemeinwohl nützlich ist, wie sie in Deutschland bereits durch das Gütesiegel „AI made in Germany“ vermarktet wird. Denn es gibt mittlerweile durchaus kritische Stimmen in Bezug auf immer größer werdende Datenmengen, um Algorithmen zu trainieren – mit dem Vorwurf, dass Modelleffizienz und Energieverbrauch in der bisherigen KI-Forschung wenig Beachtung finden (Strubell et al. 2019).

Anwenderseitig verspricht der Einsatz von KI sehr große Potenziale für die Verbesserung von Geschäftsprozessen, die Erhöhung der Leistungsfähigkeit und des Kundennutzens von Produkten sowie für die Entwicklung neuer Geschäftsfelder und Geschäftsmodelle (Rammer 2021). Gleichzeitig nutzt aktuell nur ein geringer Anteil der Unternehmen in Deutschland KI-Verfahren. Eine repräsentative Erhebung im Rahmen der Deutschen Innovationserhebung zeigt, dass im Jahr 2019 lediglich 5,8 Prozent der Unternehmen KI aktiv in Produkten oder Prozessen eingesetzt haben (Rammer et al. 2020). Jedoch zeigt sich durchaus ein positiver Trend: So setzen rund 21 Prozent der im Rahmen des KI-Monitor (Büchel et al. 2021) befragten Unternehmen der Industrie und der industrienahen Dienstleistungen aktuell KI-Verfahren ein. Teilweise kann die Nicht-Nutzung durch die Art und Weise der Geschäftstätigkeit der Unternehmen begründet werden. Dennoch gibt es viele Unternehmen, deren Geschäftsprozesse und Geschäftsmodelle mit Hilfe von KI-Verfahren verbessert oder neu aufgestellt werden könnten, die diese Möglichkeiten bislang aber nicht nutzen. Auch unter den Unternehmen, die KI bereits aktiv einsetzen, ist die Nutzungsintensität oft gering (Rammer et al. 2020).

Eine Studie des ZEW Mannheim (Rammer 2021) untersucht Herausforderungen, denen sich Unternehmen in Deutschland bei der KI-Nutzung gegenübersehen. Die Ergebnisse einer repräsentativen Befragung von fast 1.000 jungen und mittelständischen KI-nutzenden oder KI-affinen Unternehmen zeigen fünf große Themenfelder, die aus Sicht der Unternehmen für die weitere Verbreitung von KI in Geschäftsmodellen und Geschäftsprozessen entscheidend sind. Dies ist zum einen eine leistungsfähige IT-Infrastruktur. Für Unternehmen, die KI noch nicht aktiv nutzen, ist esdie wichtigste Voraussetzung, um in entsprechende Anwendungen einzusteigen. Aber auch für KI-aktive Unternehmen ist die Qualität der Infrastruktur die zweitwichtigste Maßnahme, um den KI-Standort Deutschland voranzubringen. Als weitere Herausforderungen werden Datenzugang und Cloud-Angebote genannt. Die eingeschränkte Datenverfügbarkeit (insbesondere von externen Daten) wird als ein großer Standortnachteil von Deutschland gesehen und ist - gemeinsam mit dem Datenschutz - das größte Problemfeld im Bereich Daten für KI aktiv nutzende Unternehmen (vgl. Kapitel 2.2.2.6). Dahinter folgen Fragen der Datensicherheit. Datenschutzkonforme Cloud-Angebote mit höchsten Sicherheitsstandards werden ebenso als wichtiger Beitrag für bessere Datensicherheit gesehen und stellen eine wesentliche Voraussetzung für den Einstieg in KI-Anwendungen dar. Weitere Herausforderungen, die aber in der Befragung eine geringere Rolle spielen, sind hohe Kosten und fehlende Finanzierungsmittel; Fachkräfte und Weiterbildung; Offenheit von Nutzern/Gesellschaft gegenüber KI.

In der Anwendung von KI ist grundsätzlich zu beachten, dass trotz nennenswerter Fortschritte in der KI-Forschung wichtige Aspekte von KI-basierten Systemen, zum Beispiel Robustheit und Verlässlichkeit von KI-Systemen, Transparenz, Erklärbarkeit von Entscheidungen und Nicht-Diskriminierung, derzeit noch nicht hinreichend verstanden sind (BSI 2020). Zu einem verantwortungsvollen Umgang mit KI durch Anbieter und Anwender zählt deshalb auch, Transparenz und Nachvollziehbarkeit zu erhöhen. Gleichzeitig ist ein Abschätzen der Risiken von hoher Bedeutung; nicht nur im Bereich der Nicht-Diskriminierung, sondern auch in Bezug auf den hohen Energieverbrauch von KI-Lösungen (Strubell et al. 2019). Anders gesagt: Das richtige Einordnen von Ergebnissen sowie die Abwägung, wann und unter welchen Umständen KI genutzt werden kann und sollte, kennzeichnet ein digital souveränes Unternehmen.

Fazit: Obwohl Deutschland in der KI-Forschung stark vertreten ist, zeigen sich im internationalen Vergleich Defizite in Bezug auf Gründungsaktivitäten im KI-Bereich am Standort Deutschland. Neugründungen spielen jedoch wiederum eine sehr wichtige Rolle für wirtschaftliches Wachstum und somit für die Zukunftsfähigkeit der deutschen Wirtschaft, insbesondere in Schlüsseltechnologien wie KI. Anwenderseitig zeigen sich ebenfalls ungenutzte Potenziale. Aufgrund der bisher relativ geringen Verbreitung von KI geht es zunächst darum,

Unternehmen und insbesondere kleinen und mittelständischen Unternehmen einen Zugang zu dem Thema KI zu bieten, Hemmnisse abzubauen und gleichzeitig bezüglich der Risiken zu sensibilisieren.

2.2.2.4 IT-Sicherheit

Mit der Digitalisierung von Wirtschaft und Gesellschaft wachsen zugleich deren Verwundbarkeit und das Missbrauchspotenzial im digitalen Raum. Cyber-Sicherheit und IT-Sicherheitstechnologien, mit denen sich Cyber-Angriffe abwehren lassen, stellen deshalb einen zentralen Aspekt der digitalen Souveränität eines Staates und eines Unternehmens dar. Die Cyber-Bedrohungslage in Deutschland wird grundsätzlich als hoch eingestuft (BMI 2021; BSI 2020). Die Quantität und Qualität der Cyber-Angriffe nimmt dabei kontinuierlich zu und trifft häufig unzureichend gesicherte IT-Systeme. Die Angriffe werden zudem immer professioneller durchgeführt. Die Angriffe und deren Ursprung sind deshalb immer häufiger nicht oder nur mit großem Aufwand und erheblicher Zeitverzögerung festzustellen (BMI 2016).

Die Folgen von Cyber-Angriffen begrenzen sich nicht nur auf den digitalen Raum, sondern können auch gesellschaftliche, wirtschaftliche, politische und persönliche Schäden herbeiführen. Angriffe auf staatliche Institutionen mit dem Ziel der Ausspähung oder Sabotage können die Funktionsfähigkeit von Verwaltung, Streitkräften und Sicherheitsbehörden beeinträchtigen und Auswirkungen auf die öffentliche Sicherheit und Ordnung haben. Die gezielte Verbreitung von Falschmeldungen, die durch gekaperte IT-Systeme ermöglicht wird, kann zur Desinformation und Manipulation der öffentlichen Meinung und als Angriff auf die Demokratie genutzt werden. Im Wirtschaftskontext können Cyber-Angriffe auf kritische Infrastruktur wie etwa Energieversorgungsnetze weite Bereiche des öffentlichen und privaten Lebens zum Erliegen bringen (BSI 2020). Zudem kann die Innovationstätigkeit von Unternehmen durch die Gefahr von Cyberangriffen beeinträchtigt werden (EFI 2020). Der deutschen Wirtschaft entsteht Schätzungen zufolge durch Diebstahl, Spionage und Sabotage im Cyberraum schon heute jährlich ein Gesamtschaden von 223 Milliarden Euro (Bitkom 2021). Aus diesem Grund sind Anbieter- und Anwenderkompetenzen in Deutschland im Bereich der IT-Sicherheit von sehr hoher Bedeutung.

Der IT-Sicherheitsmarkt in Deutschland entwickelt sich positiv und weist ein starkes Wachstum auf, was jedoch auch für andere Märkte gilt (Legler und Hyhorova 2019). Ein Vergleich internationaler Patentierungsaktivitäten der zehn Länder mit den meisten Patenten zeigt einen deutlichen Vorsprung der USA mit einem Anteil von 33,5% angemeldeter transnationaler Patente. Die EU liegt an zweiter Stelle mit 21,5%. Danach folgen Japan und China. Deutschland liegt hier an fünfter Stelle mit einem Anteil von 6,2% und damit an erster Stelle innerhalb der EU (EFI 2020, S. 49). Diese Stärken in Deutschland und Europa gilt es beizubehalten und weiter auszubauen. Ein Handlungsfeld wird dabei z. B. im Bereich der digitalen Identitäten gesehen (Kagermann et al. 2021). Dafür ist ein interoperables europäisches ID-Ökosystem von hoher Bedeutung, um ein ausreichendes internationales Gewicht zu erreichen und um Standards von weltweiter Bedeutung zu setzen, an denen und den darin verankerten Werten sich Hersteller orientieren können.

Im Bereich der Cybersicherheit digital souverän zu sein, bedeutet, Fähigkeiten in der gesamten Bandbreite zu besitzen, also von der Grundlagenforschung bis zur Implementierung. Europa ist hier bereits stark aufgestellt, so dass dem Erhalt und dem Ausbau dieser Stellung eine wichtige Rolle zukommt (Kagermann et al. 2021). Nur auf dieser technologischen Basis kann für die Wirtschaft und die europäische Gesellschaft ein souveränes Handeln im digitalen Raum im Sinne europäischer Wertevorstellungen sichergestellt werden. Für die Realisierung ist auch ein gemeinsamer europäischer Binnenmarkt von hoher Bedeutung, da nur dieser ein ausreichendes internationales Gewicht aufweist, um erfolgreich entsprechende Standards zu setzen (vgl.

Kapitel 2.2.3.3). Die Harmonisierung der heterogenen Cybersicherheitslandschaft Deutschlands und Europas wird deshalb als kritisch angesehen und bedarf auch politischer Begleitung. Initiativen wie der Cybersecurity Act[5], die Richtlinie zur Netz- und Informationssicherheit sowie die europäischen Datenstrategie weisen dabei bereits in die richtige Richtung (Kagermann et al. 2021).

Anwenderseitig zeigt sich zunächst ein hohes Bewusstsein für IT-Sicherheit. So gaben deutsche Unternehmen in einer Befragung (Dreißigacker et al. 2020) mehrheitlich an, dass in den Geschäftsführungen der Unternehmen und in den Belegschaften größtenteils ein Bewusstsein über IT-Risiken vorhanden ist. Nur ein sehr geringer Anteil ist der Meinung, dass sich die Geschäftsführung bzw. die Belegschaft des Unternehmens der IT-Risiken nicht bewusst sei. Die überwiegende Mehrheit (rund 85 Prozent) stimmte auch (eher) der Aussage zu, dass in ihrem Unternehmen sehr viel im Bereich IT-Sicherheit getan wird. Auch Initiativen wie die Arbeitsgruppen „Sicherheit vernetzter Systeme“ und „Rechtliche Rahmenbedingungen“ der Plattform Industrie 4.0, die Wege zur Vermeidung steigender digitaler Verwundbarkeiten im Zuge der engeren Vernetzung der industriellen Produktion erarbeiten, zeigen ein Bewusstsein für Cyberrisiken. Zudem existieren bereits mehrere Initiativen, die dafür sorgen, dass Angriffsvektoren schnell und vertrauensvoll geteilt werden, wie zum Beispiel die Deutsche Cyber-Sicherheitsorganisation (Kagermann et al. 2021).

Die oben genannte Studie (Dreißigacker et al. 2020) zeigt weiter, dass deutsche Unternehmen mehrheitlich organisatorische und technische Maßnahmen ergreifen, um die IT-Sicherheit zu erhöhen. Organisatorische Maßnahmen werden mehrheitlich von den Unternehmen durchgeführt, jedoch zeigen sich Unterschiede in der Verbreitung spezifischer Maßnahmen: Kleine Unternehmen (10-49 Beschäftigte) setzen deutlich seltener schriftlich fixierte Richtlinien zur IT-Sicherheit (ca. 63 Prozent) sowie zum Notfallmanagement (ca. 51 Prozent) ein als große Unternehmen (ab 500 Beschäftigte: ca. 92 bzw. 84 Prozent). Dies weist darauf hin, dass sich kleine Unternehmen weniger intensiv mit dem Thema auseinandersetzen. Zudem gibt es branchenspezifische Unterschiede. Innerhalb des Baugewerbes sind die zuvor genannten Maßnahmen ebenfalls deutlich seltener vorhanden als bei Finanz- und Versicherungsdienstleistern. Die Mehrheit der Unternehmen (ca. 77 Prozent), die solche Richtlinien eingeführt haben, überprüft deren Einhaltung regelmäßig und ahndet gegebenenfalls Verstöße. Dies weist darauf hin, dass diese Richtlinien nicht nur theoretisch vorhanden, sondern auch handlungsleitend sind. Schulungen zur IT-Sicherheit für Beschäftigte sind ein weiteres Beispiel für organisatorische Maßnahmen. Diese werden von über drei Viertel der großen Unternehmen (ca. 76 Prozent) aber lediglich von weniger als der Hälfte der kleinen Unternehmen (ca. 47 Prozent) durchgeführt. Auch hier existieren Branchenunterschiede, was vermutlich durch den unterschiedlichen Digitalisierungsgrad und die damit verbundene unterschiedliche Risikolage bedingt ist. Bei den technischen Maßnahmen liegen die Anteile der Unternehmen, die Mindestanforderungen für Passwörter haben, Zugangs- und Nutzerrechte individuell und nach Aufgabe vergeben, regelmäßig Backups durchführen, diese physisch getrennt aufbewahren, Antivirensoftware und Firewall einsetzen und die Sicherheitsupdates und Patches regelmäßig installieren, in allen Größenklassen bei mindestens 80 Prozent, wobei größere Unternehmen auch hier aktiver sind.

Auch in anderen Studien wird betont, dass kleine und mittlere Unternehmen oft nicht in der Lage sind, selbstständig Cybersecurity-Vorkehrungen auf höchstem Niveau zu treffen und auf Sensibilisierung, die Vermittlung von Kenntnissen und rasche externe Hilfe im Krisenfall angewiesen sind (Kagermann et al. 2021). Deshalb kommt dem Ausbau des öffentlichen Beratungsangebots eine hohe Bedeutung zu. Privatwirtschaftliche „Cyber Defence Center“ oder Kollaborationsorganisation werden dabei als wichtige

[5] Eine EU-Verordnung, die unter anderem neue Richtlinien und eine einheitliche Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik einführt.

Bestandteile des Cybersecurity-Ökosystems benannt. Diese basieren auf dem Zusammentragen und dem Austausch von Erfahrungen und können durch Kostensynergien und Bündelung von Informationen Abhilfe schaffen.

Hemmnisse im IT-Sicherheitsbereich wurden in einer Befragung von 556 IT-Beauftragten in deutschen Unternehmen untersucht (Bundesdruckerei 2018). Hier zeigen sich insbesondere hohe Kosten als Hemmnis für die Gewährleistung und die Verbesserung ihrer IT-Sicherheit (61 Prozent). Eine zumindest zeitweise Überforderung von den gesetzlichen Regeln zu IT-Sicherheit und Datenschutz sehen 63 Prozent der Unternehmen.

Fazit: Insgesamt zeigt sich im Bereich der IT-Sicherheit für Deutschland, zumindest innerhalb der EU, eine vergleichsweise starke Position hinsichtlich der Anbieterkompetenzen. Diese gilt es zu stärken. Bereits initiierte Maßnahmen wie die Gründung der Cyberagentur sollten konsequent vorangetrieben werden. Zudem ist eine Koordinierung und Harmonisierung innerhalb Europas von hoher Bedeutung. Anwenderunternehmen haben das Risiko von Cyberangriffen überwiegend erkannt, jedoch gibt es nach wie vor Unternehmen, die sich nicht in ausreichendem Maße mit dem Thema auseinandersetzen. Niedrigschwellige Informations- und Beratungsangebote können insbesondere kleine und mittlere Unternehmen adressieren. Zudem sollten die Vermittlung von Cybersicherheitskenntnissen in der beruflichen Aus- und Weiterbildung sowie an Hochschulen verstärkt werden, um den zunehmenden Bedarf an Cybersicherheitsfachkräften zu decken (EFI 2020).

2.2.2.5 Digitale Plattformen

Digitale Plattformen koordinieren die Interaktion zwischen verschiedenen Akteursgruppen (siehe z. B. Evans 2011). B2C-Plattformen wie Facebook oder Amazon unterscheiden sich von klassischen Märkten durch geringere Transaktionskosten und hohe Transaktionsvolumina sowie direkte und indirekte Netzwerkeffekte. Netzwerkeffekte steigen mit der Zahl der Plattformnutzenden und können zu einer Marktdominanz einzelner Plattformbetreiber führen. Im Vergleich zu B2C-Märkten sind B2B-Märkte in der Regel kleinteiliger und oftmals auf spezifische Branchen fokussiert, so dass Netzwerkeffekte eine geringere oder andere Rolle spielen und damit die Gefahr der Monopolisierung weniger stark ausgeprägt ist (siehe z.B. Hoffmann et al., 2021, sowie Falck und Koenen, 2020, zu Strukturunterschieden zwischen B2C- und B2B-Plattformen).

Im B2C-Segment bestehen große Abhängigkeiten zu US-Plattformanbietern wie Amazon, Facebook, Microsoft, Google aber auch zu asiatischen Plattformen (Kagermann et al. 2021). So kommen die wertvollsten Plattformunternehmen Apple, Microsoft, Alphabet (Google) und Amazon, Facebook, Alibaba und Tencent alle aus den USA und China (Cusumano et al. 2020). Die starke Marktposition dieser B2C-Hyperscaler wird von EU-Anbietern in absehbarer Zeit nicht einzuholen sein. Daraus ergeben sich zahlreiche Herausforderungen und Risiken in Bezug auf die digitale Souveränität von deutschen Unternehmen, da diese sich den Geschäftsbedingungen der großen Plattformen, sogenannter Gatekeepers, unterordnen müssen. So haben Unternehmen z. B. keinen Einfluss darauf, wie ihre Inhalte und Produkte bewertet und beworben werden und wie ihre Kommunikation über die Plattform moderiert wird. Zusätzlich ist der Zugang zu Kundendaten oftmals nicht möglich, obwohl Daten zur Kundschaft und deren Kaufverhalten zur Anpassung der Marktstrategie nützlich wären. Im direkten Wettbewerb mit der Gatekeeper-Plattform – die diese Daten zum eigenen Vorteil nutzt – sind sie also klar benachteiligt (Europäische Kommission 2020a). Deshalb ist es wichtig, den monopolartigen Stellungen dieser Plattformen politisch und regulatorisch konsequent entgegenzuwirken,

wie es bereits von der EU durch eine Reihe von regulatorischen Maßnahmen wie etwa dem Digital Markets Act und Digital Services Act vorangetrieben wird.

Im B2B-Bereich ist die Markstellung deutscher und europäischer Anbieter als gut anzusehen. Aufgrund der industriellen Domänenexpertise existieren marktführende europäische Angebote: SAP als globaler Marktführer bei ERP-Systemen, Dassault mit marktführender Rolle bei PLM-Systemen und Siemens, welches mit MindSphere ein IoT-Betriebssystem anbietet, wenn auch noch mit geringem Marktanteil. Diese europäischen Unternehmen kommen jedoch nur auf etwa zehn Prozent der Unternehmenswerte amerikanischer Firmen (Kagermann et al. 2021). Ein Grund hierfür sind unzureichende Skalierungsmöglichkeiten durch einen fragmentierten, heterogenen europäischen Markt. Wenn diese Skalierungsmöglichkeiten geschaffen werden, werdn der deutschen Industrie aufgrund ihres hohen Branchen-Know-hows und dem Zugang zu Maschinen- und Kundendaten gute Chancen zugeschrieben, Plattformen im B2B-Segment erfolgreich zu etablieren (Hoffmann et al. 2021).

In absehbarer Zeit ist außerdem nicht mit einer Dominanz einzelner Anbieter im Bereich der industriellen B2B-Plattformmärkte zu rechnen, seien es Transaktionsplattformen oder IoT-Plattformen (Hoffmann et al. 2021). Trotzdem gilt es seitens der Wettbewerbsbehörden im Blick zu behalten, ob es zu einer Marktkonzentration auf einen oder sehr wenige IoT-Softwareanbieter, insbesondere im Plattforminfrastrukturbereich, kommt und die Marktmacht missbräuchlich ausgenutzt wird. Außerdem wird betont, dass es für Europa einheitliche regulatorische Rahmenbedingungen braucht, die den ungehinderten grenzüberschreitenden Datenverkehr ohne Diskriminierung ermöglichen. Auch eine leistungsfähige Infrastruktur und insbesondere der schnelle und flächendeckende Ausbau des glasfaserbasierten Breitbandinternets und des 5G-Mobilfunkstandards sind für Funktionsfähigkeit und Datenfluss wichtig (Hoffmann et al. 2021).

Zudem bleibt zu bedenken, dass industrielle B2B-Plattformen auf die Cloud-Infrastruktur großer US-Anbieter wie Amazon oder Microsoft zurückgreifen. Diese Anbieter haben ihr Angebot mittlerweile um die Bereitstellung von Programmierumgebungen weiterentwickelt (neben der Bereitstellung von Rechen- und Speicherkapazitäten). Das bedeutet, sie stellen Unternehmen einen Werkzeugkasten zur Programmierung eigener IoT-Anwendungen zur Verfügung. So machen die Infrastrukturanbieter IoT-Software über die Cloud zugänglich und ermöglichen auch KMU, die über weniger Ressourcen verfügen, den Aufbau von IoT-Geschäftsmodellen. Durch diese Lösung „aus einer Hand“ sowie hohe Kompetenz in der Datenanalyse und hohe Marktanteile haben die großen US-Infrastrukturanbieter einen Einfluss auf die Entwicklung industrieller B2B-Plattformen. Es bleibt abzuwarten, inwiefern die großen US-Cloud-Anbieter ihren Marktanteil auch im IoT-Segment ausbauen können. Sollten sie es schaffen, ihre Dominanz im Infrastrukturbereich auch auf spezifische plattformbasierte Geschäftsmodelle im Industriebereich ausdehnen zu können, würde dies zu erheblichen Abhängigkeiten führen (Hoffmann et al. 2021).

Anwenderseitig zeigt sich, dass digitale Plattformen in der Industrie zunehmend verbreitet sind. In einer Befragung von deutschen Industrieunternehmen (Jäger und Lerch 2020) zeigt sich, dass fast ein Drittel der Unternehmen mindestens eine der beiden Plattformtypen (Transaktionsplattform und IoT-Serviceplattformen) nutzt. Transaktionsplattformen finden dabei noch häufiger Verwendung als IoT-Serviceplattformen. So verwenden insgesamt 24 Prozent aller Industriebetriebe Transaktionsplattformen, aber nur 16 Prozent IoT-Serviceplattformen. Große Betriebe (mehr als 250 Beschäftigte) setzen beide Plattformtypen häufiger ein als kleine und mittlere Unternehmen.

Die Studie von Jäger und Lerch (2020) kommt auch zu dem Ergebnis, dass die überwiegende Mehrheit der Industriebetriebe im Bereich der IoT-Serviceplattformen ausschließlich auf unternehmenseigene Plattformen setzt, sich also keinen anderen digitalen Plattformen anschließt. Besonders deutlich zeigt sich dies bei den großen Betrieben. Auch das trägt dazu bei, dass Skalen- und Netzwerkeffekte im B2B-Bereich kaum zu beobachten sind. Die Autoren legen zudem nahe, dass die überwiegende Nutzung eigener Plattformen auch eine Erklärung dafür ist, dass sich im Rahmen der Studie nur geringe Umsatzeffekte durch das Plattformgeschäft für Industriebetriebe beobachten lassen und die Insellösungen überwiegend von innovationsfreudigen und dienstleistungsaffinen Betrieben eingesetzt werden (Jäger und Lerch 2020). Gleichzeitig zeigt sich, dass nur ein sehr geringer Anteil aller Industriebetriebe (zwei Prozent) sowohl auf eigene als auch auf unternehmensexterne IoT-Serviceplattformen setzt. Somit ist nur ein sehr kleiner Anteil aller Industriebetriebe gleichzeitig in mehreren IoT-Serviceplattformen aktiv. Dieses Ergebnis lässt darauf schließen, dass bislang eine Interoperabilität der verschiedenen Insellösungen nur stark eingeschränkt möglich ist bzw. kaum angestrebt wird (Jäger und Lerch 2020). Obwohl dies bedeutet, dass Unternehmen relativ unabhängig von Drittanbietern sind, stellt die geringe Interoperabilität auch ein Problem dar, da sie gleichzeitig die Flexibilität einschränkt und sich so keine Skaleneffekte bilden können.

Auch eine Befragung von Bitkom (2020b) untersucht die Sicht deutscher Anwenderunternehmen auf digitale Plattformen, jedoch branchenübergreifend und aggregiert für B2C- und B2B-Plattformen. Es zeichnet sich ein gemischtes und teils skeptisches Bild. Insgesamt sehen Unternehmen digitale Plattformen zwar eher als Chance oder ausschließlich als Chance (45 Prozent), dennoch geben 30 Prozent der Unternehmen an, diese eher als Risiko oder ausschließlich als Risiko zu sehen (30 Prozent). Für etwa ein Fünftel der Unternehmen sind Plattformen derzeit nicht relevant. Die Frage, ob Unternehmen sich durch Plattformen in ihrer Existenz bedroht sehen, bejahen fast ein Drittel der Unternehmen (27 Prozent). Bezüglich der künftigen Nutzung zeigt sich, dass zwei Drittel der Nicht-Nutzer auch in Zukunft nicht auf Plattformen setzen wollen. Wiederum jedes dritte Unternehmen gab aber in der Umfrage an, im Jahr 2020 verstärkt in digitale Plattformen zu investieren. Im Umgang mit digitalen Plattformen wird deutlich, dass nur sechs von zehn Unternehmen eine Plattform-Strategie formuliert haben und sich somit planungsvoll und langfristig mit dem Thema auseinandersetzen. Als größte Hemmnisse bei der Nutzung digitaler Plattformen werden Datenschutz (63 Prozent), IT-Sicherheit (58 Prozent) und ein Mangel an qualifizierten Mitarbeitern (53 Prozent) genannt.

Fazit: Trotz erheblicher Abhängigkeiten deutscher Unternehmen von B2C-Plattformen existieren Stärken in Bezug auf B2B-Plattformen. Anbieterseitig existieren hier bereits marktführende Angebote, denen durch einen europäischen Binnenmarkt Skalierungsmöglichkeiten geboten werden sollten. Anwenderseitig ist der Einsatz digitaler Plattformen zwar auf dem Vormarsch, dennoch bleiben Unternehmen skeptisch und sehen insbesondere Probleme im Bereich Datenschutz und IT-Sicherheit. In Bezug auf B2B-Plattformen setzen Unternehmen vermehrt auf Eigenlösungen, was zwar die Unabhängigkeit von Drittanbietern erhöht, gleichzeitig aber Interoperabilität und somit Handlungsfähigkeit schwächt. Insgesamt sind vor allem die Stärkung der Anbieterkompetenzen im B2B-Kontext und die Regulierung von B2C-Plattformen von Bedeutung. Anwenderunternehmen müssen wiederum verstärkt ein Bewusstsein für die wirtschaftlichen Chancen von digitalen Plattformen entwickeln und im B2B-Bereich abwägen, ob eine Eigenentwicklung oder der Zusammenschluss mit anderen digitalen Plattformen im Einzelfall sinnvoll ist.

2.2.2.6 Daten

Grundsätzlich umfasst der Datenbegriff elektronisch gespeicherte und nicht-elektronisch gespeicherte Zustände oder Wiedergaben von Sachverhalten, z. B. die Ergebnisse einer Umfrage. Eng mit dem Begriff

verknüpft ist weiter der Datenraum. Hierbei handelt es sich um einen „gemeinsamen, vertrauenswürdigen Raum für Transaktionen mit Daten“, der z. B. auf „gemeinsamen Standards (oder Werten, Technologien, Schnittstellen) beruht“, welche wiederum Transaktionen mit Daten ermöglichen oder befördern (Bundesregierung 2021, S. 109).

Wie in Kapitel 2.1.2 beschrieben, hat sich der Begriff Datensouveränität als wichtiger Teilaspekt einer allgemeinen digitalen Souveränität entwickelt. Diese ist gewährleistet, „wenn die Verfügungs- und Nutzungsrechte an Daten, das heißt der Zugriff, der Transfer, die Verarbeitung und die Analyse auf jeder Wertschöpfungsebene ein selbstbestimmtes Handeln gewährleisten. Dies schließt etwa die Möglichkeit ein, auf vertraglicher Grundlage Dritte vom Zugriff auf Daten ein- oder auszuschließen, die Verknüpfung unterschiedlicher Daten sowie die Verarbeitung und Analyse von Daten zu ermöglichen oder zu unterbinden“ (BMWi 2019: S. 11). Neben diesen technischen Voraussetzungen bzw. Rahmenbedingungen ist auch der souveräne Umgang, also die verantwortungsvolle, kompetente Nutzung von Daten (d.h. Datenkompetenzen) für eine digitale Souveränität von hoher Bedeutung (Gesellschaft für Informatik 2020).

Im B2C-Bereich liegt die Kontrolle über Datenräume bereits überwiegend außerhalb Europas, d.h. in den USA und in China (vgl. Kapitel 2.2.2.1 und 2.2.2.5). Unternehmen aus Deutschland und Europa fehlen demnach diese Daten für die Entwicklung von Innovationen. Im B2B-Bereich sind solche Datenräume größtenteils noch nicht entstanden (vgl. Kapitel 2.2.2.5). Sollte es amerikanischen und chinesischen Hyperscalern gelingen, auch hier die maßgeblichen Datenräume aufzubauen bzw. zu beherrschen, hätte dies immense wirtschaftliche Folgen für Deutschland und Europa und als Konsequenz auch Einschränkungen des Handlungsspielraumes und somit der Souveränität zur Folge (Kagermann et al. 2021).

Die enormen Datenmengen, die amerikanischen und chinesischen Cloud-Anbietern zur Verfügung stehen, können auch im Bereich der Künstlichen Intelligenz zu Vorsprüngen führen, da große Datenmengen und wenig strikte Datenschutzregeln für die Entwicklung förderlich sind. Europas digitale Souveränität bzw. Datensouveränität wird zudem geschwächt, weil US-Hyperscaler rechtlich dem US-CLOUD-Act unterliegen. Dies erlaubt US-Behörden teilweise ohne richterlichen Beschluss auf Daten zuzugreifen, die von US-Cloud-Providern kontrolliert werden – selbst wenn die Daten in Rechenzentren im europäischen Raum gespeichert werden. Deshalb sind Kooperationen mit den Hyperscalern zur Etablierung des europäischen Rechts in Europa (insbesondere DSGVO) von hoher Bedeutung. Gleichzeitig gilt es die eigenen Fähigkeiten und Angebote zu entwickeln (Kagermann et al. 2021).

Aufgrund der Sorge um Europas digitale Souveränität durch Abhängigkeiten zu amerikanischen und chinesischen Datenräumen wurde das Projekt GAIA-X ins Leben gerufen. GAIA-X ist ein Konzept zur Gestaltung der nächsten Generation europäischer Dateninfrastruktur, welches derzeit von Vertretern aus Wirtschaft, Wissenschaft und Politik auf europäischer Ebene entwickelt wird. Das Ziel von GAIA-X ist es, eine sichere und vernetzte Cloud- und Dateninfrastruktur zu schaffen, die die digitale Souveränität erhält und ausbaut sowie Innovationen begünstigt. Dies gelingt durch ein offenes und transparentes digitales Ökosystem, welches die Verfügbarkeit und Zusammenführung, das vertrauensvolle Teilen und Nutzen von Daten und Diensten ermöglichen soll (BMWi 2021b). Jedoch werden amerikanische Hyperscaler im europäischen Raum auch im Falle einer erfolgreichen Umsetzung von GAIA-X vorerst nicht zu ersetzen sein (Kagermann et al. 2021). Zudem befindet sich GAIA-X noch in der Entwicklung. Insgesamt wird im Bereich der Daten betont, dass die Menge an nutzbaren, qualitativ hochwertigen Daten deutlich erhöht werden muss, ohne dabei Persönlichkeitsrechte, das Recht auf informationelle Selbstbestimmung oder andere Grundrechte zu verletzen

(BMWi 2017, 2021d). Dies zeigt erneut die Komplexität der Situation, da der Schutz der Souveränität des Einzelnen eine Herausforderung für die Souveränität auf wirtschaftlicher Ebene darstellt (da die Datennutzung eingeschränkt ist, was wiederum Implikationen für u.a. die Entwicklung von KI hat).

Anwenderseitig spielen Datenkompetenzen in Unternehmen eine zentrale Rolle, um Daten wirtschaftlich nutzen zu können und dadurch neue Wertschöpfungsmöglichkeiten zu erschließen. Zu den Datenkompetenzen zählt einerseits, dass Daten, die in Geschäftsprozessen anfallen, gesammelt, aufbereitet und für Analysen zugänglich gemacht werden. Andererseits sind spezifische Kenntnisse und Methoden notwendig, um solche Daten effektiv zu nutzen, wie etwa Methoden des Datenmanagements und der Datenanalyse. Eine Studie des ZEW zur KI-Nutzung in Deutschland (Rammer 2021) hat unter anderem den Stand des Umgangs mit Daten in den Unternehmen, die aktuell KI nicht aktiv nutzen, untersucht. Die Studie unterscheidet dabei zwischen sechs Formen der systematischen Datennutzung. Dazu zählen Kenntnisse der Beschäftigten zu Datenmanagement und analysen und die Beschäftigung von Personal, das hauptsächlich für die Erfassung und Analyse von Daten zuständig ist. Auch die Nutzung von Vertriebs- und Marketingdaten, Prozessdaten aus Maschinen und Anlagen sowie Daten aus Online-Quellen bis zur Erfassung und Auswertung von Echtzeitdaten gehört dazu. Während Kenntnisse zu Datenmanagement und -analysen relativ weit verbreitet sind (62 Prozent), beschäftigen nur relativ wenige Unternehmen Personal, das sich schwerpunktmäßig mit der Datenerfassung und -analyse befasst (24 Prozent). Mehr als die Hälfte der Unternehmen mit Digitalkompetenzen (53 Prozent) nutzt Daten aus Online-Quellen, um Kundenbedürfnisse zu identifizieren und Marketingstrategien zu entwickeln. Die Studie zeigt zudem, dass große Unternehmen in der systematischen Datennutzung vorne liegen. Insgesamt zeigt sich also Entwicklungspotenzial bezüglich der Datenkompetenzen deutscher Unternehmen.

Auch eine Befragung von 500 in Deutschland ansässigen Unternehmen (Röhl et al. 2021) beschäftigt sich mit der Datennutzung und Hürden in ebendieser. Die Ergebnisse zeigen, dass viele Unternehmen die Potenziale der Datennutzung noch nicht umfassend kennen und nutzen. Bei der „Data Readiness“ zeigen sich große Unterschiede zwischen den Unternehmen. 28 Prozent der Unternehmen weisen einen hohen Digitalisierungsstand hinsichtlich des eigenen Datenmanagements auf und wurden als digital klassifiziert, während 72 Prozent noch weniger digital sind. Mit mehr als 60 Prozent ist auch ein erheblicher Teil der Großunternehmen der Gruppe der weniger digitalen Unternehmen zugehörig. Hemmnisse bei der wirtschaftlichen Nutzung sehen Unternehmen mehrheitlich (85 Prozent) bei datenschutzrechtlichen Grauzonen. Auch die fehlende Rechtssicherheit bei der Anonymisierung von Daten wird von 73 Prozent benannt.

Nach den Plänen der Bundesregierung soll GAIA-X die Verbreitung von Cloud-Lösungen und Datenanwendungen in Deutschland und der EU maßgeblich vorantreiben (siehe oben). Doch kennen Unternehmen das Vorhaben überwiegend nicht. In der Umfrage des IW Köln (Röhl et al. 2021) geben nur 6,5 Prozent der Unternehmen an, das Vorhaben GAIA-X überhaupt zu kennen. Selbst bei den digitalen Unternehmen sind es lediglich knapp 10 Prozent. Auch der Cloud-Monitor (KPMG 2021) zeigt, dass das Projekt GAIA-X in der Wirtschaft noch nicht hinreichend bekannt ist. In der Umfrage geben vier von zehn Unternehmen mit 20 oder mehr Beschäftigten in Deutschland an, bisher noch nichts von GAIA-X gehört oder gelesen zu haben. Rund 15 Prozent kennen GAIA-X zwar namentlich, geben aber an, noch zu wenig darüber zu wissen. Etwa vier von zehn Unternehmen kennen dafür GAIA-X und haben sich bereits damit beschäftigt. Diese Unternehmen sehen prinzipiell großes Potenzial in GAIA-X. Für zwei Drittel der Unternehmen (65 Prozent), die Cloud-Lösungen nutzen, planen oder diskutieren und GAIA-X kennen, wäre eine GAIA-X-

konforme Cloud-Lösung sogar ein Must-have bei der Cloud-Provider-Auswahl. Das übrige Drittel bewertet die Kooperation mit GAIA-X zumindest als Nice-to-have. Lediglich ein Prozent sieht keine Relevanz von GAIA-X. Dieses Potenzial sollte demnach genutzt werden und GAIA-X einer breiteren Masse bekannt gemacht werden.

Fazit: Im Datenbereich, d.h. im Zugriff auf und der Verarbeitung von Daten, zeigen sich Abhängigkeiten und Defizite in der deutschen Wirtschaft. Im B2C-Bereich liegt die Kontrolle über Datenräume bereits überwiegend außerhalb Europas, d.h. in den USA und in China. Im B2B-Bereich sind solche Datenräume größtenteils noch nicht entstanden, weshalb hier ein wichtiger Hebel liegt, um die Abhängigkeiten zu den USA und China nicht weiter zu vertiefen und damit den Handlungsspielraum der deutschen Wirtschaft einzuschränken. Kritisch ist dies vor allem, weil Daten die Grundlage für Innovationen bilden (Beispiel KI), aber der unerlaubte Zugriff durch fremde Regierungen möglich wird (Beispiel US CLOUD Act). Gaia-X als europäisches Cloud-Infrastrukturprojekt ist deshalb ein wichtiger Vorstoß, muss aber auch zeitnah umgesetzt und unter Unternehmen bekannt gemacht werden. Anwenderseitig besteht ebenfalls Entwicklungspotenzial in Bezug auf Datenkompetenzen deutscher Unternehmen, die für einen souveränen Umgang und eine effektive Nutzung von hoher Bedeutung sind.

2.2.3 Rahmenbedingungen

2.2.3.1 Kompetenzentwicklung

Kompetenzen spielen eine zentrale Rolle in der Diskussion um digitale Souveränität (Bitkom 2015; BMWi 2017; Schiefdecker und March 2021; Büchel und Mertens 2021). Denn nur wenn im eigenen Land die nötigen Kompetenzen vorhanden sind bzw. Unternehmen auf diese zugreifen können, sind Unternehmen in der Lage, Schlüsseltechnologien zu entwickeln, zu produzieren und souverän zu nutzen. Kompetenzen beziehen sich dabei zum einen auf grundlegende Digitalkompetenzen, deren es in der Anwendung und Bedienung digitaler Technologien bedarf. Darüber hinaus sind auch Technikkompetenzen wichtig, d.h. ein technisches Grundverständnis der Funktionsweise digitaler Technologien zu besitzen. Zum anderen müssen genügend Fachkräfte zur Verfügung stehen, die die entsprechenden fortgeschrittenen Digitalkompetenzen bzw. technischen Fachkompetenzen zur Erforschung, Entwicklung, Produktion und Veredelung von digitalen Technologien haben. Deshalb erfolgt nachfolgend eine Bestandsaufnahme zu digitalen Kompetenzen in Deutschland sowie zu Aktivitäten zur Kompetenzentwicklung, mit einem Fokus auf Erwachsenenbildung und der betrieblichen Ebene (Weiterbildung), als wichtige Rahmenbedingung für eine digital souveräne Wirtschaft.

Das Vorhandensein von grundlegenden und fortgeschrittenen digitalen Kompetenzen auf dem Arbeitsmarkt ist für eine digital souveräne Wirtschaft von enormer Bedeutung. Auf europäischer Ebene untersucht der DESI-Index in der Dimension Humankapital sowohl das Vorhandensein grundlegender als auch fortgeschrittener Digitalkompetenzen in den europäischen Ländern (Europäische Kommission 2020b). Deutschland liegt hier insgesamt im guten Mittelfeld auf Rang 10 und somit leicht über dem EU-Durchschnitt. Im Ländervergleich offenbart sich, dass es innerhalb der EU große Differenzen in den Niveaus gibt. So sind einige europäische Länder, insbesondere Italien, Rumänien und Bulgarien, in Bezug auf digitale Kompetenzen relativ weit abgeschlagen. Auch die PIAAC-Studie (Programme for the International Assessment of Adult Competencies) zeigt, dass Erwachsene in Deutschland beim technologiebasierten Problemlösen[6] im internationalen Vergleich nur im Mittelfeld liegen (Rammstedt et al. 2015).

[6] Technologiebasiertes Problemlösen wird definiert als „die Verwendung von digitalen Technologien, Kommunikationswerkzeugen und Netzwerken mit dem Ziel, Informationen zu beschaffen und zu bewerten, mit anderen zu kommunizieren sowie alltagsbezogene Aufgaben zu bewältigen".

Innerhalb Deutschlands veröffentlicht der D21 Index jährlich ein Lagebild zur digitalen Gesellschaft. In der diesjährigen Ausgabe (2021a) zeigt sich, dass die Nutzung digitaler Technologien zwar deutlich steigt, sich die Kompetenz im Umgang mit digitaler Technik und Medien aber auf ähnlichem Niveau wie in den Vorjahren befindet. Ohne Vorerfahrungen und grundlegendes Verständnis der Funktionsweise ist es jedoch schwer, digitale Inhalte und Angebote zu bewerten. Der Umgang mit digitalen Medien und Anwendungen sollte jedoch nicht unreflektiert geschehen, denn neben den positiven Effekten für die gesellschaftliche Teilhabe sollten auch die verbundenen Risiken im Blick bleiben (Initiative D21 2021a). Auch eine Zusatzanalyse der Initiative D21 zeigt, dass sich lediglich drei von fünf deutsche Bürgerinnen und Bürger in der Lage sehen, die Seriosität einer Nachricht im Internet einzuschätzen (Initiative D21 2021b). Mehr als die Hälfte (60 Prozent) weiß nicht, wie sie eine Videokonferenz einrichten können. Wiederum weniger als die Hälfte traut sich zu, sich digitale Kompetenzen selbst anzueignen. So mangelt es an Verständnis- und Handlungskompetenz, die jedoch für das souveräne Handeln und Entscheiden im digitalen Raum von enormer Bedeutung sind.

In Bezug auf fortgeschrittene digitale Kompetenzen bzw. technische Fachkompetenzen in Deutschland gibt es unterschiedliche Prognosen. Obwohl die Zahlen zum genauen Ausmaß des Fachkräfteengpasses heterogen sind, besteht der Konsens, dass der Bedarf an digitalen Kompetenzen steigt und dieser Bedarf nicht vollständig gedeckt werden kann (IW Köln 2021; Bundesagentur für Arbeit 2020, 2021). Aktuelle Zahlen zeigen, dass schon heute Fachkräfte fehlen: Der MINT-Herbstreport (IW Köln 2021) kommt zu dem Ergebnis, dass bundesweit über sämtliche Anforderungsniveaus mindestens 258.400 offene Stellen in MINT-Berufen nicht besetzt werden konnten. Unter Berücksichtigung des qualifikatorischen Mismatches resultiert für September 2021 eine über sämtliche 36 MINT-Berufskategorien aggregierte Arbeitskräftelücke in Höhe von 262.200 Personen. Mit 119.900 Personen bilden die MINT-Facharbeiterberufe die größte Engpassgruppe, gefolgt von 102.000 Personen im Bereich der MINT-Expertenberufe sowie 40.300 im Bereich der Spezialisten- bzw. Meister- und Technikerberufe. Zudem zeigt sich in der differenzierten Betrachtung nach MINT-Bereichen, dass der Engpass insbesondere in IT-Berufen besonders hoch ist (44.700). Einen höheren Fachkräftemangel weisen nur die Energie-/Elektroberufen mit 78.800 und Berufe im Maschine-/Fahrzeugbau mit 45.100 Personen auf. Um also Schlüsseltechnologien in Deutschland zu beherrschen und diese Kompetenz auch künftig zu erhalten, braucht es noch einiger Anstrengungen, sowohl seitens der Unternehmen als auch des Staates.

Durch die dynamische und rasante Entwicklung von digitalen Technologien gewinnt auch die Weiterbildung im Erwachsenenalter zunehmend an Bedeutung und gilt als „der Schlüssel zur Fachkräftesicherung“ (BMBF 2019). Betrachtet man ganz allgemein Weiterbildungsaktivitäten von deutschen Erwachsenen, zeigt sich ein leicht positiver Trend. Laut aktuellen Ergebnissen des Adult Education Survey (BMBF/Kantar Public et al. 2019), die Weiterbildungsaktivitäten von Erwachsenen untersucht (jedoch ohne konkreten Bezug zu Digitalkompetenzen), hat die Teilnahme der 18- bis 69-jährigen Bevölkerung an non-formaler Weiterbildung deutlich zugenommen. Lag sie 2016 noch bei 47,5 Prozent, waren es 2018 schon 52 Prozent. Die Teilnahme an formalen Bildungsaktivitäten stagniert hingegen. In der AES-Erhebung 2018 gaben 11 Prozent der befragten Erwachsenen an, in den vorangegangenen 12 Monaten an einer formalen Bildungsaktivität teilgenommen zu haben. Informelle Lernaktivitäten wurden 2018 von rund 45 Prozent der Befragten ausgeführt (2016: 44 Prozent). Interessant ist, dass sich informelle Lernaktivitäten am häufigsten auf traditionelle Medien wie Fachzeitschriften und Bücher stützen. 67 Prozent aller informell Lernenden gaben dies als bevorzugt genutztes Lernmedium an. Erst dahinter lagen Lernangebote am Computer oder im Internet mit rund 52 Prozent. Dies ist insofern interessant, als digitale Medien grundsätzlich auch Chancen im Bildungsbereich bieten, z. B. zeit- und ortsflexibler Zugriff, die sowohl in der betrieblichen als auch informellen Weiterbildung genutzt werden sollten.

Die IW-Weiterbildungserhebung untersucht Aktivitäten von Unternehmen in der betrieblichen Weiterbildung und zeigt, dass die Weiterbildungsbeteiligung der deutschen Unternehmen auf einem hohen Niveau liegt (rund 88 Prozent) (Seyda und Placke 2020). Im Jahr 2019 hat sich jeder Mitarbeiter im Durchschnitt 18,3 Stunden weitergebildet. Das ist eine Zeitstunde mehr als 2016. Im Jahr 2019 investierten die Unternehmen 1.236 Euro je Mitarbeiter in Weiterbildung, knapp 16 Prozent mehr als im Jahr 2016. Beim gesamtwirtschaftlichen Investitionsvolumen zeigt sich ein Anstieg um 23 Prozent, somit belaufen sich die Investitionen auf 41,3 Milliarden Euro. Zudem zeigt sich, dass die Digitalisierung ein wesentlicher Treiber für Weiterbildungsaktivitäten darstellt: Digitalisierte Unternehmen investieren mehr Zeit und Geld in Weiterbildung als andere Unternehmen. Neben dem eigenen privatwirtschaftlichen Engagement befürworten rund 70 Prozent der Unternehmen staatliche Unterstützung. Dies gilt insbesondere für Geringqualifizierte, Ältere oder kleine und mittlere Unternehmen, damit der digitale Strukturwandel bewältigt werden kann. Mehr Information und Beratung sollte zudem eingesetzt werden, um bestehende Weiterbildungshemmnisse abzubauen und Menschen für Weiterbildung zu motivieren und Unternehmen sowie Individuen darin zu unterstützen, Weiterbildungsbedarf zu erkennen (Seyda und Placke 2020). Dazu zählt auch, Hilfestellung zu leisten, in welchen Gebieten künftig Weiterbildungsbedarf besteht. So gibt beispielsweise im Eurobarometer (Europäische Kommission 2019) ein Drittel der (deutschen) Umfrageteilnehmer an, dass sie nicht wissen, welche digitalen Kompetenzen sie verbessern sollten. Dies stellt in Deutschland das größte Hemmnis in Bezug auf den Kompetenzerwerb dar, erst danach folgt Zeitmangel (26 Prozent).

Zahlen zur Nutzung von digitalen Medien in der betrieblichen Weiterbildung zeigen, dass mittlerweile über 90 Prozent der weiterbildungsaktiven Unternehmen im Jahr 2019 mindestens ein digitales Lernmedium einsetzten. Im Jahr 2016 waren es erst 84 Prozent. Das relativ hohe Vorkrisenniveau wird voraussichtlich dazu beigetragen haben, dass die Weiterbildungsaktivitäten während des pandemie-bedingten Lockdowns nicht stärker zurückgegangen sind (Seyda 2021). Hier zeigt sich, dass die Nutzung von digitalen Medien in der (Weiter-)Bildung als Chance zu betrachten ist, welche sowohl von Unternehmen als auch von staatlicher Seite weiter gefördert werden sollte.

Zuletzt sind im wirtschaftlichen Kontext auch unternehmenseigene organisationale Kompetenzen im Bereich IT eine Stellschraube, da sie im Krisenfall den Zugang zu Kompetenzen sicherstellen können und eine Abhängigkeit von IT-Dienstleistern vermeiden. Eine Studie (Roth und Helmann 2021) im deutschsprachigen Raum zeigt, dass fast die Hälfte der 144 befragten Chief Information Officer, die bisher Wartungs- und Entwicklungsleistungen auslagern, ihre IT-Eigenleistung wieder erhöhen wollen. Der Grund dafür könnte die zunehmende Digitalisierung sein, die IT für immer mehr Organisationen zu einem Kernbereich macht. Knapp 30 Prozent der Befragten wollen hingegen künftig mehr IT-Services auslagern, um die steigende Komplexität zu beherrschen. Diese Quote ist jedoch im Vorjahresvergleich gesunken. Derzeit beauftragen die meisten Unternehmen Dienstleister aus dem eigenen Land oder aus Europa mit Wartungs- und Entwicklungs-Services. Relativ wenige IT-Verantwortliche kaufen Leistungen aus den USA oder Asien ein, darunter hauptsächlich internationale Konzerne. Ein geringer Teil von ihnen will die Lieferantenstruktur deglobalisieren, wobei sich anteilig mehr Teilnehmende aus den USA als aus Asien zurückziehen wollen. Beides hängt wahrscheinlich mit Themen rund um Datenschutz und Datensouveränität zusammen, die auch dazu geführt haben, dass knapp 45 Prozent der Kundschaft von Cloud-Anbietern aus IT und Business ihre Kapazitäten in Europa aufstocken wollen.

2.2.3.2 Innovationsumfeld

Eine wesentliche Voraussetzung zum Erhalt und zur Stärkung der digitalen Souveränität ist, dass ein innovationsförderndes Umfeld existiert und die Marktbedingungen sowohl etablierten Unternehmen als auch Start-ups erlauben, ihre digitalen Geschäftsmodelle, Produkte und Dienste erfolgreich zu skalieren.

Die F&E-Intensität beschreibt den Umsatzanteil, den Unternehmen jährlich für Forschung und Entwicklung aufwenden. Da Forschung und Entwicklung ein wesentlicher „Input-Faktor" im Innovationsprozess sind und somit die Einführung von Neuheiten positiv beeinflussen, ist die F&E-Intensität ein wichtiger Indikator der Innovationstätigkeit eines Staates oder einer Branche. Deutschland konnte seine F&E-Intensität in den letzten Jahren weiter steigern. Im Jahr 2019 erreichten die F&E-Ausgaben als Anteil am Bruttoinlandsprodukt 3,17 Prozent. Damit liegt Deutschland aber immer noch hinter Ländern wie Südkorea oder Schweden (EFI 2021, S. 97). Ein Branchenvergleich innerhalb der deutschen Wirtschaft (Bertschek et al. 2020) zeigt, dass die IKT-Branche im Jahr 2018 mit einer F&E-Intensität von 5,1 Prozent auf dem dritten Platz liegt. Damit behauptet sich die IKT-Branche neben den traditionell forschungsintensiven Industrien Fahrzeugbau (6,5 Prozent) und Elektrotechnik/Maschinenbau (5,9 Prozent). Der Anteil der Unternehmen, die in den vergangenen drei Jahren mindestens ein neues Produkt oder einen neuen Prozess eingeführt haben („Innovatorenquote"), liegt in der IKT-Branche im Jahr 2018 bei rund 85 Prozent. Dadurch ist die IKT-Branche gemessen an der Innovatorenquote die innovativste Branche Deutschlands – noch vor den Wirtschaftszweigen Elektrotechnik und Maschinenbau (81 Prozent) und Fahrzeugbau (72 Prozent). Weiter gehört die IKT-Branche in Deutschland im Branchenvergleich zu den am stärksten innovationsgetriebenen Wirtschaftszweigen. Über 9 Prozent der IKT-Umsätze flossen 2018 in die Entwicklung und Einführung von Produkt- oder Prozessinnovationen – der zweithöchste Wert für die sogenannte „Innovationsintensität" nach dem Fahrzeugbau (rund 10 Prozent). Damit sind Unternehmen der IKT-Branche im Branchenvergleich und in Bezug auf Innovationsaktivitäten sehr gut aufgestellt, jedoch zeigt sich im internationalen Vergleich weiter Entwicklungspotenzial.

Beim Vergleich der Gründungsraten von acht ausgewählten EU-Ländern auf Basis von Eurostat-Daten liegt Deutschland sowohl gesamtwirtschaftlich (6,8 Prozent) als auch in den wissensintensiven Dienstleistungen (8 Prozent) auf Rang sechs, in der F&E-intensiven Industrie (3,4 Prozent) an achter Stelle (EFI 2021, S. 109). Im innerdeutschen Branchenvergleich (Bertschek et al. 2020) liegt die IKT-Branche mit einer Gründungsrate von 6,1 Prozent (Mittelwert für die vergangenen drei Jahre) auf dem zweiten Platz und damit nur knapp hinter der Tourismusbranche (6,3 Prozent), aber noch deutlich vor dem Bereich Verkehr und Logistik (5,6 Prozent). Die Gründungsrate beschreibt dabei den Anteil der Unternehmen, die bezogen auf den Gesamtbestand in einer Branche in einem Jahr neu gegründet wurden. Auch ein Blick auf die Gründungsdynamik zeigt die Bedeutung der IKT-Branche als Innovationstreiber, denn diese ist in der IKT-Branche günstiger als in der Gesamtwirtschaft. Demnach entwickelt sich die IKT-Branche in Deutschland positiv, jedoch bedarf es weiterer Anstrengungen um Gründungen zu fördern und so im internationalen Vergleich aufzuschließen.

In Bereichen wie Servicerobotik, Künstliche Intelligenz, autonome Systeme, Cybersicherheitsapplikationen, E-Government und digitale Geschäftsmodelle hat Deutschland bereits technologische Rückstände zu verzeichnen (EFI 2021, S. 33). Diese gilt es aufzuholen, zudem ist darauf zu achten, dass bei potenziellen Schlüsseltechnologien keine Rückstände entstehen. Als Hemmnis für die Gründung von Unternehmen und deren Wachstum wird u.a. nicht in ausreichendem Umfang zur Verfügung stehendes Gründungs- und Wachstumskapital gesehen.

Die Bundesregierung hat mit der Einführung der steuerlichen F&E-Förderung sowie mit der Gründung der Agentur für Sprunginnovationen Maßnahmen ergriffen, um die Forschungs- und Innovationsaktivität von Unternehmen sowohl in der Breite als auch im Bereich der Hochrisiko-Forschung verstärkt zu fördern. Zudem hat sie Mittel für die Förderung von Zukunftstechnologien wie der Künstlichen Intelligenz und Quantencomputer bereitgestellt. Der neu aufgesetzte Zukunftsfonds soll zudem darauf abzielen, die Rahmenbedingungen für Wagnis- und Wachstumskapital zu verbessern. Jedoch stellen auch Länder wie China und die USA Mittel bereit. Daher sollten die aufgesetzten Maßnahmen evaluiert und gegebenenfalls angepasst werden.

2.2.3.3 Regulatorisch

Die Schaffung eines Marktumfeldes, das den Erhalt und die Stärkung der digitalen Souveränität sowie einen fairen Wettbewerb fördert, bedarf geeigneter regulatorischer Rahmenbedingungen. In diesem Kontext wird die Realisierung des Digitalen Binnenmarktes in Europa und seine Bedeutung zum Erhalt und zur Stärkung der digitalen Souveränität vielfach diskutiert. Dies hat im Wesentlichen zwei Gründe: Erstens sind die digitale Wirtschaft und der Handel im Cyberraum transnational ausgelegt, so dass nur durch einen europäischen Binnenmarkt sichergestellt werden kann, dass Unternehmen innerhalb der gesamten EU nach gemeinsamen Regeln und hohen gemeinsamen Sicherheits-, Verbraucher- und Datenschutzstandards handeln. Zweitens bringt der digitale Binnenmarkt in Europa internationale Wettbewerbsvorteile. Denn digitale Innovationen können so besser entwickelt und skaliert werden, da einzelne Nationalstaaten dafür zu klein sind, der europäische Binnenmarkt aber in Summe rund 450 Millionen Bürgerinnen und Bürgern umfasst (BMWi 2021a; Eurostat 2020). Auch wenn ein gemeinsames Vorgehen der EU die Souveränität einzelner Staaten einschränkt, stärkt die Zusammenarbeit die Souveränität der EU nach außen: Denn kein europäischer Nationalstaat ist groß genug um als Gegengewicht zu Großmächten wie der USA oder China agieren zu können.

Bereits 2015 wurde von der Europäischen Kommission eine Strategie zur Schaffung eines digitalen Binnenmarkts vorgestellt. Diese umfasst 16 Initiativen, z. B. eine Partnerschaft mit der Industrie zum Thema Cybersicherheit im Bereich Technologien und Lösungen für die Netzsicherheit oder die Unterbindung von ungerechtfertigtem Geoblocking. Zwar ist die Umsetzung im Gange, aber wird noch einige Zeit in Anspruch nehmen. Erste umgesetzte Maßnahmen, wie etwa die Regulierung von Geoblocking, sind Ergebnissen einer Studie zufolge effektiv gewesen und haben zu einem Wachstum des länderübergreifenden Online-Handels (innerhalb der EU und international) geführt (Alaveres et al. 2020).

Auch für den Erfolg plattformbasierter Ökosysteme ist ein ausgewogener Regulierungsrahmen erforderlich, der einerseits das Entstehen von Digitalplattformen in der EU fördert und gleichzeitig Marktmachtmissbrauch und Datenmonopole verhindert (Gesellschaft für Informatik 2020). Hier wurden mit dem Digital Markets Act bereits die Weichen gestellt (Europäische Kommission 2020a). Wettbewerbsrechtlich kommt künftig zudem einer Berücksichtigung der digitalen Souveränität Europas bei der Genehmigung von Übernahmen durch nicht-europäische Unternehmen eine hohe Bedeutung zu. Eine Genehmigung von Übernahmeplänen durch europäische Aufsichtsbehörden sollte daher Auflagen beinhalten, mit denen sowohl der Zugang zu wichtigem geistigen Eigentum als auch Know-how zu bestimmten Technologiesegmenten erhalten bleiben (Kagermann et al. 2021).

Wichtig ist jedoch auch, dass es nicht zu einer Überregulierung kommt. So geben Chief Information Officer aus deutschsprachigen Unternehmen in einer Umfrage (Roth und Helmann 2021) an, dass der Haupttreiber steigender Komplexität in der Unternehmens-IT die zunehmende Zahl von gesetzlichen Regelungen und

Vorgaben darstellt. In diesem Zusammenhang sei auch der Abbau regulatorischer Hürden erwähnt, um Markteintrittsbarrieren für KMUs und Startups zu reduzieren (vgl. Kapitel 2.2.3.2). Gleichzeitig erfordert die digitale Souveränität einen ganzheitlichen Politikansatz, der die unterschiedlichen Wertschöpfungsstufen im Innovationsprozess sowie die verschiedenen Akteure berücksichtigt (BMBF 2021).

2.2.3.4 Gesellschaftlich

Auch eine Offenheit gegenüber sowie ein Vertrauen in digitale Technologien und Unternehmen, die solche nutzen, sind für eine digital souveräne Wirtschaft von hoher Bedeutung. Denn nur so kann der Absatz der entsprechenden Produkte und Dienste sichergestellt werden.

In Bezug auf eine Offenheit gegenüber neuen Technologien zeichnet eine Umfrage unter Erwerbstätigen in deutschen Unternehmen ein grundsätzlich positives Bild (Grzymek und Wintermann 2020). So stimmen die Befragten über alle Altersgruppen hinweg zu, dass in ihrem Arbeitsumfeld eine grundsätzliche Offenheit gegenüber der Digitalisierung besteht. Beim Wunsch nach stärker digital ausgerichtetem Arbeiten und bei der Einschätzung des Potenzials und Nutzens der digitalen Transformation nimmt die jüngere Generation aber eine deutlich positivere Haltung ein als ältere Altersgruppen. Während sich 47 Prozent der 16- bis 29-jährigen Erwerbstätigen ein moderneres und digitaleres Arbeitsumfeld wünschen, lehnt die Hälfte der über 60-Jährigen (51 Prozent) dies ab. So ist anzunehmen, dass die betriebliche digitale Transformation zunehmend an Dynamik gewinnen wird, je mehr Personen aus der jüngeren (digital offeneren) Generation in Unternehmen Positionen mit Entscheidungskompetenzen innehalten.

Ergebnisse aus dem D21 Digital Index (2021a) zeigen ein gemischtes Bild in Bezug auf das Vertrauen von deutschen Bürgerinnen und Bürgern in digitale Technologien. Im Bereich der digitalen Gesundheit vertraut knapp die Hälfte darauf, dass gesetzliche Vorgaben für Datenschutz und Datensicherheit eingehalten werden. Außerdem gibt fast die Hälfte der Befragten an, dass sie digitale Dienste nutzen, deren Anbietern sie nicht wirklich trauen. Gleichzeitig ist das Zutrauen in Schulen beim Vermitteln benötigter Digitalisierungsfähigkeiten nur gering ausgeprägt (32 Prozent), die Tendenz sogar rückläufig. Wiederum ein gutes Drittel befürchtet die Gefährdung der Demokratie durch Digitalisierung.

Eine Studie von Bitkom (2020a) sieht zumindest im Bereich Datensicherheit eine positive Tendenz in Bezug auf das Vertrauen von Konsumenten in Deutschland. So geben 27 Prozent der Umfrageteilnehmer (Internetnutzer in Deutschland ab 14 Jahre) an, dass sie ihre persönlichen Daten im Internet im Allgemeinen als sehr sicher oder sicher empfinden. Dies entspricht einem neuen Höchststand seit Beginn der Studie im Jahr 2014. Nichtsdestotrotz empfinden nach wie vor 72 Prozent der Teilnehmer, dass ihre Daten im Internet eher unsicher oder völlig unsicher sind. Besonders stark vertrauen die Teilnehmer zudem Herstellern oder Anbietern aus Deutschland (60 Prozent sehr stark oder stark) und anderen Mitgliedstaaten der EU (48 Prozent) im Vergleich zu den USA (27 Prozent) oder China (21 Prozent).

Auch die Bereitschaft der Bundesbürger die eigenen persönlichen Daten zum Zwecke der Wissenschaft, z. B. im medizinischen Bereich, zu teilen, ist Randbedingung einer digital souveränen Wirtschaft. Denn durch „Datenspenden“ kann die Datenmenge erhöht und Datenqualität verbessert werden, was wiederum bei der Entwicklung von Algorithmen förderlich ist. Laut Eurobarometer (2020) sind Bürgerinnen und Bürger insbesondere im Bereich der medizinischen Forschung (44 Prozent) bereit, ihre persönlichen Daten zu spenden. Rund 36 Prozent sind jedoch grundsätzlich nicht bereit, egal für welchen Zweck, ihre personenbezogenen

Daten zu teilen. Somit muss an dieser Stelle noch Vertrauensarbeit geleistet werden, dass Bürgerinnen und Bürger sicher sein können, dass ihre Daten nicht missbraucht werden.

Es zeigt sich insgesamt eine gesellschaftliche Zurückhaltung bezogen auf digitale Technologien. Zwar ist eine positive Entwicklung in Bezug auf Offenheit und Vertrauen in unterschiedlichen Bereichen zu verzeichnen, doch bleibt ein nicht zu vernachlässigender Anteil der Bundesbürger digitalen Technologien gegenüber skeptisch. Hier sind sowohl staatliche Akteure als auch Unternehmen gefragt, die Vertrauensbildung zu fördern, z. B. durch Informationsmaßnahmen, Teilhabe oder Transparenz und Nachvollziehbarkeit.

2.2.4 Fazit zur Literaturübersicht

Im Rahmen der Literaturübersicht wurde zum einen die Diskussion um den Begriff der digitalen Souveränität zusammengefasst, um die Bedeutung des Konzepts sowie die Beweggründe für den Ruf nach mehr digitaler Souveränität zu verdeutlichen. Zum anderen wurde auf Basis bestehender Studien eine Bestandsaufnahme der Abhängigkeitsstrukturen zu anderen (insbesondere nicht-europäischen) Staaten im Bereich der digitalen Technologien herausgearbeitet und Anbieter- und Anwenderkompetenzen in Deutschland und Europa untersucht.

Trotz der Vielzahl an Impulspapieren zum Thema digitale Souveränität herrscht noch keine Einigkeit darüber, was digitale Souveränität im Kern bedeutet. Dennoch besteht der Konsens, dass digitale Souveränität grundsätzlich auf unterschiedlichen Handlungsebenen untersucht werden kann; dass digitale Souveränität keiner Eins-Null-Logik folgt, sondern graduelle Ausprägungen zulässt; und dass sich der Begriff durch eine Vielschichtigkeit und Ambiguität kennzeichnet, was eine Herausforderung für die empirische Erfassung und Bestimmung einer „vollständigen“ Souveränität darstellt.

Zudem herrscht Einigkeit darüber, dass das übergeordnete Ziel des Erhalts und der Stärkung digitaler Souveränität der Wirtschaft die Sicherung ihrer Handlungsfähigkeit und Zukunftsfähigkeit (d.h. Wettbewerbs- und Innovationsfähigkeit) in einer digitalen Welt darstellt. Dafür sind zwei Aspekte von zentraler Bedeutung: Dies ist zum einen die Verfügbarkeit von oder der Zugang zu geeigneten digitalen Technologien und Daten. Dies wird sichergestellt, indem digitale Technologien entweder im eigenen Land produziert werden oder indem der Zugang zu diesen, auch in Krisenzeiten, abgesichert ist. Dafür sind Herstellungs- und Entwicklungskompetenzen von deutschen und europäischen Unternehmen in relevanten Technologiefeldern und Schlüsseltechnologien (Anbieterkompetenzen) von zentraler Bedeutung, um zum einen die Verfügbarkeit von Technologien und Daten zu gewährleisten und zum anderen die Digitalisierung der Wirtschaft im Sinne europäischer Rechts- und Wertevorstellungen mitzugestalten. Nichtsdestotrotz wird explizit keine vollständige Unabhängigkeit im Sinne einer Autarkie in allen (Technologie-)Bereichen und ausschließlich im eigenen Land produzierter Lösungen (d.h. Protektionismus) angestrebt. Zum anderen ist der souveräne – d.h. selbstbestimmte, sichere und reflektierte – Umgang mit digitalen Technologien eine Voraussetzung für eine digital souveräne Wirtschaft. Diese Handlungs- und Entscheidungskompetenzen im digitalen Raum (Anwendungskompetenzen) beziehen sich auf die Fähigkeit, die Digitalisierung des eigenen Unternehmens selbstbestimmt, verantwortungsvoll und sicher zu gestalten und die Potenziale digitaler Technologien zu heben, demnach die unternehmenseigene Handlungs- und Wettbewerbsfähigkeit beizubehalten.

Auf der Basis dieses Verständnisses von digitaler Souveränität wurden sechs zentrale Technologiefelder identifiziert - (1) Hardware/Infrastruktur, (2) Software/Anwendungen, (3) Künstliche Intelligenz, (4) IT-

Sicherheit, (5) Digitale Plattformen, (6) Daten – und in diesen Teilbereichen eine Bestandsaufnahme der gegenwärtigen Abhängigkeitsstrukturen und Anbieter- und Anwenderkompetenzen in Europa und insbesondere in Deutschland durchgeführt. Insgesamt zeigen sich in allen Technologiefeldern teils erhebliche Abhängigkeiten zu nicht-europäischen Staaten, insbesondere den USA und China. So existieren in Deutschland zwar Stärken in den Bereichen B2B-Plattformen, IT-Sicherheit, energieeffiziente Rechenzentren sowie in der wissenschaftlichen Erforschung (z. B. im Bereich KI und IT-Sicherheit). Dennoch sind die Handlungsfähigkeit und Zukunftsfähigkeit der deutschen Wirtschaft durch kritische Abhängigkeiten in den Bereichen Komponenten (Mikrochips), (Daten-)Infrastruktur (Hyperscaler) und digitale B2C-Plattformen eingeschränkt oder gefährdet. Auch im Bereich der betrachteten Zukunfts- und Schlüsseltechnologien, Quantencomputer und Künstliche Intelligenz, besteht die Gefahr, dass China und die USA den Wettkampf um die Technologieführerschaft gewinnen. Insgesamt zeigt sich also die hohe Bedeutung von leistungsfähigen Alternativen aus Deutschland und der EU, die sich durch Qualität, Sicherheit und Verlässlichkeit als Markenzeichen deutscher und europäischer Produkte kennzeichnen. Gleichzeitig wird betont, dass nicht in allen Bereichen die technologischen Aktivitäten erhöht und versucht werden sollte, technologische Vorsprünge anderer Länder aufzuholen. Stattdessen sollte auf die bestehenden Stärken Deutschlands aufgebaut werden – etwa im Bereich der industriellen B2B-Plattformen, Zukunftstechnologien (z. B. Quantencomputer) und neuartigen Produktkategorien (z. B. spezialisierte Chiptypen) – so dass wechselseitige Abhängigkeiten entstehen.

Anwenderseitig, d.h. bezogen auf den souveränen Umgang mit digitalen Technologien, zeigt sich ebenfalls ein gemischtes Bild. Zum einen wird in diversen Studien und bezogen auf unterschiedliche Technologiefelder deutlich, dass ein Teil der deutschen Unternehmen die wirtschaftlichen Chancen digitaler Technologien sowie deren Risiken erkannt hat und Maßnahmen einleitet, um Abhängigkeiten zu Anbietern zu reduzieren und so einen Lock-in zu vermeiden. Beispiele sind die vermehrte Nutzung von Open-Source-Software, Multi- oder Hybrid-Cloud-Strategien zur Vermeidung von Abhängigkeiten zu den zentralen Cloud-Anbietern oder teilweise und wenn sinnvoll auch die Eigenentwicklung bzw. der Eigenbetrieb. Zum anderen gilt dies nicht für alle Unternehmen gleichermaßen. Insbesondere kleine und mittlere Unternehmen hinken in Bereichen wie etwa Maßnahmen zur Stärkung der IT-Sicherheit oder der Entwicklung von konkreten Strategien im Umgang mit Technologien hinterher. Gleichzeitig mangelt es vielen Unternehmen an grundlegenden als auch fortgeschrittenen digitalen Kompetenzen und einer Kultur, die die Chancen neuer Technologien begreift und offen gegenübersteht (z. B. im Bereich der Daten).

Das Kernproblem im Kontext der digitalen Souveränität der Unternehmen bleibt ein Zielkonflikt, der derzeit in vielen Bereichen besteht: Die Wahl zwischen der leistungsstärksten und der vertrauenswürdigsten, sichersten Lösung. So ist weder eine komplette Abschottung durch Insellösungen in allen Technologiebereichen eine erstrebenswerte und umsetzbare Lösung, denn dies erschwert den Austausch von technologischem Wissen und Kooperationen. Gleichzeitig sind Insellösungen kostspielig und gegebenenfalls von verminderter Leistungsfähigkeit, so dass wiederum die Wettbewerbsfähigkeit eingeschränkt ist. Jedoch ist auch die Nutzung von EU-Alternativen, wenn diese nicht mit der Leistungsfähigkeit nicht-europäischer Anbieter konkurrieren können, wenig förderlich für die Wettbewerbs- und Innovationsfähigkeit – trotz höherer Sicherheitsanforderungen.

In Summe zeigt sich, dass nicht die eine, für alle Anwender und alle Einsatzfälle optimale Lösung in jedem Technologiefeld existiert. Vielmehr bleibt es eine individuelle Entscheidung und ein Abwägen von Aufwand und Risiken in der Gesamtbetrachtung. So muss jedes Unternehmen für sich und auf Basis der eigenen

Rahmenbedingungen austarieren, in welchen Bereichen es mehr Unabhängigkeit im Allgemeinen und speziell von nicht-europäischen Anbietern anstrebt – beispielsweise eine Open-Source-Software statt Microsoft-Office nutzt. Doch im Kern zeichnet genau diese Entscheidungs- und Handlungskompetenz auch das digital souveräne Unternehmen aus: Überhaupt eine Wahlfreiheit zu besitzen und nicht fremdbestimmt und durch hohe Wechselbarrieren handlungsunfähig zu sein, die bewusste Entscheidung für oder gegen eine Technologie sowie in der Konsequenz die effektive Umsetzung der Entscheidung und der verantwortungsvolle, sichere Umgang mit der entsprechenden Lösung.

Um Anbieter- und Anwenderkompetenzen in Deutschland und Europa zu stärken, bedarf es entsprechender Rahmenbedingungen, welche ebenfalls Gegenstand der Untersuchung waren. Die Bestandsaufnahme der gegenwärtigen digitalen Kompetenzen in Deutschland und entsprechender Maßnahmen seitens der Unternehmen und des Staates zeigen, dass hier noch Verbesserungspotenzial besteht – insbesondere vor dem Hintergrund des bestehenden und sich weiter verschärfenden Fachkräftemangels. Auch beim Innovationsumfeld gibt es Handlungsbedarf. So gilt es weiter gründungs- und innovationsfreundliche Rahmenbedingungen zu schaffen. Denn nur durch Innovationen und Neugründungen kann eine Vorreiterrolle in Schlüsseltechnologien erreicht werden. Beim regulatorischen Rahmen zeigt sich, dass erkannt wurde, dass digitale Souveränität nur durch einen gemeinsamen Kraftakt aller EU-Mitgliedstaaten erreicht werden kann. So wurden auf europäischer Ebene zwar die richtigen Weichen gestellt – etwa Bemühungen zur Schaffung eines europäischen Binnenmarkts für bessere Skalierungsmöglichkeiten von Innovationen, die Regulierung von Plattformmärkten für einen freien, fairen Wettbewerb oder die europäische Cloud- und Daten-Infrastruktur GAIA-X. Doch gilt es hier zum einen die Maßnahmen schnell und effektiv umzusetzen und zum anderen die Bekanntheit in der Wirtschaft zu steigern. Letztlich sind auch die gesellschaftlichen Rahmenbedingungen wichtig, d.h. Offenheit und Vertrauen gegenüber digitalen Technologien und Unternehmen, die diese verwenden. Zwar zeigt sich hier in Studien eine stetige, wenn auch inkrementelle Verbesserung, doch besteht weiter Aufklärungsbedarf und ein stärkeres Bewusstsein für die Chancen und Risiken von digitalen Technologien. Dazu zählt auch, unter welchen Umständen Verbraucher die eigene Souveränität zugunsten der Wirtschaft (z. B. in Bezug auf Datenspenden von personenbezogenen Daten) einschränken sollten. Andersrum sind Unternehmen in der Pflicht, digitale Lösungen transparent, nachvollziehbar und nach europäischen Rechts- und Wertevorstellungen zu gestalten, so dass Vertrauen seitens der Verbraucher entstehen kann.

3. Unternehmensbefragung

3.1 Zielsetzung und Methodik

Im Rahmen der Literaturrecherche wurde eine Bestandsaufnahme der Anbieter- und Anwenderkompetenzen in Deutschland und der EU und der Rahmenbedingungen durchgeführt und dadurch wichtige Stellschrauben zum Erhalt und zur Stärkung digitaler Souveränität identifiziert. Aufbauend auf den Erkenntnissen der Literaturrecherche hat das ZEW Mannheim eine repräsentative Unternehmensbefragung durchgeführt. Hiermit soll untersucht werden,

- inwieweit die Unternehmen mit dem Begriff der digitalen Souveränität vertraut sind und ob sie das Thema, für ihr eigenes Unternehmen sowie für die deutsche Wirtschaft insgesamt, für relevant halten,
- ob Abhängigkeiten in zentralen Technologiefeldern bestehen und welche Gründe es dafür gibt,
- inwiefern Unternehmen, die Abhängigkeiten empfinden, Maßnahmen zum Erhalt und zur Stärkung der digitalen Souveränität planen,
- in welchen Bereichen die Bundesregierung die höchste Priorität zum Erhalt und zur Stärkung der digitalen Souveränität der deutschen Wirtschaft setzen sollte.

Befragt wurden Unternehmen in der „Informationswirtschaft“ (IKT-Branche, Mediendienstleister, wissensintensive Dienstleister) und im „Verarbeitenden Gewerbe“ (Chemie und Pharma, Fahrzeugbau, Maschinenbau, Sonstiges Verarbeitendes Gewerbe). Dazu wurde die quartalsweise erhobene ZEW-Konjunkturumfrage in der Informationswirtschaft im zweiten Quartal 2021 um das Verarbeitende Gewerbe erweitert. Die Unternehmen hatten die Wahl, den Fragebogen schriftlich oder online auszufüllen. Insgesamt konnten 1.219 Unternehmen mit mindestens fünf Beschäftigten zum Thema digitale Souveränität befragt werden. Um die Repräsentativität der Befragungsergebnisse zu gewährleisten, erfolgt eine Hochrechnung der Antworten der Umfrageteilnehmer.

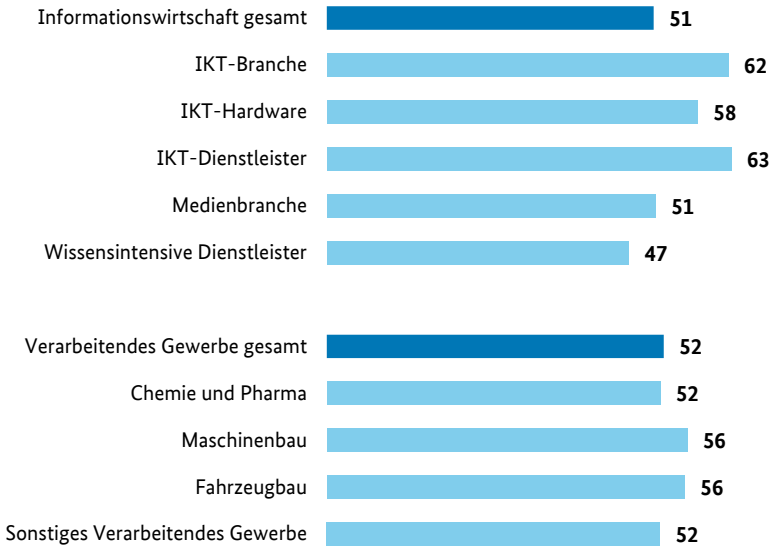
3.2 Ergebnisse

3.2.1 Jedes zweite Unternehmen kennt den Begriff „Digitale Souveränität“

Zur Klärung des Begriffs wurde den Umfrageteilnehmern zunächst die folgende, vereinfachte Definition von Digitaler Souveränität genannt: „*Digitale Souveränität beschreibt die Fähigkeit, die digitale Transformation mit Blick auf Hardware, Software, Dienstleistungen sowie Kompetenzen selbstbestimmt zu gestalten. Dies bedeutet in Bezug auf digitale Technologien und Anwendungen selbstständig entscheiden zu können, inwieweit man eine Abhängigkeit von Anbietern und Partnern eingeht oder vermeidet*“.

Die Befragung zeigt, dass jedes zweite Unternehmen den Begriff „Digitale Souveränität“ bereits kennt (51 Prozent in der Informationswirtschaft und 52 Prozent im Verarbeitenden Gewerbe). Das Thema digitale Souveränität ist also in den betrachteten Wirtschaftszweigen angekommen, aber noch nicht flächendeckend verbreitet.

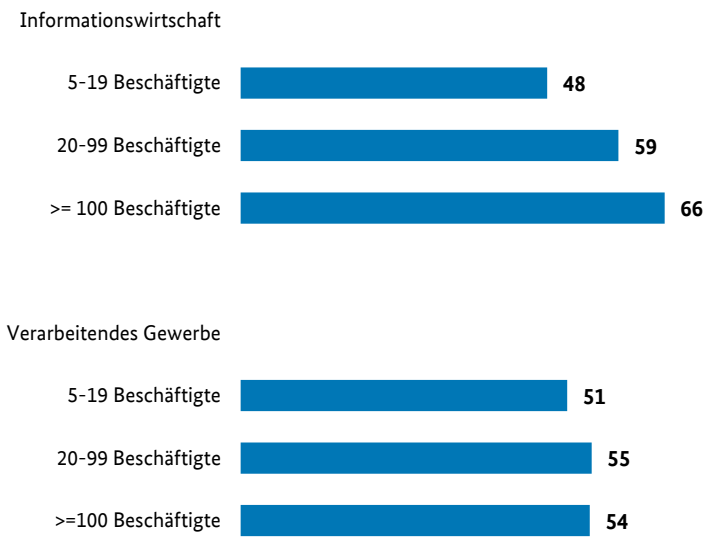
Abbildung 1: Bekanntheit des Begriffs „Digitale Souveränität“ (Anteil der Unternehmen, die den Begriff kennen, in Prozent)



Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Ist Ihnen der Begriff Digitale Souveränität bekannt?

Die Bekanntheit des Begriffs steigt zudem mit der Unternehmensgröße. Während in der Informationswirtschaft nur etwa jedes zweite kleine Unternehmen (5 bis 19 Beschäftigte) den Begriff kennt, ist es bei den großen Unternehmen (100 oder mehr Beschäftigte) bereits jedes dritte Unternehmen (66 Prozent). Im Verarbeitenden Gewerbe ist diese Tendenz abgeschwächt zu erkennen, jedoch ist der Begriff bei mittleren und großen Unternehmen mit 55 bzw. 54 Prozent ebenfalls etwas bekannter als bei kleinen Unternehmen (51 Prozent).

Abbildung 2: Bekanntheit des Begriffs „Digitale Souveränität“ nach Unternehmensgröße (Anteil der Unternehmen in Prozent)



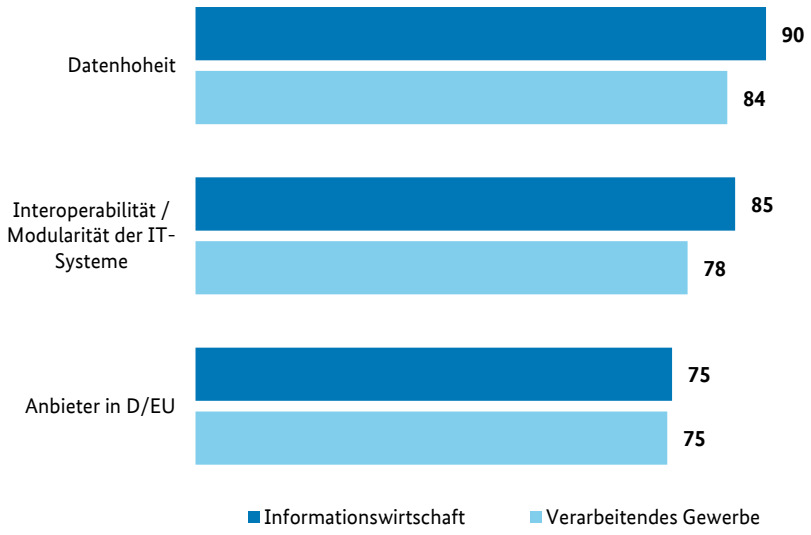
Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Ist Ihnen der Begriff Digitale Souveränität bekannt?

3.2.2 Datenhoheit ist wichtigstes Merkmal einer Digitalen Souveränität

Die Unternehmen wurden nach der Relevanz einzelner, beispielhafter Merkmale, die mit einer hohen digitalen Souveränität verbunden sind (BMWi 2017), für das eigene Unternehmen befragt. Das erste Merkmal bezieht sich auf den Standort der Anbieter von digitalen Technologien/Anwendungen in Deutschland oder der EU. Das zweite Merkmal beschreibt den Aspekt der Interoperabilität und Modularität von IT-Systemen, d.h. dass bestehende IT-Systeme möglichst nahtlos zusammenarbeiten und Komponenten mit geringem Aufwand angepasst und durch andere ersetzt werden können. Das dritte und letzte Merkmal bezieht sich auf die Datenhoheit, also dass die von digitalen Technologien/Anwendungen gespeicherten und verarbeiteten Daten vor unbefugtem Zugriff geschützt sind und jederzeit in andere Systeme übertragen werden können.

Die überwiegende Mehrheit der Unternehmen in beiden Wirtschaftszweigen (mindestens 75 Prozent) hält alle drei Merkmale für wichtig für das eigene Unternehmen. Die Rangfolge ist dabei in beiden Wirtschaftszweigen gleich: Besonders wichtig ist der Aspekt der Datenhoheit. In der Informationswirtschaft geben 90 Prozent und im Verarbeitenden Gewerbe 84 Prozent der Unternehmen an, dass der Aspekt der Datenhoheit für das eigene Unternehmen eine hohe Bedeutung besitzt. Auch die Interoperabilität ist den Unternehmen sehr wichtig: In der Informationswirtschaft bejahen 85 Prozent und im Verarbeitenden Gewerbe 78 Prozent der Unternehmen, dass die Interoperabilität und Modularität von IT-Systemen für das eigene Unternehmen von hoher Bedeutung ist. An dritter Stelle, aber dennoch mit hohen Zustimmungswerten, steht bei beiden Wirtschaftszweigen mit jeweils rund 75 Prozent der Standort des Anbieters in Deutschland oder der EU. Es zeigt sich, dass Unternehmen diesen Aspekten durchweg eine hohe Bedeutung für das eigene Unternehmen zuschreiben, so dass digitale Souveränität für die Unternehmen durchaus einen hohen Stellenwert hat.

Abbildung 3: Wichtigkeit einzelner Merkmale einer hohen digitalen Souveränität für das eigene Unternehmen (Anteil der Unternehmen in Prozent)



Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Sind die folgenden Merkmale einer hohen Digitalen Souveränität für Ihr Unternehmen wichtig?

3.2.3 Digitale Souveränität gewinnt langfristig weiter an Bedeutung

Um ein konkreteres Bild des Stellenwertes von digitaler Souveränität in deutschen Unternehmen zu erhalten, wurde im Rahmen der Umfrage gefragt, welche Bedeutung das Thema schon heute sowie für den langfristigen Erfolg des eigenen Unternehmens und für die deutsche Wirtschaft hat.

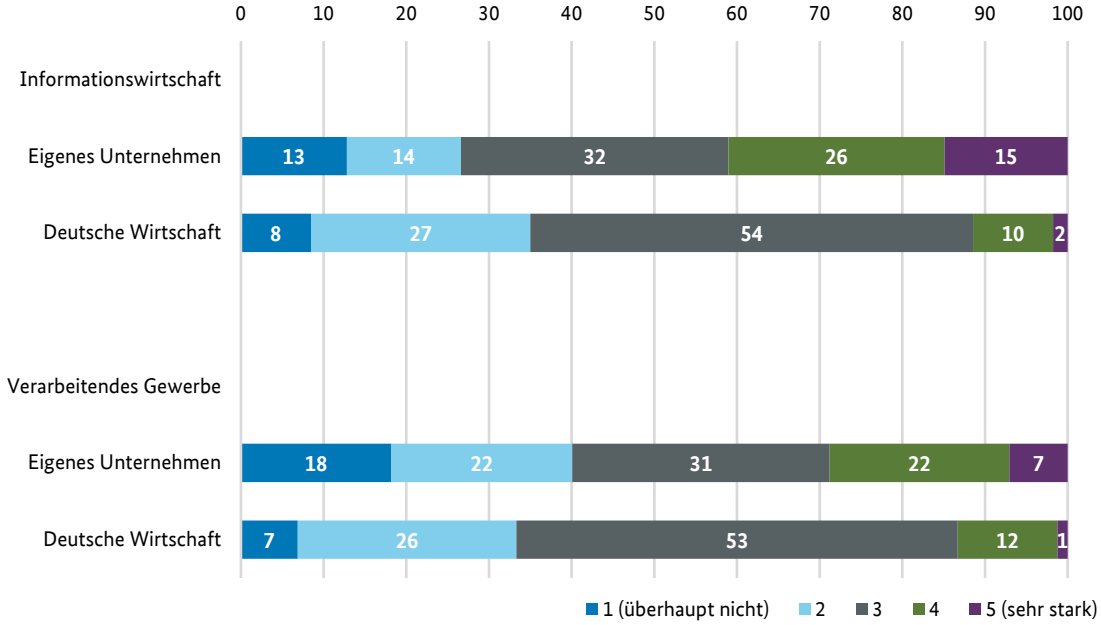
In Bezug auf die aktuelle Berücksichtigung des Themas im eigenen Unternehmen und der deutschen Wirtschaft zeigt sich ein gemischtes Bild – sowohl zwischen als auch innerhalb der Wirtschaftszweige. Während in der Informationswirtschaft 27 Prozent der Unternehmen digitale Souveränität im eigenen Unternehmen aktuell überhaupt nicht oder wenig berücksichtigen, geben 41 Prozent der Unternehmen an, dass das Thema sehr stark oder stark berücksichtigt wird. Bezogen auf die deutsche Wirtschaft nehmen Unternehmen der Informationswirtschaft eine schwächere Berücksichtigung wahr: Nur 12 Prozent geben an, dass digitale Souveränität aktuell sehr stark oder stark in der deutschen Wirtschaft berücksichtigt wird. Jedes dritte Unternehmen (35 Prozent) empfindet hingegen, dass das Thema überhaupt nicht oder wenig in der Wirtschaft berücksichtigt wird.

Im Verarbeitenden Gewerbe findet das Thema derzeit nach Angabe der Unternehmen weniger Berücksichtigung: In 40 Prozent der Unternehmen findet digitale Souveränität überhaupt keine oder wenig Beachtung, in knapp einem Drittel (29 Prozent) hingegen eine starke oder sehr starke Berücksichtigung. Bezogen auf die Gesamtwirtschaft sehen ein Drittel der Unternehmen des Verarbeitenden Gewerbes überhaupt keine oder wenig und nur 13 Prozent eine sehr starke oder starke Berücksichtigung des Themas.

Insgesamt zeigt sich also keine eindeutige Tendenz, was wiederum daran liegen könnte, dass das Thema noch nicht in allen Unternehmen bekannt ist (vgl. 3.2.1). Es zeigt sich dennoch in beiden Wirtschaftszweigen die

Wahrnehmung, dass das Thema in der deutschen Wirtschaft weniger starke Berücksichtigung findet als im eigenen Unternehmen. Zwar ist die Einschätzung der Digitalen Souveränität für die deutsche Wirtschaft insgesamt in beiden Wirtschaftszweigen sehr ähnlich. Jedoch sehen die Unternehmen in der Informationswirtschaft das Thema im eigenen Unternehmen häufiger berücksichtigt als in der gesamten deutschen Wirtschaft. Im Verarbeitenden Gewerbe ist dies umgekehrt.

Abbildung 3: Aktuelle Berücksichtigung des Themas digitale Souveränität im eigenen Unternehmen und in der deutschen Wirtschaft (Anteil der Unternehmen in Prozent)



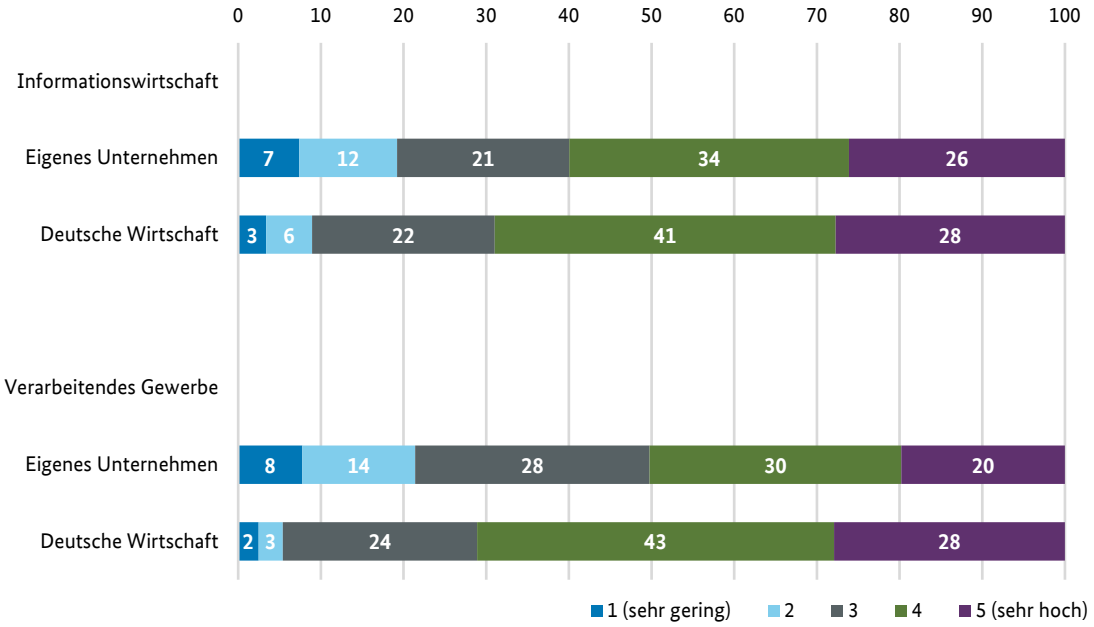
Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Wie stark wird das Thema Digitale Souveränität schon heute berücksichtigt in Ihrem Unternehmen / in der deutschen Wirtschaft?

Bezogen auf den langfristigen Erfolg des eigenen Unternehmens und der deutschen Wirtschaft gibt die Mehrheit der Unternehmen in beiden Wirtschaftszweigen an, dass die Bedeutung digitaler Souveränität hoch oder sehr hoch ist. Obwohl das Thema heute also noch nicht in allen Unternehmen Berücksichtigung findet, wird digitale Souveränität langfristig durchaus als erfolgskritisch angesehen. So sind sowohl in der Informationswirtschaft (60 Prozent) als auch im Verarbeitenden Gewerbe (50 Prozent) die Unternehmen der Meinung, dass digitale Souveränität eine hohe oder sehr hohe Bedeutung für den langfristigen Erfolg des eigenen Unternehmens hat.

Deutlich höher sind die Zustimmungswerte für die gesamte deutsche Wirtschaft und liegen in der Informationswirtschaft bei 69 Prozent und im Verarbeitenden Gewerbe bei 71 Prozent. Insgesamt sehen die Unternehmen das Thema demnach als wichtiger für den Erfolg der gesamten deutschen Wirtschaft als für das eigene Unternehmen an. Dies zeigt sich auch in dem jeweils geringen Anteil an Unternehmen (9 Prozent in der Informationswirtschaft und 5 Prozent im Verarbeitenden Gewerbe), die angeben, dass digitale Souveränität nur eine sehr geringe oder geringe Bedeutung für den langfristigen Erfolg der deutschen Wirtschaft hat.

Insgesamt messen Unternehmen der digitalen Souveränität für die Zukunft eine hohe bis sehr hohe Bedeutung bei, auch wenn das Thema heute noch nicht flächendeckend in den Unternehmen Berücksichtigung findet.

Abbildung 4: Bedeutung des Themas digitale Souveränität für den langfristigen Erfolg des eigenen Unternehmens und der deutschen Wirtschaft (Anteil der Unternehmen in Prozent)



Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Welche Bedeutung messen Sie der Digitalen Souveränität bei für den langfristigen Erfolg Ihres Unternehmens / der deutschen Wirtschaft?

3.2.4 Über 80 Prozent der Unternehmen fühlen sich technologisch abhängig von nicht-europäischen Anbietern/Partnern

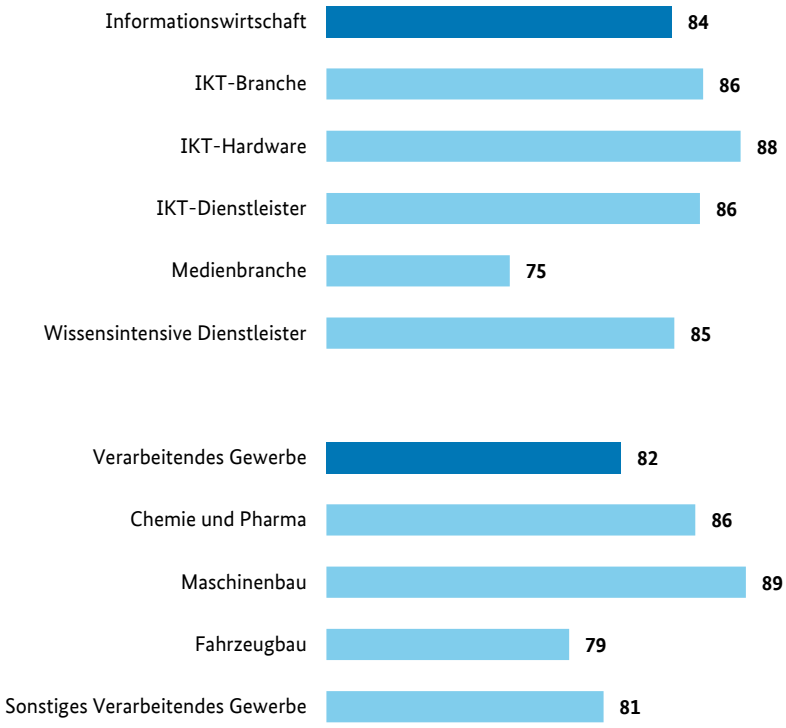
Im Rahmen der Umfrage wurden Unternehmen zudem nach ihrer gefühlten Abhängigkeit zu ausländischen Anbietern/Partnern in sechs Technologiefeldern befragt. Die sechs Technologiefelder lauten Software/Anwendungen, Künstliche Intelligenz, IT-Sicherheitstechnologien, Hardware/Infrastruktur, digitale Plattformen und Daten (Zugriff auf bzw. Verarbeitung von Daten des eigenen Unternehmens).

In beiden Wirtschaftszweigen fühlen sich über 80 Prozent der Unternehmen in mindestens einem der sechs Technologiefelder etwas oder stark abhängig von ausländischen Anbietern/Partnern (84 Prozent in der Informationswirtschaft und 82 Prozent im Verarbeitenden Gewerbe). Dies bestätigt das Bild einer im Bereich der digitalen Technologien abhängigen deutschen Wirtschaft, welches sich auch in anderen Unternehmensbefragungen gezeigt hat (Bitkom 2021, 2019a). Betrachtet man nur den Anteil der Unternehmen, die sich in mindestens einem Technologiefeld stark abhängig fühlen, sind es in der Informationswirtschaft immer noch 56 Prozent und im Verarbeitenden Gewerbe 46 Prozent[7].

[7] Anmerkung: Diese Ergebnisse sind nicht separat in einem Diagramm abgebildet.

Zwischen den Teilbereichen der Wirtschaftszweige zeigen sich leichte Unterschiede in der wahrgenommenen Abhängigkeit. In der Informationswirtschaft ist der Anteil der Unternehmen, die sich abhängig fühlen, in der IKT-Hardwarebranche mit 88 Prozent am höchsten. In der Medienbranche liegt der Anteil jedoch nur bei 75 Prozent. Im Verarbeitenden Gewerbe ist der Anteil der abhängigen Unternehmen im Maschinenbau am höchsten (89 Prozent) und im Fahrzeugbau am geringsten (79 Prozent).

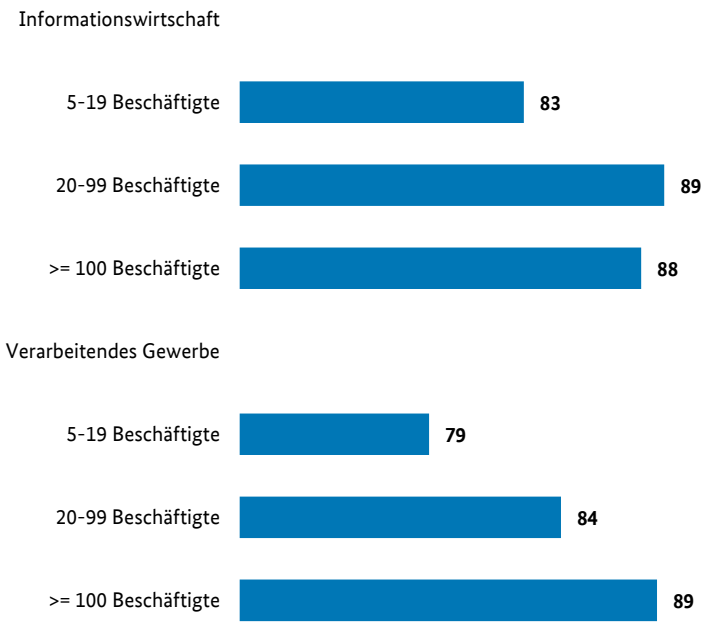
Abbildung 5: Anteil der Unternehmen, die sich in mindestens einem vorgegebenen Technologiefeld sehr oder etwas abhängig von nicht-europäischen Anbietern/Partnern fühlen (in Prozent)



Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Wenn Sie an die in Ihrem Unternehmen eingesetzten digitalen Technologien und Anwendungen denken, fühlen Sie sich in den folgenden Bereichen abhängig von nicht-europäischen Anbietern/Partnern?

Betrachtet man die gefühlte Abhängigkeit nach Unternehmensgröße zeigt sich eine tendenzielle Zunahme der Abhängigkeit von nicht-europäischen Anbietern/Partnern. In der Informationswirtschaft liegt der Anteil der kleinen Unternehmen, die sich in mindestens einem Technologiefeld abhängig fühlen, bei 83 Prozent. Bei den mittleren und großen Unternehmen sind es hingegen 89 und 88 Prozent. Im Verarbeitenden Gewerbe ist diese Tendenz noch eindeutiger zu beobachten. So liegt der Anteil der Unternehmen, die sich in mindestens einem Bereich abhängig fühlen, bei kleinen Unternehmen bei 79 Prozent, bei den mittleren bei 84 Prozent und bei den großen bei 89 Prozent. Diese Tendenz könnte sich zum einen damit erklären lassen, dass größere Unternehmen tendenziell ein breiteres Spektrum an digitalen Technologien nutzen und damit auch vermehrt auf Technologien aus dem nicht-europäischen Ausland zurückgreifen. Zum anderen sind kleine Unternehmen aufgrund ihrer Größe flexibler und agiler, so dass z. B. der Wechsel zu anderen Anbietern und folglich die Migration weniger komplex sind. Geringere Wechselbarrieren könnten wiederum das Gefühl der Abhängigkeit reduzieren.

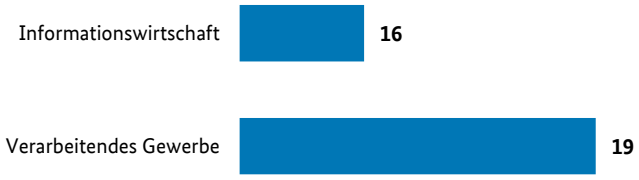
Abbildung 6: Anteil der Unternehmen, die sich in mindestens einem vorgegebenen Technologiefeld sehr oder etwas abhängig von nicht-europäischen Anbietern/Partnern fühlen (nach Unternehmensgröße, in Prozent)



Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Wenn Sie an die in Ihrem Unternehmen eingesetzten digitalen Technologien und Anwendungen denken, fühlen Sie sich in den folgenden Bereichen abhängig von nicht-europäischen Anbietern/Partnern?

Eine Auswertung der wahrgenommenen Abhängigkeiten zeigt zudem, dass sich in beiden Wirtschaftszweigen mindestens ein Sechstel der Unternehmen (16 Prozent in der Informationswirtschaft und 19 Prozent im Verarbeitenden Gewerbe) in allen vorgegebenen Technologiefeldern mindestens etwas abhängig bis stark abhängig von nicht-europäischen Anbietern/Partnern fühlen. Diese Unternehmen empfinden also über eine große Bandbreite an digitalen Technologien Abhängigkeiten von Anbietern/Partnern außerhalb der Europäischen Union.

Abbildung 7: Anteil der Unternehmen, die sich in allen vorgegebenen Technologiefeldern mindestens etwas abhängig von nicht-europäischen Anbietern/Partnern fühlen (in Prozent)

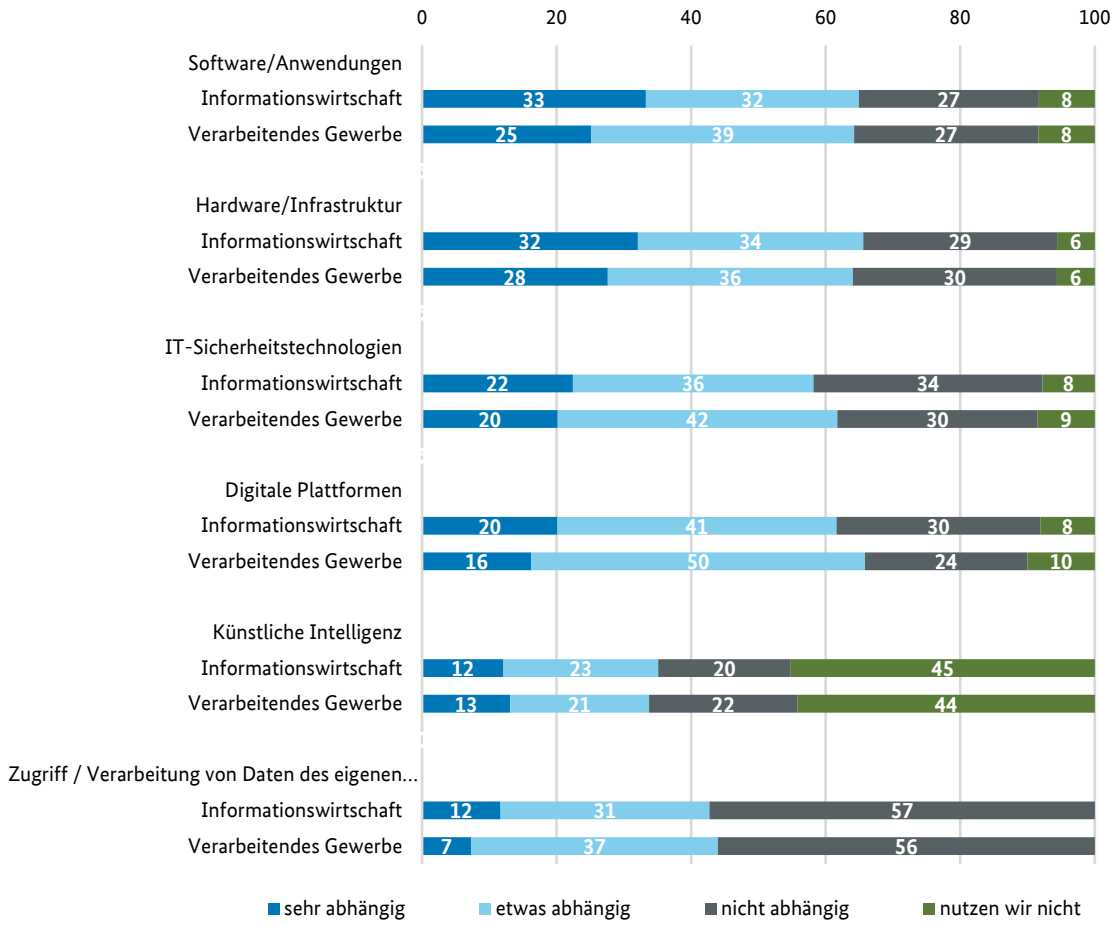


Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Wenn Sie an die in Ihrem Unternehmen eingesetzten digitalen Technologien und Anwendungen denken, fühlen Sie sich in den folgenden Bereichen abhängig von nicht-europäischen Anbietern/Partnern?

Aufgeschlüsselt nach den einzelnen Technologiefeldern zeigen sich leichte Unterschiede in Bezug auf die gefühlte Abhängigkeit der Unternehmen von Nicht-EU-Anbietern/-Partnern. In der Informationswirtschaft

fühlen sich Unternehmen insbesondere sehr abhängig im Technologiefeld Software/Anwendungen (33 Prozent), Hardware/Infrastruktur (32 Prozent) und IT-Sicherheitstechnologien (22 Prozent), gefolgt von digitalen Plattformen (20 Prozent), Künstlicher Intelligenz (12 Prozent) und Daten (12 Prozent). Im Verarbeitenden Gewerbe zeichnet sich ein ähnliches Bild: Im Technologiefeld Hardware/Infrastruktur fühlen sich 28 Prozent der Unternehmen sehr abhängig, im Bereich Software/Anwendungen sind es 25 Prozent und bei IT-Sicherheitstechnologien 20 Prozent. Dahinter folgen digitale Plattformen (16 Prozent), Künstliche Intelligenz (13 Prozent) und Daten (7 Prozent). Dies ist insofern interessant, als dass die Position Deutschlands im Bereich der IT-Sicherheitstechnologien (vgl. Literaturteil) als hoch eingestuft wird, somit vergleichbare Lösungen aus Deutschland existieren sollten.

Abbildung 8: Grad der Abhängigkeit eines Unternehmens von nicht-europäischen Anbietern/Partnern nach Technologiefeld (Anteil der Unternehmen in Prozent)



Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Wenn Sie an die in Ihrem Unternehmen eingesetzten digitalen Technologien und Anwendungen denken, fühlen Sie sich in den folgenden Bereichen abhängig von nicht-europäischen Anbietern/Partnern? Anmerkung: Die Antwortoption „nutzen wir nicht“ kann sich sowohl darauf beziehen, dass eine Technologie nicht im Unternehmen eingesetzt wird oder innerhalb der EU bezogen wird, weshalb keine Abhängigkeit zu Nicht-EU-Anbietern/Partnern besteht.

Insgesamt wird deutlich, dass sich die Unternehmen in den beiden Wirtschaftszweigen in einer großen Bandbreite an digitalen Technologien abhängig von nicht-europäischen Anbietern und Partnern fühlen. Dies

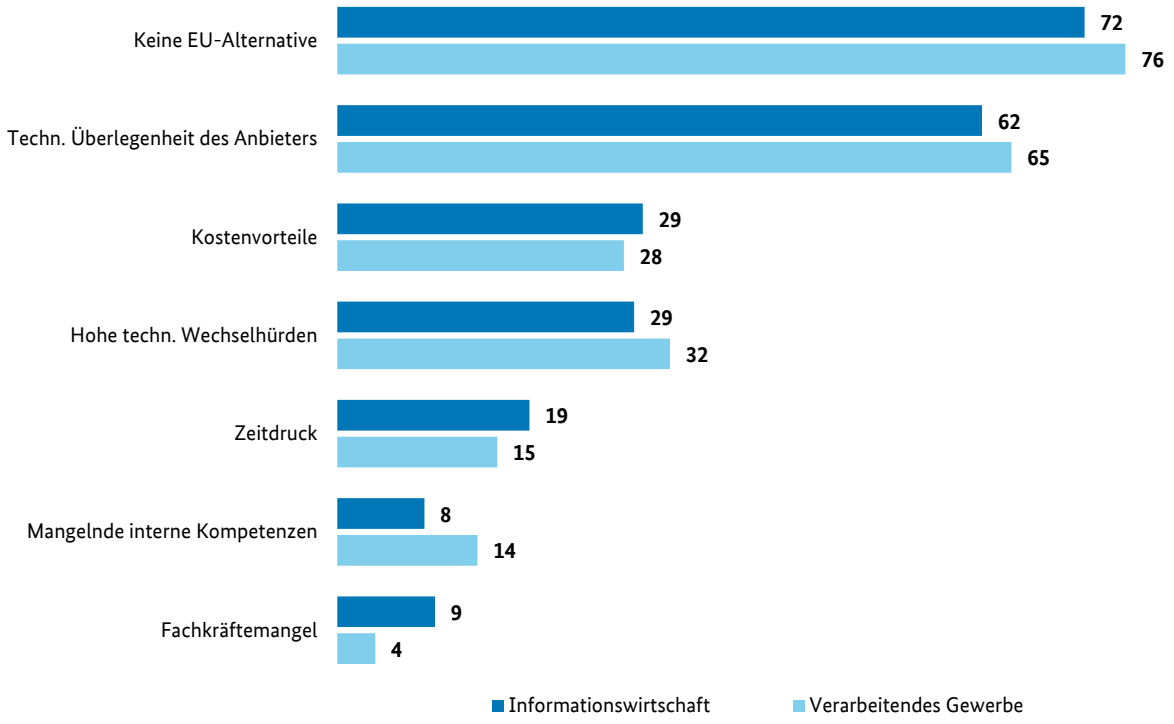
bestätigt das Bild einer technologisch abhängigen deutschen Wirtschaft, welches bereits in der Literaturrecherche herausgearbeitet wurde.

3.2.5 Fehlende EU-Alternativen als Hauptgrund für bestehende Abhängigkeiten

Diejenigen Unternehmen, die den Fragebogen online ausgefüllt haben (n= 752), wurden zudem nach den Gründen für bestehende Abhängigkeiten befragt. Bei den Gründen für bestehende Abhängigkeiten dominieren bei den Unternehmen, die in der vorherigen Frage von mindestens einer Abhängigkeit berichtet haben (vgl. Abbildung 7), in beiden Wirtschaftszweigen zwei Antwortoptionen: Keine EU-Alternative (72 Prozent der Unternehmen bzw. 76 Prozent in der Informationswirtschaft und 76 Prozent der Unternehmen im Verarbeitenden Gewerbe) und die technologische Überlegenheit des Anbieters (62 Prozent bzw. 65 Prozent der Unternehmen in der Informationswirtschaft und 65 Prozent im Verarbeitenden Gewerbe). Demnach existieren entweder keine Alternativen aus der EU oder sie werden als nicht gleichwertig in Bezug auf deren technologische Leistungsfähigkeit eingestuft. Dies bekräftigt noch einmal die Ergebnisse der Literaturrecherche, dass die Anbieterkompetenzen in Deutschland und der EU ausbaufähig sind.

Auch Kostenvorteile sowie technologische Wechselhürden spielen in beiden Wirtschaftszweigen eine Rolle. Etwas weniger als ein Drittel der Unternehmen (29 bzw. 28 Prozent) in beiden Wirtschaftszweigen geben Kostenvorteile als Grund für bestehende Abhängigkeiten an. Hohe technologische Wechselbarrieren werden von 29 Prozent der Unternehmen in der (Informationswirtschaft) bzw. 32 Prozent der Unternehmen im (Verarbeitendes Gewerbe) als Grund benannt. Zudem spielte Zeitdruck bei 19 Prozent (Informationswirtschaft) und 15 Prozent (Verarbeitendes Gewerbe) der Unternehmen eine Rolle. Ein Beispiel wären kurzfristige Digitalisierungsentscheidungen, die aufgrund der Corona-Pandemie und des hohen Anteils an Mitarbeitenden im Homeoffice getätigt wurden. Der Fachkräftemangel am Markt sowie mangelnde interne Kompetenzen spielen eine untergeordnete Rolle für Unternehmen.

Abbildung 9: Gründe für bestehende Abhängigkeit eines Unternehmens von nicht-europäischen Anbietern/Partnern (Anteil der Unternehmen in Prozent; Mehrfachnennung möglich)



Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Aus welchen Gründen bestehen in Ihrem Unternehmen die oben genannten Abhängigkeiten von nicht-europäischen Anbietern/Partnern? (Mehrfachnennungen möglich)
Anmerkung: Diese Frage wurde lediglich im Online-Fragebogen gestellt. Zudem wurden die Antwortoptionen gefiltert für diejenigen Unternehmen hochgerechnet, die bei der vorherigen Frage angaben, in mindestens einem Technologiefeld etwas oder sehr abhängig zu sein.

Insgesamt zeigt sich, dass Unternehmen in beiden Wirtschaftszweigen teilweise starke Abhängigkeiten in unterschiedlichen Technologiefeldern verspüren und insbesondere die mangelnde Auswahl an leistungsfähigen Alternativen aus der EU eine zentrale Rolle dabei spielt.

3.2.6 Maßnahmen zur Reduzierung von technologischen Abhängigkeiten sind „Chefsache“

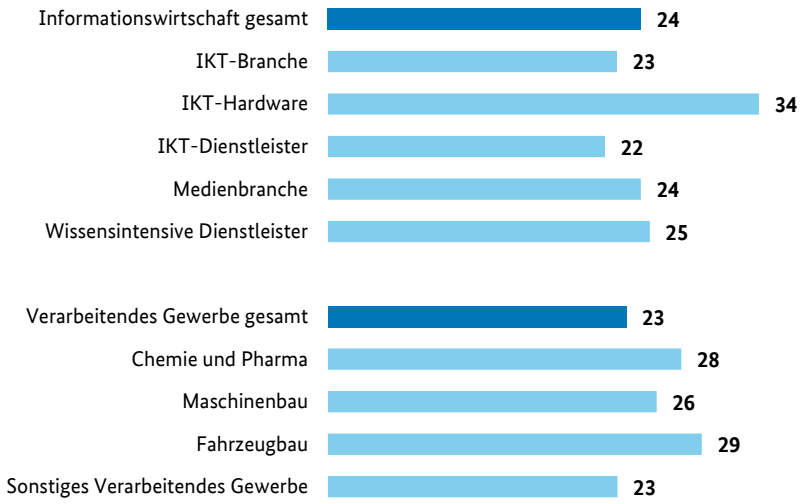
Unternehmen in beiden Wirtschaftszweigen zeigen sich zurückhaltend in Bezug auf Maßnahmen zur Reduzierung von Abhängigkeiten von Nicht-EU-Anbietern/-Partnern. Lediglich rund ein Viertel der Unternehmen (24 Prozent in der Informationswirtschaft und 23 Prozent im Verarbeitenden Gewerbe), die in mindestens einem der vorgegebenen Technologiefelder eine Abhängigkeit empfinden, planen in den kommenden drei Jahren Maßnahmen durchzuführen, um die bestehenden Abhängigkeiten zu reduzieren.

Innerhalb der Wirtschaftszweige zeigen sich leichte Unterschiede in der geplanten Durchführung von Maßnahmen. In der Informationswirtschaft weicht die IKT-Hardwarebranche positiv ab und zeigt mit 34 Prozent den höchsten Anteil an Unternehmen, die konkrete Maßnahmen planen. Die IKT-Dienstleister sind mit 22 Prozent die Teilbranche mit der geringsten Aktivität. Im Verarbeitenden Gewerbe planen insbesondere Unternehmen im Fahrzeugbau (29 Prozent) sowie Chemie und Pharma (28 Prozent) Maßnahmen

durchzuführen, wohingegen das Sonstige Verarbeitende Gewerbe mit einem Anteil von 23 Prozent den niedrigsten Wert aufweist.

Zusammenfassend zeigt sich, dass ein Großteil der Unternehmen zwar Abhängigkeiten wahrnehmen und diese für den langfristigen Erfolg des Unternehmens durchaus als kritisch erachten. Jedoch planen nur wenige dieser Unternehmen konkrete Maßnahmen zur Reduzierung dieser Abhängigkeiten. Dies könnte zum einen am Mangel an leistungsfähigen EU-Alternativen liegen, da dies auch als Hauptgrund für bestehende Abhängigkeiten angegeben wurde. Zum anderen könnte die Unwissenheit über Maßnahmen, die Abhängigkeiten reduzieren (wie etwa die Nutzung von Open-Source-Lösungen oder der Betrieb bzw. die Entwicklung eigener Lösungen), eine Rolle spielen. Auch könnte es sein, dass Unternehmen die Risiken bestehender Abhängigkeiten nicht einschätzen können und demnach auch keinen Handlungsdruck verspüren, diese abzubauen.

Abbildung 10: Anteil der Unternehmen mit bestehenden Abhängigkeiten, die planen, in den kommenden drei Jahren Maßnahmen durchzuführen, um Abhängigkeiten zu reduzieren (in Prozent)



Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Plant Ihr Unternehmen in den kommenden drei Jahren Maßnahmen durchzuführen, um die bestehenden Abhängigkeiten zu reduzieren?
Anmerkung: Diese Frage wurde gefiltert für diejenigen Unternehmen hochgerechnet, die bei der vorherigen Frage angaben, in mindestens einem Technologiefeld etwas oder sehr abhängig zu sein.

Im Online-Fragebogen hatten Unternehmen zudem die Möglichkeit, in einem offenen Antwortfeld die geplanten Maßnahmen inhaltlich zu benennen. Auch wenn es sich lediglich um anekdotische Evidenz von knapp 100 Teilnehmern[8] handelt, geben diese Antworten dennoch einen interessanten Einblick in die Art der geplanten Maßnahmen. Am häufigsten wurde der Wechsel zu Anbietern/Partner aus Deutschland oder der EU genannt (32 Nennungen). Direkt dahinter folgt der Anbieter-/Partnerwechsel ohne konkrete Herkunftsangabe (24). Somit ist der Anbieter-/Partnerwechsel mit insgesamt 56 Nennungen die mit Abstand am häufigsten genannte Maßnahme. Dies ist insofern überraschend, als ein Anbieterwechsel i.d.R. mit einem hohen Aufwand und hohen Kosten verbunden ist. Dies könnte darauf hindeuten, dass Abhängigkeiten vermehrt als kritisch

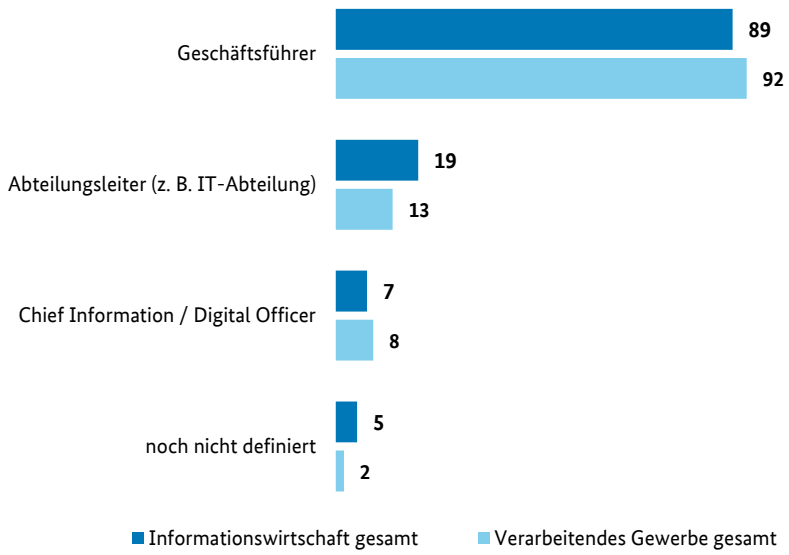
[8] 102 Teilnehmer haben das offene Antwortfeld ausgefüllt. Davon konnten 90 Antwortfelder ausgewertet werden. Ein Feld konnte mehrere Maßnahmen enthalten. Die Kategorien wurden nachträglich gebildet. Acht nicht-kategorisierbare Maßnahmen wurden unter Sonstiges zusammengefasst.

erachtet werden. Weitere beschriebene Maßnahmen sind Personalaufbau/-weiterbildung (13), Entwicklung/Betrieb eigener Lösungen (12), Verbesserung der IT-Sicherheit (7), Multi-Sourcing (6) und der Einsatz von Open-Source-Lösungen (4). Ein Großteil dieser rund 100 Unternehmen hat also umfassende und somit kosten- und zeitintensive Maßnahmen geplant.

Die Unternehmen mit bestehenden Abhängigkeiten, die in den kommenden drei Jahren Maßnahmen planen, wurden zudem zur Umsetzung ebendieser befragt. Dabei ging es zum einen um die Hierarchieebene, auf der die Entscheidungskompetenz liegt, und zum anderen um das Bereitstehen von personellen und finanziellen Ressourcen.

Maßnahmen zur Reduzierung von technologischen Abhängigkeiten sind eindeutig „Chefsache“: Jeweils rund 90 Prozent der Unternehmen in beiden Wirtschaftszweigen geben an, dass die Entscheidungskompetenz auf der Geschäftsführerebene liegt (89 Prozent Informationswirtschaft und 92 Prozent Verarbeitendes Gewerbe). Abteilungsleiter werden in der Informationswirtschaft von 19 Prozent der Unternehmen und im Verarbeitenden Gewerbe von 13 Prozent genannt. Seltener liegen Entscheidungen auf der Ebene von Chief Information / Digital Officer. Lediglich 7 Prozent der Unternehmen in der Informationswirtschaft und 8 Prozent im Verarbeitenden Gewerbe geben diese Hierarchieebene an. In einigen Unternehmen ist die Ebene noch nicht definiert, jedoch ist der Anteil der Unternehmen sehr gering (5 Prozent Informationswirtschaft bzw. 2 Prozent Verarbeitendes Gewerbe).

Abbildung 11: Hierarchieebene, auf der die Entscheidungskompetenz bei Maßnahmen liegt (Anteil der Unternehmen mit bestehenden Abhängigkeiten und geplanten Maßnahmen in Prozent, Mehrfachnennungen möglich)

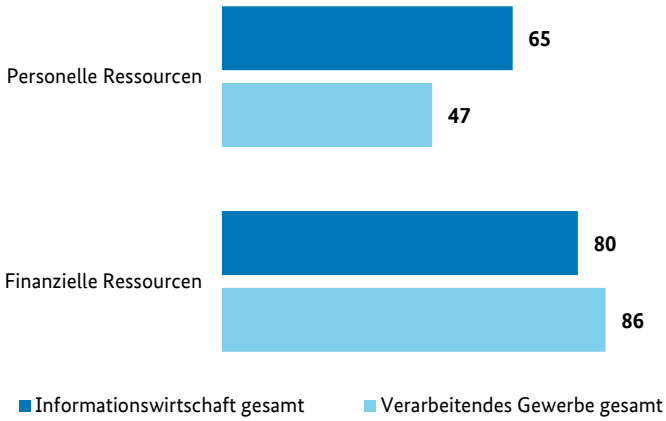


Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Falls Ihr Unternehmen solche Maßnahmen plant, auf welcher Hierarchieebene liegt die Entscheidungskompetenz?
Anmerkung: Diese Frage wurde gefiltert für diejenigen Unternehmen hochgerechnet, die bei den vorherigen Frage angaben, in mindestens einem Technologiefeld etwas oder sehr abhängig zu sein sowie Maßnahmen geplant zu haben.

Denjenigen Unternehmen, die bestehende Abhängigkeiten besitzen und bereits Maßnahmen geplant haben, stehen zur Durchführung ebendieser Maßnahmen nur teilweise die entsprechenden Ressourcen bereit. In

knapp zwei Drittel der Unternehmen (65 Prozent) aus der Informationswirtschaft, aber nur in 47 Prozent der Unternehmen aus dem Verarbeitenden Gewerbe stehen die entsprechenden personellen Ressourcen bereit. Finanzielle Ressourcen stehen hingegen mehrheitlich zur Verfügung (80 Prozent in der Informationswirtschaft und 86 Prozent im Verarbeitenden Gewerbe).

Abbildung 12: Bereitstehen von personellen und finanziellen Ressourcen bei Maßnahmen (Anteil der Unternehmen mit bestehenden Abhängigkeiten und geplanten Maßnahmen in Prozent)



Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Falls Ihr Unternehmen solche Maßnahmen plant, stehen dafür personelle Ressourcen / finanzielle Ressourcen bereit?
Anmerkung: Diese Frage wurde gefiltert für diejenigen Unternehmen hochgerechnet, die bei den vorherigen Frage angaben, in mindestens einem Technologiefeld etwas oder sehr abhängig zu sein sowie Maßnahmen geplant zu haben.

Insgesamt planen zwar nur rund ein Viertel der Unternehmen konkrete Maßnahmen, um bestehende Abhängigkeiten zu reduzieren und somit die eigene digitale Souveränität zu erhalten bzw. zu stärken. Sind diese jedoch geplant, dann liegt die Entscheidungskompetenz auf höchster Führungsebene und finanzielle Ressourcen stehen bereits bereit. Demnach kommt diesen Maßnahmen innerhalb der Unternehmen durchaus eine hohe Bedeutung zu.

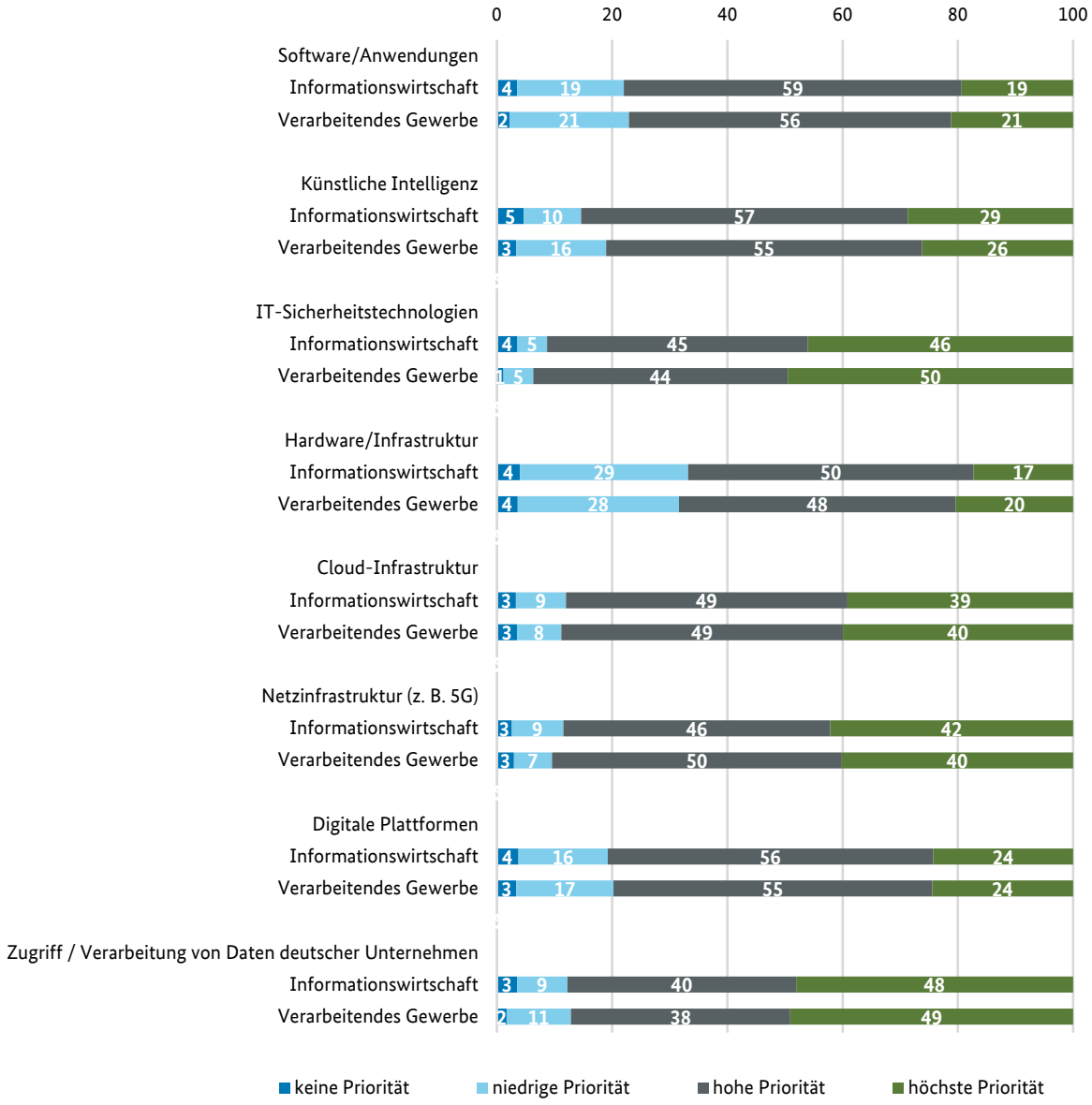
Die Unternehmen wurden zudem um eine Einschätzung gebeten, in welchen Technologiefeldern die Bundesregierung künftig eine Abhängigkeit der deutschen Wirtschaft von nicht-europäischen Anbietern/Partnern vermeiden sollte. Für ein differenzierteres Bild wurde das Technologiefeld Hardware/Infrastruktur dafür noch um Cloud-Infrastruktur und Netzinfrastruktur (z. B. 5G) als separate Antwortoptionen erweitert.

In beiden Wirtschaftszweigen zeigt sich eine sehr ähnliche Einschätzung bezüglich der Priorisierung von Maßnahmen der Bundesregierung. Unternehmen schätzen insbesondere im Bereich IT-Sicherheitstechnologien die Vermeidung von Abhängigkeiten als besonders relevant ein. Rund die Hälfte der Unternehmen in beiden Wirtschaftszweigen (46 Prozent Informationswirtschaft bzw. 50 Prozent im Verarbeitenden Gewerbe) gibt in diesem Bereich die höchste Priorität an. Der Anteil der Unternehmen, die diesem Bereich keine oder eine niedrige Priorität zuordnen ist hingegen sehr gering (4 bzw. 5 Prozent in der Informationswirtschaft und ein bzw. 5 Prozent im Verarbeitenden Gewerbe).

Auch mehr Unabhängigkeit der deutschen Wirtschaft im Bereich Daten wird eine hohe Bedeutung beigemessen. Sowohl in der Informationswirtschaft als auch im Verarbeitenden Gewerbe sehen ebenfalls rund 50 Prozent der Unternehmen die höchste Priorität für die Bundesregierung (48 bzw. 49 Prozent). Dahinter folgen der Bereich Netzinfrastruktur (42 Prozent in der Informationswirtschaft und 40 Prozent im Verarbeitenden Gewerbe) und Cloud-Infrastruktur (39 Prozent in der Informationswirtschaft und 40 Prozent im Verarbeitenden Gewerbe).

Interessanterweise erachten Unternehmen ihre eigenen bestehenden Abhängigkeiten im Bereich Software/Anwendungen und Hardware/Infrastruktur häufig als wenig kritisch, da in diesen Bereichen ein hoher Anteil der Unternehmen (jeweils rund ein Drittel) keine Priorität oder eine niedrige Priorität sieht – obwohl sich Unternehmen in diesen Bereichen besonders abhängig fühlen. Damit liegen diese beiden Technologiefelder im unmittelbaren Vergleich nur am unteren Ende der Prioritätenliste.

Abbildung 13: Priorisierung der Unternehmen, in welchen Technologiefeldern die Bundesregierung künftig Abhängigkeiten der deutschen Wirtschaft von Nicht-EU-Anbietern/Partnern vermeiden sollte (Anteil der Unternehmen in Prozent)



Quelle: ZEW-Konjunkturumfrage Informationswirtschaft, 2. Quartal 2021. Frage: Im Folgenden geht es um Ihre Einschätzung zur deutschen Wirtschaft. In welchen der folgenden Bereiche sollte die Bundesregierung künftig eine Abhängigkeit der deutschen Wirtschaft von nicht-europäischen Anbietern/Partnern vermeiden?

3.3 Fazit zur Unternehmensbefragung

Im Rahmen der Unternehmensbefragung wurden die Bekanntheit des Begriffs der digitalen Souveränität und die Bedeutung des Konzepts für den langfristigen Erfolg untersucht. Zudem waren bestehende Abhängigkeiten zu nicht-europäischen Anbietern/Partnern in zentralen Technologiefeldern Gegenstand der Untersuchung.

Zuletzt wurde die Planung und Umsetzung von Maßnahmen zum Abbau ebendieser Abhängigkeiten, sowohl seitens der Unternehmen als auch der Bundesregierung, durchleuchtet.

Die Befragung zeigt, dass mittlerweile jedes zweite Unternehmen den Begriff Digitale Souveränität kennt (51 Prozent in der Informationswirtschaft und 52 Prozent im Verarbeitenden Gewerbe). Somit ist das Thema zwar in den betrachteten Wirtschaftszweigen angekommen, hat diese aber auch noch nicht vollständig durchdrungen. Dennoch nehmen Unternehmen digitale Souveränität überwiegend als wichtig und erfolgskritisch wahr: Zum einen bewerten Unternehmen einzelne Merkmale einer hohen digitalen Souveränität – Datenhoheit, Interoperabilität/Modularität von IT-Systemen und Standort des Anbieters in Deutschland bzw. der EU – durchweg als sehr wichtig für das eigene Unternehmen (Zustimmungswerte von mindestens 75 Prozent). Besonders wichtig wird dabei in beiden Wirtschaftszweigen der Aspekt der Datenhoheit betrachtet (90 Prozent in der Informationswirtschaft und 84 Prozent im Verarbeitenden Gewerbe). Zum anderen messen die Unternehmen beider Wirtschaftszweige der digitalen Souveränität für den langfristigen Erfolg sowohl des eigenen Unternehmens als auch für die gesamte deutsche Wirtschaft mehrheitlich eine hohe bis sehr hohe Bedeutung bei, auch wenn das Thema heute nur in vier von zehn (Informationswirtschaft) bzw. drei von zehn Unternehmen (Verarbeitendes Gewerbe) eine starke oder sehr starke Berücksichtigung findet. Interessant ist, dass die Bedeutung für den langfristigen Erfolg anderer Unternehmen (also der gesamten deutschen Wirtschaft) tendenziell höher eingeschätzt wird als für das eigene Unternehmen.

Des Weiteren offenbart die Umfrage, dass sich über 80 Prozent der Unternehmen in beiden Wirtschaftszweigen in mindestens einem Technologiefeld abhängig von nicht-europäischen Anbietern und Partnern fühlen (84 Prozent in der Informationswirtschaft und 82 Prozent im Verarbeitenden Gewerbe). Besonders stark wird dies im Bereich Software/Anwendungen und Hardware/Infrastruktur gesehen. Ein Sechstel bzw. ein Fünftel der Unternehmen (16 Prozent in der Informationswirtschaft und 19 Prozent im Verarbeitenden Gewerbe) gibt sogar an, in allen vorgegebenen Technologiefeldern etwas oder stark abhängig von nicht-europäischen Anbietern/Partnern zu sein. Als Gründe für bestehende Abhängigkeiten werden insbesondere die mangelnde Auswahl an leistungsfähigen Alternativen aus der EU sowie die technologische Überlegenheit des Anbieters benannt. Somit existiert durchaus eine Bereitschaft, den Fokus stärker auf europäische Angebote zu legen, wenn diese eine vergleichbare Leistung bieten.

Trotz der wahrgenommenen Abhängigkeiten und der hohen Bedeutung, die der digitalen Souveränität grundsätzlich beigemessen wird, plant aktuell nur rund ein Viertel der Unternehmen, die von bestehenden Abhängigkeiten berichten, in den kommenden drei Jahren konkrete Maßnahmen zur Reduzierung durchzuführen. Wenn diese Maßnahmen allerdings geplant sind, werden sie in den Unternehmen als „Chefsache“ behandelt und haben demnach einen hohen Stellenwert. Zudem geben die Unternehmen mit geplanten Maßnahmen mehrheitlich an, dass die finanziellen Ressourcen für die Umsetzung bereitstehen (80 Prozent Informationswirtschaft bzw. 86 Prozent Verarbeitendes Gewerbe). Gleichwohl mangelt es teilweise noch an personellen Ressourcen, so stehen diese in 35 Prozent (Informationswirtschaft) bzw. 53 Prozent der Unternehmen (Verarbeitendes Gewerbe) derzeit nicht bereit. Dies könnte gegebenenfalls an der Komplexität der Maßnahmen liegen. So deutet anekdotische Evidenz darauf hin, dass Unternehmen insbesondere Anbieter-/Partnerwechsel anstreben, um Abhängigkeiten abzubauen, wofür wiederum Ressourcen und Kompetenzen für die technische und organisationale Umsetzung benötigt werden.

Zuletzt wurde beleuchtet, in welchen Technologiefeldern die Bundesregierung nach der Einschätzung der Unternehmen künftig eine Abhängigkeit von Nicht-EU-Anbietern/Partnern vermeiden sollte. Rund die Hälfte der Unternehmen (46 Prozent Informationswirtschaft bzw. 50 Prozent im Verarbeitenden Gewerbe) sieht insbesondere Bedarf im Bereich IT-Sicherheitstechnologien und gibt dort die höchste Priorität an. Mit nur geringem Abstand folgt in beiden Wirtschaftszweigen der Bereich Daten und weiter die Netzinfrastruktur (z. B. 5G) und Cloud-Infrastruktur.

Im Branchenvergleich zeigen sich über alle Fragen hinweg nur geringe Unterschiede zwischen den Unternehmen, jedoch ergeben sich durchaus unterschiedliche Wahrnehmungen zwischen den Größenklassen: So steigt z. B. die Bekanntheit des Begriffs mit der Unternehmensgröße, gleichwohl auch die wahrgenommene Abhängigkeit von nicht-europäischen Anbietern/Partnern. Letzteres könnte zum einen an höheren Wechselbarrieren und -kosten für große Unternehmen liegen, aber zum anderen auch durch eine stärkere Verbreitung von State-of-the-Art-Technologien aus dem nicht-europäischen Raum bedingt sein. So sind große Unternehmen z. B. weniger zurückhaltend in Bezug auf Cloud-Technologien (vgl. Kapitel 2.2.2.1), bei welchen insbesondere amerikanische und chinesische Anbieter hohe Marktanteile halten.

Insgesamt wird deutlich, dass Unternehmen der digitalen Souveränität eine hohe Bedeutung beimessen, sowohl für das eigene Unternehmen als auch für die deutsche Wirtschaft. Gleichzeitig werden teils erhebliche Abhängigkeiten zu Nicht-EU-Anbietern/-Partnern wahrgenommen. Dennoch plant derzeit nur ein geringer Anteil der Unternehmen Maßnahmen durchzuführen, um diese Abhängigkeiten abzubauen. Handlungsbedarf besteht somit vor allem in der Sensibilisierung für Risiken bei bestehenden Abhängigkeiten, aber auch bei der Entwicklung von Lösungsstrategien zur Reduzierung von Abhängigkeiten und Umsetzung dieser Maßnahmen.

4. Zusammenfassung und Handlungsfelder

Im Rahmen der Schwerpunktstudie wurde das Konzept der digitalen Souveränität aus der Perspektive der Wirtschaft untersucht. Dabei ist unter digitaler Souveränität keineswegs Autarkie und Protektionismus zu verstehen. Vielmehr geht es um die Fähigkeit, die digitale Transformation selbstbestimmt zu gestalten und in Bezug auf digitale Technologien und Anwendungen selbstständig entscheiden zu können, inwieweit man eine Abhängigkeit von Anbietern und Partnern eingeht oder vermeidet. Sowohl die Bestandsaufnahme auf Basis bestehender Studien als auch die repräsentative Unternehmensbefragung geben aufschlussreiche Einsichten zur digitalen Souveränität in Deutschland. Insgesamt zeigt sich ein gemischtes Bild: Der Begriff der digitalen Souveränität ist nur etwa jedem zweiten Unternehmen bekannt. Jedoch messen die Unternehmen dem Thema langfristig eine hohe Bedeutung bei, sowohl für das eigene Unternehmen als auch für die deutsche Wirtschaft insgesamt. Insbesondere der Aspekt der Datenhoheit bzw. Datensouveränität wird von nahezu allen Unternehmen als besonders wichtig für das eigene Unternehmen angesehen. Die deutsche Wirtschaft kann auf einigen Stärken aufbauen, wie etwa Anbieterkompetenzen im Bereich IT-Sicherheit, dennoch zeigt sich an vielen Stellen Entwicklungspotenzial. Im Folgenden werden auf Basis der relevanten Ergebnisse potenzielle Handlungsfelder für die Politik und die Wirtschaft zum Erhalt und zur Stärkung der digitalen Souveränität aufgezeigt.

Abbau von Informationsdefiziten und Sensibilisierung

Zum Abbau von Informationsdefiziten ist es wichtig, die Informationslage zur digitalen Souveränität sowie mögliche Lösungsstrategien (z. B. Open-Source-Software, GAIA-X) zu verbessern. Da insbesondere kleine und mittlere Unternehmen weniger vertraut sind mit dem Konzept der digitalen Souveränität, aber auch mit Maßnahmen wie GAIA-X, könnten hier beispielsweise die Zentren im Netzwerk Mittelstand-Digital involviert werden und Aufklärungs-, aber auch „Übersetzungsarbeit“ leisten.

Auf Unternehmensebene sollten Maßnahmen zur Sensibilisierung der Beschäftigten initiiert werden. Zwar ist ein Verständnis von Abhängigkeitsbeziehungen insbesondere für Entscheidungsträger innerhalb der Unternehmen von Bedeutung. Dennoch sind Themen wie etwa IT-Sicherheit auf allen Beschäftigungsebenen relevant.

Eng verbunden mit der Verbesserung der Informationslage sind auch die Stärkung des Vertrauens und der Akzeptanz, insbesondere in Bezug auf Datensicherheit, seitens der Unternehmen und der Endnutzer essenziell für die Nutzung digitaler Technologien. Im Bereich KI bzw. KI-Anwendungen zählt dazu z. B. die Schaffung von Transparenz und die Nachvollziehbarkeit von Algorithmen, etwa durch konkrete Vorgaben in der öffentlichen Vergabe oder durch eine Verpflichtung zur Überprüfung durch Dritte (Deutscher Bundestag 2019). Auch Gütesiegel wie das für Ende 2021 geplante IT-Sicherheitskennzeichen (BSI 2021) zur Kennzeichnung von IT-Produkten mit bestimmten Sicherheitseigenschaften können helfen, Informationsdefizite bezüglich der Vertrauenswürdigkeit von Produkten abzubauen.

Kontinuierliches Monitoring und Risikoanalyse

Die Entwicklung eines geeigneten Indikatorensets, das digitale Souveränität möglichst umfassend abbildet, ist ein wichtiger Schritt und Grundlage für künftige Maßnahmen. Dieses kann die technologiespezifischen Fähigkeiten, wechselseitige Abhängigkeiten zu anderen Staaten sowie die Bewertung von Risiken umfassen. Auch technologische Foresight-Prozesse, also Methoden der strategischen Vorausschau, können helfen, frühzeitig Technologiefelder und durch neue Technologien und Anbieter bedingte Veränderungen und Entwicklungen in Märkten und der Gesellschaft zu identifizieren.

Auf Unternehmensebene wären eine Bestandsaufnahme und kritische Prüfung der im Unternehmen in unterschiedlichen Wertschöpfungsstufen genutzten Komponenten und digitalen Technologien inklusive der Anbieter und einer Risikobewertung hilfreich. Dazu sollte auch zählen, den Markt stetig nach neuen Anbietern, z. B. aus der EU, zu durchleuchten und gegebenenfalls einen Wechsel vorzunehmen oder das Lieferantennetzwerk zu erweitern, wenn eine Abhängigkeit als kritisch angesehen wird.

Stärkung der Technologie- und Datensouveränität

Um auf bestehenden Stärken aufzubauen, sollte die Entwicklung und Produktion von digitalen Technologien, die sich durch Qualität, Sicherheit und Verlässlichkeit als Markenzeichen deutscher und europäischer Produkte kennzeichnen, vorangetrieben werden. Dabei sollte insbesondere in Zukunftstechnologien wie Quantencomputer, Künstliche Intelligenz und in die IT-Sicherheit investiert werden. Auch wenn es in diesen Bereichen bereits verschiedene Instrumente zur Forschungsförderung sowie zur Gründungs- und Wachstumsförderung gibt, ist es wichtig, hier weitere Impulse zu setzen und den Anschluss im internationalen Wettbewerb nicht zu verlieren. Dies ermöglicht wiederum, den Zugang zu relevanten Technologien und Daten durch wechselseitige Abhängigkeitsbeziehungen („Verhandlungsmasse“) abzusichern.

Der erfolgreichen Umsetzung einhergehend mit einer breiten Marktakzeptanz von GAIA-X kommt eine Schlüsselstellung zu, insbesondere da Unternehmen den Aspekt der Datenhoheit für ihr Unternehmen als sehr wichtig bewerten. Schließlich ist die verstärkte Entwicklung und Förderung von Open-Source-Lösungen eine Möglichkeit, bestehende Abhängigkeiten im Bereich der Software abzubauen und Lock-in-Effekte von Anwendern zu vermeiden. Ein Hebel ist dabei die gezielte Förderung von Open-Source bei öffentlichen Ausschreibungen und der öffentlichen Beschaffung sowie der Digitalisierung der Verwaltung.

Aufbau von digitalen Kompetenzen

Die Verfügbarkeit von und der Zugang zu grundlegenden und fortgeschrittenen digitalen Kompetenzen in einer Gesellschaft sind essenziell für den Erhalt und die Stärkung der digitalen Souveränität. In diversen Studien zeigt sich, dass hier weiter enormer Handlungsbedarf besteht. So zeigt sich z. B. Verbesserungsbedarf in einem niedrigschwelligen Zugang, sowohl zu Weiterbildungsangeboten im Allgemeinen als auch Informationen darüber, welche Kompetenzen auf dem Arbeitsmarkt benötigt werden, also in welchem Bereich eine Weiterbildung sinnvoll ist. Des Weiteren bedarf es kreativer und digitaler Lösungen um den Kompetenzerwerb zu erleichtern. In Bezug auf den Fachkräftemangel ist zum einen die weitere Förderung von MINT-Studiengängen, insbesondere ein Ausbau des Frauenanteils, wichtig. Zum anderen kommen der Verankerung digitaler Fähigkeiten in der beruflichen Ausbildung, aber auch einem niedrigschwelligen Zugang zu Informationen darüber, wie ein Quereinstieg in ein gefragtes Berufsbild erfolgen und auch finanziert werden kann, eine hohe Bedeutung zu.

Unternehmen haben hier ebenfalls eine Verantwortung und sind angehalten, ihre Weiterbildungsaktivitäten weiter auszubauen, etwa im Bereich IT-Sicherheit, aber auch mit neuen Möglichkeiten zu experimentieren, um den Kompetenzerwerb zu verbessern und zu erleichtern. Die Digitalisierung bietet diesbezüglich auch Chancen: Die Einführung von digitalen Kompetenzmanagementtools kann helfen, Mitarbeiterkompetenzen im Unternehmen transparent zu machen und Kompetenzlücken in der Belegschaft („skill gaps“) und entsprechende Fort- und Weiterbildungsmaßnahmen in Kooperation mit den Arbeitnehmervertretern zu identifizieren und die Passgenauigkeit zwischen Kompetenzen und Jobs zu verbessern. Auch die Zusammenarbeit mit Start-ups aus dem Bildungsbereich kann zu Innovationen in der Weiterbildung führen und so die Kompetenzentwicklung weiter vorantreiben.

Agiles und kooperatives Handeln

Digitale Souveränität ist kein statischer Zustand, sondern unterliegt einer fortwährenden Dynamik. Daher ist Agilität auf allen Handlungsebenen von hoher Bedeutung. Auf nationaler sowie europäischer Ebene bedeutet dies u.a., die angestoßenen Projekte wie GAIA-X und die Realisierung eines digitalen Binnenmarktes konsequent voranzutreiben, bürokratische Hürden abzubauen, öffentliche Einrichtungen zu digitalisieren und personell sowie finanziell gut aufzustellen, so dass Entscheidungen evidenzbasiert, schnell und effizient getroffen werden können. Es bedeutet aber auch, getroffene Maßnahmen regelmäßig zu bewerten, zu reflektieren und bei Bedarf zu revidieren. Auch kooperatives Handeln ist im Kontext der digitalen Souveränität wichtig. Digitale Souveränität bleibt eine gesamtgesellschaftliche und auch europäische Aufgabe. Auf staatlicher Ebene bedeutet dies, dass europäische Initiativen, wie etwa GAIA-X oder der Digital Markets Act, wichtige Bestandteile sind, um ein Gegengewicht zu bestehenden Großmächten zu schaffen und die digitale Transformation auf Basis europäischer Rechts- und Wertevorstellungen zu gestalten. Auf Unternehmensebene sollte ebenfalls erwogen werden, ob strategische Kooperationen und die Bündelung von Kompetenzen sowohl innerhalb der Wirtschaft, z.B. mit Start-ups, als auch mit der Wissenschaft intensiver genutzt werden können, um Innovationsfähigkeit und internationale Wettbewerbsfähigkeit zu stärken.

5. Anhang

5.1 Übersichtstabelle: Definitionen von Digitaler Souveränität

Tabelle 1: Definitionen von Digitaler Souveränität

Institution	Autorin und/oder Autor	Jahr	Definition
Acatech	Kagermann, Henning; Streibich, Karl-Heinz; Suder, Katrin	2021	Digitale Souveränität meint die Fähigkeit von Individuen, Unternehmen und Politik, frei zu entscheiden, wie und nach welchen Prioritäten die digitale Transformation gestaltet werden soll.
Bertelsmann Stiftung	Steiner, Falk; Grzymek, Viktoria	2020	Digitale Souveränität ist die Fähigkeit einer Entität, über die zukünftige Ausgestaltung festgestellter Abhängigkeiten in der Digitalisierung selbst entscheiden zu können und über die hierfür notwendigen Befugnisse zu verfügen.
Bitkom	k.A.	2015	Wir verstehen unter Digitaler Souveränität die Fähigkeit zu Selbstbestimmung im digitalen Raum – im Sinne eigenständiger und unabhängiger Handlungsfähigkeit. (...) 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.
Bundesministerium für Bildung und Forschung (BMBF)	k.A.	2021	Unter technologischer Souveränität versteht das BMBF den Anspruch und die Fähigkeit zur kooperativen (Mit-)Gestaltung von Schlüsseltechnologien und technologiebasierten Innovationen. Dies umfasst die Fähigkeiten, Anforderungen an Technologien, Produkte und Dienstleistungen entsprechend der eigenen Werte zu formulieren, Schlüsseltechnologien entsprechend dieser Anforderungen (weiter) zu entwickeln und herzustellen sowie Standards auf den globalen Märkten mitzubestimmen. Technologische Souveränität kann dabei auch erfordern, Schlüsseltechnologien und technologiebasierte Innovationen in Europa eigenständig zu entwickeln und hierfür eigene Produktionskapazitäten aufzubauen, wenn dies zum Erhalt der staatlichen Handlungsfähigkeit oder zur Vermeidung einseitiger Abhängigkeiten notwendig ist.
Bundesministerium für Wirtschaft und Energie (BMWi)	k.A.	2017	Die Fähigkeit zu selbstbestimmten Handeln und Entscheiden im digitalen Raum.
Bundesverband der Deutschen Industrie (BDI)	k.A.	2020	Die vollständige „digitale Souveränität eines Staates [...], einer Organisation [u.a. Unternehmen] sowie jeder Bürgerin und jedes Bürgers umfasst zwingend die vollständige Kontrolle [und Verarbeitungsmöglichkeit] über gespeicherte und verarbeitete

			Daten sowie die unabhängige Entscheidung darüber, wer darauf zugreifen darf. Sie umfasst weiterhin die Fähigkeit, technologische Komponenten und Systeme [bei Bedarf] eigenständig zu entwickeln [, zu produzieren], zu verändern, zu kontrollieren und durch andere Komponenten zu ergänzen.“ (Digital Gipfel, 2018)
CESifo	March, Christoph; Schieferdecker, Ina	2021	Technological sovereignty is the ability of a polity to self-determinedly shape the development and use of technologies and technology-based innovations which impact its political and economic sovereignty.
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)	Gräf, Eike; Lahmann, Henning; Otto, Philipp	2018	**Zitation von vier Definitionen mit Bezug auf die digitale Souveränität von Nationalstaaten, Wirtschaft und Individuen:** [1] Nationalstaaten: „Wir können die digitale Souveränität Europas nur dann erhalten, wenn es uns gelingt, in der Zukunft die technologische Souveränität über die Netzinfrastruktur und die Netztechnik zu erlangen und zu verstärken.“ (Friedrichsen und Bisa 2016) [2] Wirtschaft: „Technologische Souveränität heißt, dass nationale Unternehmen in entscheidenden Bereichen eine Marktposition besitzen, die es ihnen erlaubt, ihre Geschäftsmodelle weiterzuentwickeln und neue Dienstleistungen sicher anzubieten. Dazu gehört, dass bestimmte digitale Schlüsseltechnologien in Deutschland und Europa beherrscht oder zumindest verstanden werden sollten.“ (Bundesdruckerei 2018) sowie [4] „Digital souveräne Systeme verfügen bei digitalen Schlüsseltechnologien und -kompetenzen, entsprechenden Diensten und Plattformen über eigene Fähigkeiten auf internationalem Spitzenniveau. Sie sind darüber hinaus in der Lage, selbstbestimmt und selbstbewusst zwischen Alternativen leistungsfähiger und vertrauenswürdiger Partner zu entscheiden, sie bewusst und verantwortungsvoll einzusetzen und sie im Bedarfsfall weiterzuentwickeln und zu veredeln. Nicht zuletzt sind souveräne Systeme in der Lage, ihr Funktionieren im Innern zu sichern und ihre Integrität nach außen zu schützen.“ (Bitkom 2015) [4] Individuen: „Unter Digitaler Souveränität verstehen wir die Handlungsfähigkeit und Entscheidungsfreiheit der Verbraucher, in der Digitalen Welt in verschiedenen Rollen zu agieren, nämlich als Marktteilnehmer, als Konsumentenbürger einer Gesellschaft sowie als „Prosumer“ in Netzwerken.“ (Sachverständigenrats für Verbraucherfragen 2017)
Digital-Gipfel 2018	Mitglieder der Fokusgruppe: „Digitale Souveränität in einer vernetzten Gesellschaft“	2018	Souveränität bezeichnet die Möglichkeit zur unabhängigen Selbstbestimmung von Staaten, Organisationen oder Individuen. Digitale Souveränität ist heute ein wichtiger Teilaspekt allgemeiner Souveränität, der die Fähigkeit zur unabhängigen Selbstbestimmung in Bezug auf die Nutzung und Gestaltung digitaler Systeme selbst, der darin erzeugten und gespeicherten Daten sowie der damit abgebildeten Prozesse umfasst. (...) Digitale Souveränität eines Staates oder einer Organisation umfasst zwingend die vollständige Kontrolle über gespeicherte und verarbeitete Daten sowie die unabhängige Entscheidung darüber, wer darauf zugreifen darf. Sie umfasst weiterhin die Fähigkeit, technologische Komponenten und Systeme eigenständig zu entwickeln, zu verändern, zu kontrollieren und durch andere Komponenten zu ergänzen.
Digital-Gipfel 2020	Mitglieder der Fokusgruppen „Digitale Souveränität“	2020	Digitale Souveränität wird als Teilaspekt der allgemeinen Souveränität eingeordnet und umfasst die Selbstbestimmtheit im Digitalen. (vgl. Digital-Gipfel, 2018) Grundlagen dafür sind Vertrauenswürdigkeit von Kommunikation, Kontrolle über Datenflüsse und Möglichkeit zu selbstbestimmter Handlung und Innovation.

Fraunhofer-Institut für System- und Innovationsforschung	Edler, Jakob; Blind, Knut; Frietsch, Rainer; Kimpeler, Simone; Kroll, Henning; Lerch, Christian; Reiss, Thomas; Roth, Florian; Schubert, Torben; Schuler, Johanna; Walz, Rainer	2020	Wir definieren Technologiesouveränität als die Fähigkeit eines Staates oder Staatenbundes, die Technologien, die er für sich als kritisch für Wohlfahrt, Wettbewerbsfähigkeit und staatliche Handlungsfähigkeit definiert, selbst vorzuhalten und weiterentwickeln zu können, oder ohne einseitige strukturelle Abhängigkeit von anderen Wirtschaftsräumen beziehen zu können.
Gesellschaft für Informatik	Krupka, Daniel	2020	[...] Digitale Souveränität [ist] unverzichtbare Voraussetzung für unabhängiges staatliches und wirtschaftliches Handeln. Unter digitaler Souveränität wird also das selbstbestimmte Handeln und Entscheiden von (1) Individuen, (2) Unternehmen und anderen Institutionen sowie (3) von ganzen Staaten oder transnationalen Institutionen wie der Europäischen Union im digitalen Raum verstanden.
Institut für Innovation und Technik (iit) Berlin	Wittpahl, Volker (Hg.)	2017	[Digitale Souveränität bezeichnet] die Fähigkeit zu Selbstbestimmung im digitalen Raum – im Sinne eigenständiger und unabhängiger Handlungsfähigkeit. (Bitkom, 2015)
Kompetenzzentrum Öffentliche IT	Goldacker, Gabriel	2017	Digitale Souveränität ist die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.
	Mohabbat Kar, Resa; Thapa, Basanta	2020	Ziel strategischen Handelns zur digitalen Souveränität des Staates ist der »selbstständige, selbstbestimmte & sichere Zugang« zu Digitaltechnologien, damit der Staat öffentliche Leistungen verlässlich erbringen kann. Im Umkehrschluss ist zu vermeiden, dass der Staat durch fehlenden Zugang zu oder unzureichende Kontrolle über Digitaltechnologien in seiner Entscheidungs- und Handlungsfreiheit eingeschränkt wird.
Konrad-Adenauer-Stiftung	Pohle, Julia	2020	Vor dem Hintergrund dieser vielfältigen Entwicklungen lassen sich die aktuellen Forderungen nach digitaler bzw. technologischer Souveränität in Deutschland und Europa als Wunsch nach mehr Handlungs- und Gestaltungsfreiheit verstehen, um es den Akteurinnen und Akteuren zu ermöglichen, den Prozess der digitalen Transformation nach eigenen Wertvorstellungen mitzugestalten und selbstbestimmt im digitalen Raum zu handeln. Wie im traditionellen Souveränitätsverständnis stellt die Fähigkeit zur Selbstbestimmung im Digitalen den Mittelweg zwischen Fremdbestimmung und Autarkie dar und grenzt sich gleichzeitig von beiden ab. Eine solche Idee von digitaler Souveränität lässt sich nicht nur auf den Staat beziehen, sondern auch auf einzelne Bürgerinnen und Bürger oder Unternehmen. Daher beinhaltet der Begriff dieser Souveränität, so wie er in Deutschland und anderen europäischen Ländern zunehmend genutzt wird, auch die Fähigkeit von Individuen sowie von staatlichen oder wirtschaftlichen Institutionen, selbstbestimmt digitale Technologien zu nutzen und ihre jeweiligen Rollen in Zeiten der Digitalisierung selbstständig und sicher auszuüben.
Nationaler IT-Gipfel	Mitglieder Fokusgruppe 1	2015	Souveränität grenzt sich einerseits von Autarkie und andererseits von Fremdbestimmung ab. Digitale Souveränität bezeichnet in diesem Sinne die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum. Gerade in einer digital vernetzten Welt gibt es keine Autarkie. [...] Souverän zu sein bedeutet daher, zu selbstbestimmtem Handeln und Entscheiden fähig zu sein, ohne dabei ausschließlich auf eigene Ressourcen zurückzugreifen. Dazu gehört, dass Wirtschaft, Wissenschaft und Gesellschaft

			(digitale) Produkte, Dienstleistungen, Plattformen und Technologien so nutzen können, dass beispielsweise eigene Sicherheits- oder Datenschutzinteressen nicht beeinträchtigt sind, dass keine unausweichlichen Abhängigkeiten entstehen und dass eigene Geschäftsideen und -modelle verwirklicht werden können. Digitale Souveränität bedeutet darüber hinaus, dass Wirtschaft, Wissenschaft (und in einigen Fällen die öffentliche Verwaltung) in der Lage sind, digitale Technologien zu entwickeln, zur Marktreife auf internationalem Spitzenniveau zu bringen und national wie international zu vertreiben.
Sachverständigenrat für Verbraucherfragen (SVRV)	Mitglieder des SVRV	2017	Unter Digitaler Souveränität verstehen wir demnach die Handlungsfähigkeit und Entscheidungsfreiheit der Verbraucher, in der digitalen Welt in verschiedenen Rollen agieren zu können, nämlich als Marktteilnehmer, als Konsumentenbürger einer Gesellschaft sowie als „Prosumer“ in Netzwerken. Der Begriff verweist darüber hinaus auf die Rechte und Pflichten von Bürgern im staatlichen Ordnungsrahmen und unterstreicht die Rahmenbedingungen, unter denen die Bürger frei, kompetent und verantwortungsvoll digitale Medien und Dienste nutzen können und somit in die Lage versetzt werden, aktiv an einer digitalen Gesellschaft teilzuhaben.
Verband der Elektrotechnik (VDE)	k.A.	2020	Technologische Souveränität ist die Fähigkeit eines Staates oder einer Gesellschaft, politische und gesellschaftliche Prioritäten umsetzen zu können, ohne dabei durch unzureichende oder fehlende Kontrolle über Technologien behindert zu werden.

5.2 Informationen zur Unternehmensbefragung

Die vierteljährliche ZEW-Konjunkturumfrage in der Informationswirtschaft wird vom ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung seit Mitte 2011 durchgeführt. Dazu werden jeweils im letzten Quartalsmonat rund 5.000 Unternehmen mit mindestens fünf Beschäftigten aus der Informationswirtschaft in Deutschland schriftlich kontaktiert. Regelmäßig nehmen etwa 1.000 Unternehmen an der Befragung teil. Jede Umfragewelle behandelt zusätzlich ein aktuelles IKT-Schwerpunktthema; im zweiten Quartal 2021 etwa die Fragen zum Thema Digitale Souveränität.

Die Informationswirtschaft gliedert sich in die folgenden neun Branchen: (1) IKT-Hardware, (2) IKT-Dienstleister, (3) Medien, (4) Rechts- und Steuerberatung, Wirtschaftsprüfung, (5) Public-Relations- und Unternehmensberatung, (6) Architektur- und Ingenieurbüros, technische, physikalische und chemische Untersuchung, (7) Forschung und Entwicklung, (8) Werbung und Markforschung, (9) sonstige freiberufliche, wissenschaftliche und technische Tätigkeiten. Der Bereich IKT-Hardware und IKT-Dienstleister bilden zusammen die IKT-Branche. Die Branchen (4) bis (9) umfassen die wissensintensiven Dienstleister.

Im Rahmen der vorliegenden Studie wurde die ZEW-Konjunkturumfrage Informationswirtschaft um Branchen des Verarbeitenden Gewerbes ergänzt (Abschnitt C nach der Klassifikation der Wirtschaftszweige, Ausgabe 2008). Die Studie untergliedert die untersuchten Branchen des Verarbeitenden Gewerbes nach den Subbranchen Chemie und Pharma, Maschinenbau, Fahrzeugbau sowie Sonstiges Verarbeitendes Gewerbe. Tabelle 2 zeigt eine Übersicht der für die Hochrechnungen verwendeten Branchen und Subbranchen nach der Klassifikation der Wirtschaftszweige, Ausgabe 2008.

Die Umfrage wurde im Juni 2021 durch eine kombinierte schriftliche und internetgestützte Befragung durchgeführt. Die in dieser Studie hochgerechneten Ergebnisse basieren auf insgesamt 1.217 verwertbaren Antworten.

Tabelle 2: Branchenabgrenzung Informationswirtschaft und Verarbeitendes Gewerbe nach der Klassifikation der Wirtschaftszweige (Ausgabe 2008)

Branchen und Subbranchen			WZ 2008
Informationswirtschaft	IKT-Branche	IKT-Hardware	26.1-26.4, 26.8
		IKT-Dienstleister	58.2, 61, 62, 63.1
	Mediendienstleister		58.1, 59, 60, 63.9
	Wissensintensive Dienstleister	Rechts- und Steuerberatung, Wirtschaftsprüfung	69
		Public-Relations- und Unternehmensberatung	70.2
		Architektur- und Ingenieurbüros, technische, physikalische und chemische Untersuchung	71
		Forschung und Entwicklung	72
		Werbung und Marktforschung	73
		Sonstige freiberufliche, wissenschaftliche und technische Tätigkeiten	74
Verarbeitendes Gewerbe	Chemie und Pharma		20, 21
	Maschinenbau		28
	Fahrzeugbau		29, 30
	Sonstiges Verarbeitendes Gewerbe		10-19, 22-25, 26.5-26.7, 27, 31-33

Quelle: Statistisches Bundesamt 2008.

Um die Repräsentativität der Analysen zu gewährleisten, rechnet das ZEW die Antworten der Umfrageteilnehmer auf die Anzahl aller Unternehmen der betrachteten Branchen hoch. Die Hochrechnungen für den Wirtschaftszweig Informationswirtschaft insgesamt und die Teilbereiche IKT-Branche und wissensintensive Dienstleister werden nach Branchen und drei Größenklassen (5-19, 20-99, 100 und mehr Beschäftigte) durchgeführt. Die Mediendienstleister werden nur nach Größenklassen hochgerechnet. Die Hochrechnung für das Verarbeitende Gewerbe erfolgt nach den vier Subbranchen und den oben beschriebenen drei Größenklassen. Die Angaben zu Unternehmens-, Beschäftigungs- und Umsatzzahlen der Grundgesamtheit sind einer Sonderauswertung des Unternehmensregisters des Statistischen Bundesamtes entnommen, die sich momentan auf das Referenzjahr 2018 bezieht.

6. Literatur

Alaveres, Georgios; Duch-Brown, Nestor; Martens, Bertin (2020): Geo-blocking regulation: an assessment of its impact on the EU Digital Single Market (JRC Digital Economy Working Paper, 2020-02). Online verfügbar unter https://ec.europa.eu/jrc/sites/default/files/jrc121480.pdf, zuletzt geprüft am 11.09.2021.

Alffen, Guntram (2019): Cloud-Repatriation – Warum migrieren Unternehmen aus der Public Cloud zurück? NetMediaEurope Deutschland (silicon.de). Online verfügbar unter https://www.silicon.de/experten-tipp/cloud-repatriation-warum-migrieren-unternehmen-aus-der-public-cloud-zurueck, zuletzt geprüft am 31.08.2021.

appliedAI - Initiative for applied artificial intelligence (2021): German AI Startup Landscape 2021. Online verfügbar unter https://www.appliedai.de/de/hub/2021-ai-german-startup-landscape-2, zuletzt geprüft am 03.09.2021.

Bertschek, Irene; Niebel, Thomas; Rammer, Christian; Seifried, Mareike (2020): IKT-Branchenbild. Volkswirtschaftliche Kennzahlen, Innovations- und Gründungsgeschehen. Hg. v. Bundesministerium für Wirtschaft und Energie (BMWi). ZEW - Leibniz-Zentrum für Europäische Wirtschaftsforschung (ZEW). Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/ikt-branchenbild.pdf?__blob=publicationFile&v=14, zuletzt geprüft am 13.09.2021.

Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (2015): Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Berlin. Online verfügbar unter https://www.bitkom.org/sites/default/files/file/import/BITKOM-Position-Digitale-Souveraenitaet.pdf, zuletzt geprüft am 26.08.2021.

Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (2019a): Eckpunkte für eine souveräne Cloud- und Dateninfrastruktur in Deutschland und Europa. Berlin. Online verfügbar unter https://www.bitkom.org/sites/default/files/2019-10/20191022-bitkom_eckpunkte_souverane-cloudinfrastruktur_final.pdf, zuletzt geprüft am 26.08.2021.

Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (2019b): Open Source Monitor 2019. Studie zu Status Quo und Perspektiven in Deutschland. Online verfügbar unter https://www.bitkom.org/opensourcemonitor2019, zuletzt geprüft am 03.09.2021.

Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (2020a): Vertrauen & IT-Sicherheit. Online verfügbar unter https://www.bitkom.org/sites/default/files/2020-02/bitkom_vertrauenitsicherheit2020.pdf, zuletzt geprüft am 03.09.2021.

Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (2020b): Digitale Plattformen. Chartbericht. Berlin. Online verfügbar unter https://www.bitkom.org/sites/default/files/2020-02/bitkom_digitaleplattformen_2020.pdf, zuletzt geprüft am 26.08.2021.

Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (2021): Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr. Online verfügbar unter https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr, zuletzt geprüft am 03.09.2021.

Blind, K.; Böhm, M.; Grzegorzewska, P.; Katz, A.; Muto, S.; Pätsch, S.; Schubert, T. (2021): The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy. Final Study Report. Europäische Kommission. Brüssel. Online verfügbar unter https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and, zuletzt geprüft am 31.08.2021.

BMBF/Kantar Public; Bilger, Frauke; Strauß, Alexandra (2019): Weiterbildungsverhalten in Deutschland 2018 | Ergebnisse des Adult Education Survey – AES-Trendbericht. Hg. v. Bundesministerium für Bildung und Forschung (BMBF). Online verfügbar unter https://www.bmbf.de/upload_filestore/pub/Weiterbildungsverhalten_in_Deutschland_2018.pdf, zuletzt geprüft am 05.03.2021.

BMBF - Bundesministerium für Bildung und Forschung (2019): Nationale Weiterbildungsstrategie. Hg. v. Bundesministerium für Arbeit und Soziales (BMAS) und Bundesministerium für Bildung und Forschung (BMBF). Online verfügbar unter https://www.bmbf.de/files/NWS_Strategiepapier_barrierefrei_DE.pdf, zuletzt geprüft am 05.03.2021.

BMBF - Bundesministerium für Bildung und Forschung (2021): Technologisch souverän die Zukunft gestalten. BMBF Impulspapier zur technologischen Souveränität. Online verfügbar unter https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/pdf/technologisch-souveraen-die-zukunft-gestalten.pdf?__blob=publicationFile&v=2, zuletzt geprüft am 08.09.2021.

BMI - Bundesministerium des Innern, für Bau und Heimat (2016): Cyber-Sicherheitsstrategie für Deutschland (BMI16013). Online verfügbar unter https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf, zuletzt geprüft am 26.08.2021.

BMI - Bundesministerium des Innern, für Bau und Heimat (2021): Eckpunkte für die Cyber-Sicherheitsstrategie 2021. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/03/eckpunkte-cyber-sicherheitsstrategie-2021.pdf?__blob=publicationFile&v=3#:~:text=Hierzu%20z%C3%A4hlen%20insbesondere%20die%20in,globalen%2C%20offenen%20Cyber%2DRaums., zuletzt geprüft am 26.08.2021.

BMWi - Bundesministerium für Wirtschaft und Energie (2015): Leitplanken Digitaler Souveränität. Berlin. Online verfügbar unter https://www.de.digital/DIGITAL/Redaktion/DE/Downloads/it-gipfel-2015-leitplanken-digitaler-souveraenitaet.pdf?__blob=publicationFile&v=1, zuletzt geprüft am 26.08.2021.

BMWi - Bundesministerium für Wirtschaft und Energie (2017): Kompetenzen für eine Digitale Souveränität. Hg. v. FZI Forschungszentrum Informatik (FZI), Accenture und Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom). Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompetenzen-fuer-eine-digitale-souveraenitaet.pdf?__blob=publicationFile&v=14, zuletzt geprüft am 03.09.2021.

BMWi - Bundesministerium für Wirtschaft und Energie (2018): Digitale Souveränität und Künstliche Intelligenz. Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen. Nürnberg. Online verfügbar unter https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=5, zuletzt geprüft am 26.08.2021.

BMWi - Bundesministerium für Wirtschaft und Energie (2019): Digitale Souveränität im Kontext plattformbasierter Ökosysteme. Dortmund. Online verfügbar unter https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digitale-souveraenitaet.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 26.08.2021.

BMWi - Bundesministerium für Wirtschaft und Energie (2020): Digitale Souveränität und Resilienz. Voraussetzungen, Treiber und Maßnahmen für mehr Nachhaltigkeit. Berlin. Online verfügbar unter https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/digitale-souveraenitaet-und-resilienz.pdf?__blob=publicationFile&v=10, zuletzt geprüft am 26.08.2021.

BMWi - Bundesministerium für Wirtschaft und Energie (2021a): Digitaler Binnenmarkt. Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/digitaler-binnenmarkt.html, zuletzt geprüft am 02.09.2021.

BMWi - Bundesministerium für Wirtschaft und Energie (2021b): GAIA-X. Eine vernetzte Datenstruktur für ein europäisches digitales Ökosystem. Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.htm, zuletzt geprüft am 31.08.2021.

BMWi - Bundesministerium für Wirtschaft und Energie (2021c): IPCEI Mikroelektronik: Halbleiterfabrik in Dresden eröffnet. Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/20210604-infopapier-ipcei-mikroelektronik-halbleiterfrabrik-in-dresden-eroeffnet.pdf?__blob=publicationFile&v=4, zuletzt geprüft am 03.09.2021.

BMWi - Bundesministerium für Wirtschaft und Energie (2021d): Künstliche Intelligenz. Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Artikel/Technologie/kuenstliche-intelligenz.html, zuletzt geprüft am 31.08.2021.

Brozus, Lars (2014): Sind Demokratien souveräner als Autokratien?: in: Josef Braml et al. (Hg.): Außenpolitik mit Autokratien, DGAP-Jahrbuch Internationale Politik, Band 30, Verlag DeGruyter Oldenbourg. Online verfügbar unter https://www.swp-berlin.org/publications/products/fachpublikationen/Brozus_2014_Sind_Demokratien_Souveraener_Als_Autokratien_Jahrbuch_IP.pdf, zuletzt geprüft am 03.09.2021.

BSI - Bundesamt für Sicherheit in der Informationstechnik (2020): Die Lage der IT-Sicherheit in Deutschland 2020. Bonn (BSI-LB20/509). Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1, zuletzt geprüft am 26.08.2021.

BSI - Bundesamt für Sicherheit in der Informationstechnik (2021): Das IT-Sicherheitskennzeichen kommt Ende 2021. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/it-sicherheitskennzeichen_node.html;jsessionid=1C2F02C5EB8CECE0450C57F1C3FCFB3B.internet462, zuletzt geprüft am 11.09.2021.

Büchel, Jan; Demary, Vera; Goecke, Henry; Kohlisch, Enno; Koppel, Oliver; Mertens, Armin et al. (2021): KI-Monitor 2021. Status quo der Künstlichen Intelligenz in Deutschland. Hg. v. Bundesverband Digitale Wirtschaft (BVDW) e.V. Institut der deutschen Wirtschaft Köln (IW Köln). Online verfügbar unter https://www.iwkoeln.de/studien/vera-demary-henry-goecke-status-quo-der-kuenstlichen-intelligenz-in-deutschland-1.html, zuletzt geprüft am 04.10.2021.

Büchel, Jan; Mertens, Armin (2021): KI-Bedarfe der Wirtschaft am Standort Deutschland. Eine Analyse von Stellenanzeigen für KI-Berufe. Institut der deutschen Wirtschaft Köln (IW Köln). Online verfügbar unter https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-download-ki-bedarfe-wirtschaft.pdf?__blob=publicationFile&v=4, zuletzt geprüft am 13.09.2021.

Bundesagentur für Arbeit (2020): Fachkräfteengpassanalyse 2019. Online verfügbar unter https://statistik.arbeitsagentur.de/DE/Navigation/Footer/Top-Produkte/Fachkraefteengpassanalyse-Nav.html, zuletzt geprüft am 11.10.2021.

Bundesagentur für Arbeit (2021): Fachkräfteengpassanalyse 2020. Online verfügbar unter https://statistik.arbeitsagentur.de/DE/Navigation/Footer/Top-Produkte/Fachkraefteengpassanalyse-Nav.html, zuletzt geprüft am 11.10.2021.

Bundesdruckerei (2018): IT-Sicherheit im Rahmen der Digitalisierung. Eine empirische Untersuchung in deutschen Unternehmen in Zusammenarebeit mit Bitkom Research. Online verfügbar unter https://www.bundesdruckerei.de/de/studie-it-sicherheit, zuletzt geprüft am 26.08.2021.

Bundesregierung (2021): Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum. Berlin. Online verfügbar unter

https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1, zuletzt geprüft am 31.08.2021.

CB Insights (2021): AI 100: The Artificial Intelligence Startups Redefining Industries. Online verfügbar unter https://www.cbinsights.com/research/report/artificial-intelligence-top-startups/, zuletzt geprüft am 31.08.2021.

Cusumano, Michael A.; Yoffie, David B.; Gawer, Annabelle (2020): The Future of Platforms. MIT Solan. Online verfügbar unter https://sloanreview.mit.edu/article/the-future-of-platforms/, zuletzt geprüft am 31.08.2021.

Demary, Vera; Goecke, Henry (2019): Künstliche Intelligenz: Israel und Finnland vor China. Institut der deutschen Wirtschaft Köln (IW Köln). Köln (IW-Kurzbericht, 8/2019). Online verfügbar unter https://www.iwkoeln.de/fileadmin/user_upload/Studien/Kurzberichte/PDF/2019/IW-Kurzbericht_2019_K%C3%BCnstliche_Intelligenz.pdf, zuletzt geprüft am 31.08.2021.

Deutscher Bundestag (2019): Transparenz-Anforderungen an KI-Systeme. Künstliche Intelligenz - Gesellschaftliche Verantwortung und wirtschaftliche Potenziale/ Ausschuss - 06.05.2019 (hib 509/2019). Online verfügbar unter https://www.bundestag.de/presse/hib/640518-640518, zuletzt geprüft am 11.09.2021.

Deutscher Bundestag (2021): Quantentechnologie – Förderung der Bundesregierung und aktuelle Herausforderungen im Wettbewerb um die Quantenüberlegenheit. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Mario Brandenburg (Südpfalz), Dr. h. c. Thomas Sattelberger, Katja Suding, weiterer Abgeordneter und der Fraktion der FDP. Deutscher Bundestag. Berlin (Drucksache 19/26407). Online verfügbar unter https://dserver.bundestag.de/btd/19/264/1926407.pdf, zuletzt geprüft am 26.08.2021.

Draghi, Mario (2019): Souveränität in einer globalisierten Welt. Europäische Zentralbank (EZB). Bologna. Online verfügbar unter https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190222~fc5501c1b1.de.html, zuletzt geprüft am 31.08.2021.

Dreißigacker, Arne; Skarczinski, Bennet von; Wollinger, Gina Rosa (2020): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019. Kriminologisches Forschungsinstitut Niedersachsen. Online verfügbar unter https://www.pwc.de/de/cyber-security/cyberangriffe-gegen-unternehmen-in-deutschland.pdf, zuletzt geprüft am 26.08.2021.

Duden (2021): Definition von Souveränität. Online verfügbar unter https://www.duden.de/rechtschreibung/Souveraenitaet, zuletzt geprüft am 02.09.2021.

Eckert, Claudia; Magedanz, Thomas; Hauswirth, Manfred; Schell, Martin; Heuberger, Albert; Niemann, Bernhard et al. (2020): 5G – Netze und Sicherheit. Fraunhofer-Gesellschaft. München. Online verfügbar unter https://www.fraunhofer.de/content/dam/zv/de/forschung/artikel/2018/5G-die-zukunft-im-netz/5G-Netze-und-Sicherheit_Fraunhofer-Positionspapier.pdf, zuletzt geprüft am 26.08.2021.

Edler, Jakob; Blind, Knut; Frietsch, Rainer; Kimpeler, Simone; Kroll, Henning; Lerch, Christian et al. (2020): Technologiesouveränität. Von der Forderung zum Konzept. Fraunhofer-Institut für System- und Innovationsforschung (Fraunhofer ISI). Karlsruhe. Online verfügbar unter https://www.isi.fraunhofer.de/content/dam/isi/dokumente/publikationen/technologiesouveraenitaet.pdf, zuletzt geprüft am 26.08.2021.

EFI - Expertenkommission Forschung und Innovation (2020): Gutachten 2020. Gutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands 2020. Online verfügbar unter https://www.e-fi.de/fileadmin/Assets/Gutachten/EFI_Gutachten_2020.pdf, zuletzt geprüft am 16.09.2021.

EFI - Expertenkommission Forschung und Innovation (2021): Gutachten 2021. Jahresgutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands 2021. Online verfügbar unter https://www.e-fi.de/publikationen/gutachten, zuletzt geprüft am 11.10.2021.

Europäische Kommission (2018): Artificial Intelligence for Europe. Brüssel. Online verfügbar unter https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2018)237&lang=en, zuletzt geprüft am 31.08.2021.

Europäische Kommission (2019): Eurobarometer. Attitudes towards the impact of digitalisation on daily lives. Online verfügbar unter https://europa.eu/eurobarometer/surveys/detail/2228, zuletzt geprüft am 11.09.2021.

Europäische Kommission (2020a): Das Gesetz über digitale Märkte: für faire und offene digitale Märkte. Brüssel. Online verfügbar unter https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_de, zuletzt geprüft am 31.08.2021.

Europäische Kommission (2020b): Digital Economy and Society Index (DESI) 2020. Online verfügbar unter https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020, zuletzt geprüft am 11.09.2021.

Eurostat - Statistische Amt der Europäischen Union (2020): Erste Bevölkerungsschätzungen. EU-Bevölkerung im Jahr 2020 bei fast 448 Millionen. Hg. v. Europäische Kommission. Online verfügbar unter https://ec.europa.eu/eurostat/documents/2995521/11081097/3-10072020-AP-DE.pdf/7f863daa-c1ac-758f-e82b-954726c4621f, zuletzt geprüft am 04.10.2021.

Fraunhofer-Allianz Cloud Computing (2021): Was bedeutet Public, Private und Hybrid Cloud? Online verfügbar unter https://www.cloud.fraunhofer.de/de/faq/publicprivatehybrid.html, zuletzt geprüft am 03.09.2021.

Friedrichsen, Mike; Bisa, Peter-J. (2016): Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft. Fachmedien: Springer. Online verfügbar unter https://www.springer.com/de/book/9783658073480, zuletzt geprüft am 11.10.2021.

Gesellschaft für Informatik (2020): Schlüsselaspekte digitaler Souveränität. Berlin. Online verfügbar unter https://gi.de/fileadmin/GI/Allgemein/PDF/Arbeitspapier_Digitale_Souveraenitaet.pdf, zuletzt geprüft am 26.08.2021.

Goldacker, Gabriel (2017): Digitale Souveränität. Kompetenzzentrum Öffentliche IT (ÖFIT). Berlin. Online verfügbar unter https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t, zuletzt geprüft am 26.08.2021.

Gräf, Eike; Lahmann, Henning; Otto, Philipp (2018): Die Stärkung der digitalen Souveränität. Wege der Annäherung an ein Ideal im Wandel. Unter Mitarbeit von Wiebke Glässer, Ulrike Thalheim und Julia Schrader. Hg. v. Deutsches Institut für Vertrauen und Sicherheit im Internet. Online verfügbar unter https://www.divsi.de/wp-content/uploads/2018/05/DIVSI-Themenpapier-Digitale-Souveraenitaet.pdf, zuletzt geprüft am 26.08.2021.

Grzymek, Viktoria; Wintermann, Ole (2020): Wie digital sind die Unternehmen in Deutschland? Ergebnisse einer repräsentativen Befragung unter Erwerbstätigen. Bertelsmann Stiftung. Online verfügbar unter https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Wie_digital_sind_die_Unternehmen_in_DE_BertelsmannStiftung_Blog_ZukunftderArbeit.pdf, zuletzt geprüft am 02.09.2021.

Hintemann, Ralph (2017): Update 2017: Rechenzentren in Deutschland: Eine Studie zur Darstellung der wirtschaftlichen Bedeutung und der Wettbewerbssituation. Borderstep Institut. Berlin. Online verfügbar unter https://www.bitkom.org/sites/default/files/file/import/Kurzstudie-RZ-Markt-Bitkom-final-20-11-2017.pdf, zuletzt geprüft am 26.08.2021.

Hintemann, Ralph (2020): Energiebedarf der Rechenzentren steigt trotz Corona weiter an. Borderstep Institut. Berlin. Online verfügbar unter https://www.borderstep.de/wp-content/uploads/2021/03/Borderstep_Rechenzentren2020_20210301_final.pdf, zuletzt geprüft am 26.08.2021.

Hoffmann, Marina; Schröder, Christian; Pasing, Philipp (2021): Digitale B2B-Plattformen: Status quo und Perspektiven der Industrie in Deutschland. Hg. v. Friedrich-Ebert-Stiftung. Online verfügbar unter https://library.fes.de/pdf-files/wiso/17339.pdf, zuletzt geprüft am 29.07.2021.

Initiative D21 (2021a): D21 Digital Index 2020/21. Jährliches Lagebild zur Digitalen Gesellschaft. Online verfügbar unter https://initiatived21.de/app/uploads/2021/02/d21-digital-index-2020_2021.pdf, zuletzt geprüft am 26.08.2021.

Initiative D21 (2021b): Digital Skills Gap. Sonderstudie des D21-Digital-Index 2020/2021. Initiative D21. Online verfügbar unter https://initiatived21.de/d21skillsgap/, zuletzt geprüft am 04.10.2021.

Institut der deutschen Wirtschaft Köln (IW Köln) (2021): Sonderauswertung aus dem IW-MINT-Report. Unter Mitarbeit von Christina Anger, Enno Kohlisch, Oliver Koppel und Axel Plünnecke.

Jäger, Angela; Lerch, Christian (2020): Digitale Plattformen auf dem Vormarsch? Verbreitung und Umsatzeffekte des Plattformgeschäfts im Verarbeitenden Gewerbe. Fraunhofer-Institut für System- und Innovationsforschung (Fraunhofer ISI). Karlsruhe. Online verfügbar unter https://www.isi.fraunhofer.de/content/dam/isi/dokumente/modernisierung-produktion/erhebung2018/PI_77_B2B_Plattformoekonomie.pdf, zuletzt geprüft am 26.08.2021.

Kagermann, Henning; Streibich, Karl-Heinz; Suder, Katrin (2021): Digitale Souveränität. Status quo und Handlungsfelder. Deutsche Akademie der Technikwissenschaften (acatech). Online verfügbar unter https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/, zuletzt geprüft am 26.08.2021.

Kar, Resa Mohabbat; Thapa, Basanta E. p. (2020): Digitale Souveränität als strategische Autonomie. Kompetenzzentrum Öffentliche IT (ÖFIT). Berlin. Online verfügbar unter http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-6056723.pdf, zuletzt geprüft am 26.08.2021.

Koch, Moritz; Sigmund, Thomas; Herwartz, Christoph (2021): Appell von vier Regierungschefinnen an die EU: „Europa muss seine digitale Souveränität stärken". Handelsblatt. Online verfügbar unter https://www.handelsblatt.com/meinung/gastbeitraege/digitalisierung-appell-von-vier-regierungschefinnen-an-die-eu-europa-muss-seine-digitale-souveraenitaet-staerken/26962398.html?ticket=ST-12931865-eW4DeA7RS6Lbg56x2r4i-ap2, zuletzt geprüft am 26.08.2021.

KPMG (2021): Cloud-Monitor 2021. Die goldenen Zwanziger für die Cloud? Online verfügbar unter https://hub.kpmg.de/cloud-monitor-2021?gclid=CjwKCAjwyvaJBhBpEiwA8d38vAcdL9b9ekFuEZIFW5Jl4VOSvts8No5YPYgHtGYFlFnnPnvuhwb5lBoCv3UQAvD_BwE, zuletzt geprüft am 11.09.2021.

Krasner, Stephen D. (2001): Abiding Sovereignty. In: *International Political Science Review / Revue internationale de science politique* 22 (3), S. 229–251. Online verfügbar unter http://www.jstor.org/stable/1601484.

Kühl, Eike (2021): "Wir könnten in einigen Bereichen noch Erster werden". In: *Spektrum*, 26.07.2021. Online verfügbar unter https://www.spektrum.de/news/quantencomputer-wir-koennen-in-einigen-bereichen-noch-erster-werden/1898095, zuletzt geprüft am 03.09.2021.

Legler, Benno; Hyhorova, Hanna (2019): Der IT-Sicherheitsmarkt in Deutschland. Hg. v. Bundesministerium für Wirtschaft und Energie (BMWi). Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheitsmarkt-in-deutschland-studie-2019.pdf?__blob=publicationFile&v=8, zuletzt geprüft am 03.08.2021.

Marcus, Scott; Petropoulos, Georgios; Yeung, Timothy (2019): Contribution to Growth: The European Digital Single Market Delivering economic benefits for citizens and businesses. European Parliament (IMCO Committee). Online verfügbar unter https://www.bruegel.org/wp-content/uploads/2019/02/IPOL_STU2019631044_EN.pdf, zuletzt geprüft am 03.09.2021.

ntv.de (2021): Daimler rechnet auch 2022 mit Chipmangel. Engpass bremst Autobauer aus. Online verfügbar unter https://www.n-tv.de/wirtschaft/Daimler-rechnet-auch-2022-mit-Chipmangel-article22696152.html, zuletzt geprüft am 31.08.2021.

Ostler, Ulrike (2019): 73 Prozent der Unternehmen holen Apps zurück ins Rechenzentrum. Vogel IT-Medien (datacenter-inside.de). Online verfügbar unter https://www.datacenter-insider.de/73-prozent-der-unternehmen-holen-apps-zurueck-ins-rechenzentrum-a-886379/, zuletzt geprüft am 31.08.2021.

Plattform Lernende Systeme (2020): Künstliche Intelligenz zum Nutzen der Gesellschaft gestalten. München. Online verfügbar unter https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/PLS_Fortschrittsbericht_2020.pdf, zuletzt geprüft am 26.08.2021.

Pohle, Julia (2020): Digitale Souveränität. Ein neues digitalpolitisches Schlüsselkonzept in Deutschland und Europa. Konrad-Adenauer-Stiftung. Berlin. Online verfügbar unter https://www.kas.de/documents/252038/7995358/Digitale+Souver%C3%A4nit%C3%A4t.pdf/c04017b5-11d6-94b5-5e50-ce9f71829b1e?version=1.0&t=1608034330280, zuletzt geprüft am 26.08.2021.

PwC (2019): Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Berlin. Online verfügbar unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile, zuletzt geprüft am 26.08.2021.

Rammer, Christian (2021): Herausforderungen beim Einsatz von Künstlicher Intelligenz. Ergebnisse einer Befragung von jungen und mittelständischen Unternehmen in Deutschland. Unter Mitarbeit von Janna Axenbeck, Patrick Breithaupt, Jan Büchel, Theresa Geyer, Manuel Lauer, Thomas Niebel und Mareike Seifried. Hg. v. Bundesministerium für Wirtschaft und Energie (BMWi). ZEW - Leibniz-Zentrum für Europäische Wirtschaftsforschung (ZEW). Berlin. Online verfügbar unter https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-download-ki-herausforderungen.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 26.08.2021.

Rammer, Christian; Bertschek, Irene; Schuck, Bettina; Demary, Vera; Goecke, Henry (2020): Einsatz von Künstlicher Intelligenz in der Deutschen Wirtschaft. Stand der KI-Nutzung im Jahr 2019. Hg. v. Bundesministerium für Wirtschaft und Energie (BMWi). ZEW - Leibniz-Zentrum für Europäische Wirtschaftsforschung (ZEW). Berlin. Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/einsatz-von-ki-deutsche-wirtschaft.pdf?__blob=publicationFile&v=8, zuletzt geprüft am 31.08.2021.

Rammstedt, Beatrice; Perry, Anja; Maehler, Débora (2015): Zentrale Ergebnisse von PIAAC aus deutscher Perspektive. In: *Zeitschrift für Pädagogik* (61), S. 162–191. Online verfügbar unter https://www.pedocs.de/volltexte/2018/15320/pdf/ZfPaed_2015_2_Rammstedt_Perry_Maehler_Zentrale_Ergebnisse.pdf, zuletzt geprüft am 11.09.2021.

Regenfuß, Tobias; Riemensprenger, Frank; Falk, Svenja (2020): Gaia-X und die Public Cloud. IDG Business Media GmbH (computerwoche.de). Online verfügbar unter https://www.computerwoche.de/a/gaia-x-und-die-public-cloud,3548425,2, zuletzt geprüft am 31.08.2021.

Röhl, Klaus-Heiner; Bolwin, Lennart; Hüttl, Paula (2021): Datenwirtschaft in Deutschland. Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse? Institut der deutschen Wirtschaft Köln (IW Köln). Köln. Online verfügbar unter https://www.iwkoeln.de/fileadmin/user_upload/Studien/Gutachten/PDF/2021/Hemmnisse_der_Datenwirtschaft_Studie_final.pdf, zuletzt geprüft am 03.08.2021.

Roth, Sven L.; Helmann, Thomas (2021): IT ermöglicht Business trotz Kontaktbeschränkungen. Studie IT-Trends 2021. Capgemini. Online verfügbar unter https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2021/02/IT-Trends-Studie-2021.pdf, zuletzt geprüft am 26.08.2021.

Rüdiger, Ariana; Ostler, Ulrike (2021): Kein Ende des Datacenter-Booms in Sicht. Datacenter-Insider. Online verfügbar unter https://www.datacenter-insider.de/kein-ende-des-datacenter-booms-in-sicht-a-1001868/?cmp=nl-86&uuid=FB2DBC7C-120B-4715-B31797404926E695, zuletzt geprüft am 11.09.2021.

Sachverständigenrats für Verbraucherfragen (Hg.) (2017): Digitale Souveränität. Gutachten des Sachverständigenrats für Verbraucherfragen. Berlin. Online verfügbar unter https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/SVRV_Gutachten_DigitaleSouveraenitaet.pdf;jsessionid=E177609C026AAF73792C42F8F34C6648.2_cid289?__blob=publicationFile&v=2, zuletzt geprüft am 26.08.2021.

Savage, Neil (2020): The race to the top among the world's leaders in artificial intelligence. In: *Nature* 588 (7837), S102-S104. Online verfügbar unter https://www.nature.com/articles/d41586-020-03409-8, zuletzt geprüft am 03.09.2021.

Sawall, Achim (2021): O-RAN Alliance schließt erstes chinesisches Unternehmen aus. Golem.de. Online verfügbar unter https://www.golem.de/news/kindroid-o-ran-alliance-schliesst-erstes-chinesisches-unternehmen-aus-2109-159495.html, zuletzt geprüft am 11.09.2021.

Schiefdecker, Ina; March, Christoph (2021): Technological Sovereignty as Ability, Not Autarky. Hg. v. Munich Society for the Promotion of Economic Research (CESinfo). Online verfügbar unter https://www.cesifo.org/DocDL/cesifo1_wp9139.pdf, zuletzt geprüft am 26.08.2021.

Schmoch, Ulrich; Beckert, Bernd; Reiß, Thomas; Neuhäusler, Peter; Rothengatter, Oliver (2020): Identifizierung und Bewertung von Zukunftstechnologien für Deutschland. Fraunhofer-Institut für System- und Innovationsforschung (Fraunhofer ISI). Karlsruhe. Online verfügbar unter http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-6335302.pdf, zuletzt geprüft am 26.08.2021.

Seyda, Susanne (2021): Digitale Lernmedien beflügeln die betriebliche Weiterbildung: Ergebnisse der zehnten IW-Weiterbildungserhebung. Institut der deutschen Wirtschaft Köln (IW Köln). Köln. Online verfügbar unter https://www.iwkoeln.de/fileadmin/user_upload/Studien/IW-Trends/PDF/2021/IW-Trends_2021-01-05_Seyda.pdf, zuletzt geprüft am 02.09.2021.

Seyda, Susanne; Placke, Beate (2020): IW-Weiterbildungserhebung 2020: Weiterbildung auf Wachstumskurs. Institut der deutschen Wirtschaft Köln (IW Köln). Köln (IW-Trends, 47. Jg, Nr. 4). Online verfügbar unter https://www.iwkoeln.de/fileadmin/user_upload/Studien/IW-Trends/PDF/2020/IW-Trends_2020-04-07_Seyda_Placke.pdf, zuletzt geprüft am 26.08.2021.

Statistische Amt der Europäischen Union (Eurostat) (2021): Cloud computing - statistics on the use by enterprises. Online verfügbar unter https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Types_of_cloud_computing:_public_and_private_cloud, zuletzt geprüft am 31.08.2021.

Statistisches Bundesamt (Hg.) (2008): Klassifikation der Wirtschaftszweige. Online verfügbar unter https://www.destatis.de/DE/Methoden/Klassifikationen/Gueter-Wirtschaftsklassifikationen/klassifikation-wz-2008.html, zuletzt geprüft am 02.11.2020.

Steiner, Falk; Grzymek, Viktoria (2020): Digitale Souveränität in der EU. Bertelsmann Stiftung. Berlin. Online verfügbar unter https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/digitale-souveraenitaet-in-der-eu-all, zuletzt geprüft am 26.08.2021.

Strubell, Emma; Ganesh, Ananya; McCallum, Andrew (2019): Energy and Policy Considerations for Deep Learning in NLP. Online verfügbar unter https://arxiv.org/pdf/1906.02243.

Thiel, Thorsten (2019): Souveränität: Dynamisierung und Kontestation in der digitalen Konstellation. In: Jeanette Hofmann, Norbert Kersting, Claudia Ritzi und Wolf J. Schünemann (Hg.): Politik in der digitalen Gesellschaft: transcript Verlag, S. 47–60.

Thomson, Janice E. (1997): Law, Power, and the Sovereign State: The Evolution and Application of the Concept of Sovereignty. By Michael Ross Fowler and Julie Marie Bunck. University Park: Pennsylvania State University, 1995. 200p. In: *American Political Science Review* 91 (3), S. 777–778. DOI: 10.2307/2952151.

Vanson Bourne (2020): Third annual Nutanix enterprise cloud index. Online verfügbar unter https://www.nutanix.com/content/dam/nutanix/resources/gated/analyst-reports/enterprise-cloud-index-2020.pdf, zuletzt geprüft am 31.08.2021.

Verband der Elektrotechnik Elektronik Informationstechnik (VDE) (2020): Technologische Souveränität. Vorschlag einer Methodik und Handlungsempfehlungen. Unter Mitarbeit von Roland Gabriel, Wolfgang Halang, Albert Heuberger, Klaus Illgner, Dorothea Kolossa, Sebastian Möller et al. Frankfurt. Online verfügbar unter https://www.vde.com/resource/blob/2025612/323b195e11506fd4350f9efe89d8211f/vde-studie-technologische-souveraenitaet---download-data.pdf, zuletzt geprüft am 26.08.2021.

Wietholtz, Almuth (2021): Donröschen schlägt die Augen auf. Leibniz-Gemeinschaft. Berlin. Online verfügbar unter https://www.leibniz-magazin.de/alle-artikel/magazindetail/newsdetails/dornroesschen-schlaegt-die-augen-auf, zuletzt geprüft am 31.08.2021.

Wittpahl, Volker (Hg.) (2017): Digitale Souveränität. Bürger | Unternehmen | Staat. Institut für Innovation und Technik (iit). Berlin. Online verfügbar unter https://vdivde-it.de/sites/default/files/document/Digitale-Souveraenitaet-2017.pdf, zuletzt geprüft am 26.08.2021.

Zandonella, Bruno (2005): Pocket Europa. EU-Begriffe und Länderdaten. Souveränität. Bundeszentrale für politische Bildung. Bonn. Online verfügbar unter https://www.bpb.de/nachschlagen/lexika/pocket-europa/16944/souveraenitaet, zuletzt aktualisiert am 2009, zuletzt geprüft am 31.08.2021.