Charta digitale Vernetzung

Risiken für die Digitale Souveränität in Deutschland sowie Handlungsempfehlungen

Positionspapier des Kooperationsbeirats des Vereins Charta Digitale Vernetzung e.V.

I. Risiken für die digitale Souveränität in Deutschland

Digitale Technologien durchdringen zunehmend alle Lebens- und Arbeitsbereiche. Die damit einhergehende Transformation birgt enorme volkswirtschaftliche und gesellschaftliche Potenziale. Digitale Technologien können dabei helfen, die großen gesellschaftlichen Herausforderungen zu adressieren - allen voran der Klimawandel. Ein gelingender digitaler Wandel bringt neue Geschäftsmodelle hervor, die zusätzliche Wertschöpfung und Beschäftigungsmöglichkeiten schaffen.

Gleichzeitig sind die Risiken für eine erfolgreiche sozial-ökologische und digitale Transformation heute so hoch wie nie zuvor: Die SARS-CoV-2-Pandemie hat einerseits gezeigt, welche Potenziale die Digitalisierung beispielsweise im Gesundheitswesen oder in der Bildung birgt, uns aber auch eindrücklich vor Augen geführt, welch weiten Weg wir als Gesellschaft noch zu gehen haben. Mit dem völkerrechtswidrigen Angriff von Russland auf die Ukraine rücken auch Fragen der digitalen Wehrhaftigkeit zunehmend in den Fokus. In ihrer gemeinsamen Erklärung zur „Cyber-Resilienz“ betonen die G7-Staaten, dass der Unterstützung der Widerstandsfähigkeit der Informations-, Kommunikations- und Telekommunikationsinfrastruktur Vorrang eingeräumt werden muss. [1]

Der kürzlich veröffentlichte Digitale-Dependenz-Index der Universität Bonn zeigt: Während Deutschland und die Europäische Union in digitalen Angelegenheiten zunehmend von anderen abhängig ist, konnten die USA, China und Südkorea ihre digitale Autonomie ausbauen. Vor allem beobachten die Autoren eine doppelte Abhängigkeit Europas bei der Informationsinfrastruktur einerseits und beim Handel mit digitalen Technologien andererseits. Dadurch werde das bestehende technopolitische Ordnungsmodell zunehmend infrage gestellt, urteilen die Forscher in ihrer Studie. [2]

Der VDE weist in einem Positionspapier zur technologischen Souveränität darauf hin, dass Deutschland und Europa bezüglich wichtiger Schlüsseltechnologie eigenständig handeln und entscheiden können sowie die letzte Entscheidungsgewalt behalten müssen. Technologische Souveränität wird hier entlang verschiedener Dimensionen der Wertschöpfungskette definiert: Vom Wissen bzw. der Bildung, über die Forschung und Entwicklung, Infrastruktur und Daten, bis hin zur Produktion und dem Betrieb. [3]

II. Risiken für eine erfolgreiche digitale Transformation in Deutschland und Europa

Der Kooperationsbeirat der Charta Digitale Vernetzung e.V. hat vier zentrale Risiken für eine erfolgreiche digitale Transformation und die damit einhergehende digitale Souveränität in Deutschland identifiziert, die noch nicht ausreichend im Fokus der Öffentlichkeit liegen und behandelt werden:

1. **Angreifbarkeit kritischer IT-Systeme / Infrastrukturen:**
   Die Gefährdungslage im Cyber-Raum ist hoch und wird auch dauerhaft hoch bleiben. Cyber-Angriffe - sei es durch private oder staatliche Akteure - führen zu schwerwiegenden IT-Ausfällen in Kommunen, Krankenhäusern und Unternehmen. Sie verursachen zum Teil erhebliche wirtschaftliche Schäden und bedrohen existenzgefährdend Produktionsprozesse, Dienstleistungsangebote und Kunden. Die erfolgreiche Digitalisierung und damit auch Handlungsfähigkeit von Wirtschaft und Gesellschaft ist laut dem aktuellen BSI-Lagebericht aufgrund der fortschreitenden Vernetzung, einer Vielzahl gravierender

[1] https://www.bmvi.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-joint-declaration.html
[2] https://digitaldependence.eu/
[3] https://www.vde.com/resource/blob/2025612/323b195e11506fd4350f9efe89d8211f/vde-studie-technologische-souveraenitaet—download-data.pdf
[4] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Schwachstellen in IT-Produkten sowie der Weiterentwicklung und Professionalisierung von Angriffsmethoden zunehmend gefährdet. [4]

2. **Schleichender Verlust der Datenhoheit:** Der rasante technologische Fortschritt in der digitalen Welt führt aufgrund unzureichender kompetenter Strategiebildung, Steuerung und Gestaltung zu einem schleichenden Verlust der Datenhoheit und einer massiven Gefährdung der Datensouveränität - sowohl jedes Einzelnen, der Unternehmen und Institutionen aber auch von Deutschland und Europa als Gesellschaft und Wirtschaftsstandort. Daten sind die Grundlage für viele neue Geschäftsmodelle beispielsweise basierend auf Technologien der künstlichen Intelligenz. Im Internet sind Plattformen weniger, überwiegend nicht in Europa ansässiger Unternehmen der Informations- und Kommunikationsindustrie (IKT) entstanden, die zahlreiche Märkte und Dienstleistungen bereits nur noch schwer umkehrbar dominieren.
3. **Rohstoffabhängigkeit und Abhängigkeit von Vorprodukten:** In Pharmaprodukten, Fahrzeugen oder Maschinen die in Deutschland produziert werden, stecken Rohstoffe, Vorprodukte und Bauteile wie Microchips aus der ganzen Welt. Wie problematisch die Abhängigkeit von einzelnen Lieferländern sein kann, zeigt sich unter anderem in der Corona-Pandemie und dem Ukraine-Krieg. So sind seltene Erden für die Produktion nahezu aller elektronischer Bauteile und infolgedessen für die Herstellung nahezu aller heutigen Geräte von essenzieller Bedeutung. Diese selten in der Erdkruste vorhandener Metalle weisen zwar Vorkommen in zahlreichen Ländern der Erde auf, stammen jedoch zu großen Teilen aus China. Diese Abhängigkeit kann wiederum zu massiven Auswirkungen auf Risiko 1 und 2 führen, da ungleiche Partnerschaften eingegangen werden müssen, um die Versorgungssicherheit zu gewährleisten.
4. **Fachkräftemangel:** Der Bedarf an Fachkräften z.B. in den mathematisch-naturwissenschaftlichen Bereichen wie der Informatik oder auch Cyber-Sicherheit ist mittlerweile dramatisch. Laut dem MINT-Frühjahrsreport des Instituts der deutschen Wirtschaft lagen im April 2022 in den MINT-Berufen insgesamt rund eine halbe Million offener zu besetzende Stellen vor. [5] Mit der demographischen Veränderung und der Verrentung der geburtenstarken Jahrgänge in den kommenden Jahren, wird sich dieser Trend noch verstärken.

III. Den vier zentralen Risiken zügig und angemessen begegnen

Risiko 1: Um den Gefahren der Angreifbarkeit der kritischen IT-Systeme und -Infrastrukturen in Deutschland und Europa zu begegnen und die Risiken zu minimieren, schlägt der Kooperationsbeirat folgende Maßnahmen vor:

- **Stärkung der IT-Sicherheit in Wirtschaft, Gesellschaft und Verwaltung:** Der Cyber- und Informationssicherheit muss höchste Bedeutung eingeräumt werden. Die passive Cyberabwehr muss gestärkt werden sowie Sicherheitslücken konsequent identifiziert und geschlossen werden. Eine Schwächung von Sicherheit und Vertraulichkeit der digitalen Kommunikation erzeugt enormen Schaden für die Sicherheit aller EU-Bürger*innen, der Unternehmen und der Behörden. Deswegen ist eine anlasslose Massenüberwachung wie z.B. „Chatkontrolle“ auf europäischer und nationaler Ebene abzulehnen.
- **Know-How-Aufbau an zentralen Stellen in Wirtschaft und Gesellschaft:** Nur wer die Gefahren von Datenverlust und -missbrauch in kritischen Lieferketten analysieren und verstehen kann, wird mit angemessenen Mitteln reagieren können. Darum müssen die Kompetenzen für einen unaufgeregte Erkennung von Risiken und den angemessenen Umgang mit Sicherheitsthemen in allen gesellschaftlichen Bereichen durch gezielte Wissensangebote ausgebaut werden.

[5] https://www.iwkoeln.de/studien/christina-anger-enno-kohlisch-oliver-koppel-axel-pluennecke-demografie-dekarbonisierung-und-digitalisierung-erhoehen-mint-bedarf.html

- **Recht auf Verschlüsselung europaweit umsetzen:** Die Vertraulichkeit und Sicherheit digitaler Kommunikation sind essenziell für Gesellschaft und Wirtschaft. Der demokratische Diskurs lebt von einem freien Meinungsaustausch. Unternehmen, Institutionen und Behörden benötigen sichere Kommunikation. Die Informationsfreiheit ist ein hohes Gut und in Artikel 11 der EU-Grundrechtecharta verbrieft. Deshalb ist ein uneingeschränktes Recht auf starke und wirksame Verschlüsselung für alle EU-Bürger*innen, -Unternehmen und -Institutionen notwendig. Darüber hinaus müssen Anbieter von Kommunikationsdiensten dazu verpflichtet werden, EU-Bürger*innen eine sichere IKT-Infrastruktur bereitzustellen.[6]
- **Unabhängigkeit des BSI forcieren:** Das Bundesamt für Sicherheit in der Informationstechnik (BSI) muss weiter gestärkt und mit zusätzlichen Kompetenzen bei der Detektion von Sicherheitslücken und bei der Abwehr von Cyber-Angriffen ausgestattet werden.
  Der Unabhängigkeit der Behörde vom Bundesministerium des Innern bemisst der Kooperationsbeirat dabei hohe Bedeutung bei, um den Begehrlichkeiten der Strafverfolgungsbehörden besser widerstreben zu können.

Risiko 2: Um dem schleichenden Verlust der Datenhoheit in Deutschland und Europa zu begegnen und die Risiken zu minimieren, schlägt der Kooperationsbeirat folgende Maßnahmen vor:

- **Datensouveränität und Datenschutz stärken:** Europa braucht eine leistungsstarke, wettbewerbsfähige und sichere Dateninfrastruktur - die nach europäischen Werten und Regeln funktioniert. Mit Gaia-X sollen neue Maßstäbe bspw. bezüglich des Datenschutzes im internationalen Datenraum gesetzt werden und neue Standards hinsichtlich der Interoperabilität gesetzt werden. Deshalb muss der erfolgreichen Umsetzung von Gaia-X oder vergleichbarer Vorhaben oberste Priorität eingeräumt werden.
- **International Standards setzen:** Neben Gaia-X als regulatorischer Rahmen zur Gestaltung von Datenräumen in der Wirtschaft gilt es darüber hinaus in internationalen Standardisierungs- und Normungsgremien zur Digitalisierung als Wirtschaftsregion Europa Standards zu setzen und dieses Feld nicht asiatischen oder amerikanischen Akteuren zu überlassen. So empfiehlt die Expertenkommission für Forschung und Innovation (EFI) für das Gesundheitswesen, die Etablierung interoperabler und internationaler Standards im Rahmen der Digitalisierungsstrategie für das Gesundheitssystem, um einen effizienten und friktionsfreien Austausch von Daten und Informationen zu ermöglichen und Interoperabilität zwischen IT-Systemen zu gewährleisten. [7]
- **Künstliche Intelligenz „Made in Europe“ fördern:** Bei der Entwicklung von Künstlicher Intelligenz und der Stärkung der Datenwirtschaft muss Europa eine internationale Führungsposition erlangen. Dazu müssen Forschung und Innovation in diesem Bereich deutlich forciert werden. Deutsche Datenverarbeitungsunternehmen und Forschungseinrichtungen sollten - im Rahmen der gesetzlichen Möglichkeiten und Berücksichtigung der Persönlichkeitsrechte jedes einzelnen Menschen - von regulatorischen Hürden für die Sammlung und Auswertung von Daten befreit werden. Sie benötigen technisch wie auch rechtlich sichere Repositorien, Austausch- und Verarbeitungsplattformen für qualitativ hochwertige Datensets.
- **Ausbau der digitalen Infrastruktur:** Deutschland hat beim Breitbandausbau international großen Nachholbedarf, insbesondere in ländlichen Gebieten. Dabei ist längst klar: Schnelles Internet und neue digitale Technologien sind echte Standortvorteile für Unternehmen, Städte und Gemeinden. Glasfaseranschlüsse zum oder direkt ins Haus bilden hierbei die Basis für den flächendeckenden Ausbau. Grundbedingung für die digitale Transformation und die erfolgreiche Etablierung von Datenräumen ist eine leistungsfähige digitale Infrastruktur und die Breitbandanbindung.

[6] https://gi.de/meldung/europaeische-initiative-fordert-recht-auf-verschluesselung
[7] https://www.e-fi.de/fileadmin/Assets/Gutachten/2022/EFI_Kurzfassung_2022.pdf

Risiko 3: Da Deutschland ein rohstoffarmes Land ist, wird es immer auf Importe in diesem Bereich angewiesen sein. Um die aus der Abhängigkeit von Rohstoffen und Vorprodukten erwachsende Abhängigkeit von einzelnen - insbesondere autokratischen Staaten - zu reduzieren, schlägt der Kooperationsbeirat folgende Maßnahmen vor:

- **Risikoanalyse und Monitoring kritischer Abhängigkeiten:** Es bedarf einer größeren steuernden Kontrolle des Staates, wenn einerseits die Abhängigkeiten von Rohstoffen von einzelnen Ländern zu groß werden und Unternehmen in kritischen Sektoren oder anderen gesellschaftlich relevanten Bereichen an Unternehmen in Staaten außerhalb der EU verkauft werden sollen. Deshalb ist eine kontinuierliche und systematische Risikoanalyse sowohl technologischer und digitaler Abhängigkeiten als auch der Abhängigkeiten von Rohstoffen und Vorprodukten von entscheidender Bedeutung. Und letztlich müssen dann Strategien entwickelt werden, um risikoreiche Abhängigkeiten in diesen kritischen Bereichen zu reduzieren bspw. durch die Diversifikation in der Beschaffung von Rohstoffen und Vorprodukten.
- **Technologische Rückstände bei digitalen Schlüsseltechnologien aufholen**: Deutschland zeigt in der Entwicklung von Digitalen Technologien erhebliche Schwächen. Es besteht die Gefahr, den Anschluss in diesen zentralen Schlüsseltechnologien vollends zu verlieren. Deshalb müssen digitale Schlüsseltechnologien auf der Grundlage adäquater Strategien gefördert und geeignete Rahmenbedingungen geschaffen werden. Darüber hinaus sollten geeignete Grundlagen geschaffen werden, damit die zum Teil erheblichen Innovations- und Wertschöpfungspotenziale von Daten stärker als bisher genutzt werden. Zudem erachtet es der Kooperationsbeirat für notwendig, den Ausbau der digitalen Infrastruktur weiter zu forcieren und die Cybersicherheit vor dem Hintergrund einer verschärften Bedrohungslage zu stärken. [7]
- **Open-Source im Hardwarebereich stärken**: Ob in Unterhaltungselektronik, Medizintechnik oder Automobilhardware – Halbleiterchips als wesentliche elektronischer Produkte werden rar. Die Gründe für den seit ca. zwei Jahren andauernden, weltweiten Mangel an Halbleitern sind zahlreich: Nach der erhöhten Nachfrage nach Grafikprozessoren durch Hypes beim Gaming und dem Bitcoin-Mining [8] und den erschwerten Produktionsbedingungen während der Corona-Pandemie, führt auch der andauernde Ukraine-Krieg zu reißenden Lieferketten. Die Europäische Kommission versucht mit dem Chips Act die Produktionsfähigkeit innerhalb der EU zu stärken und sich als Technologieführer zu positionieren. Open-Source-Ansätze können einen Beitrag bei der Linderung des Chipmangels in Europa leisten. Insbesondere kann mit ihrer Hilfe ein niederschwelliger Zugang für Start-Ups, Forschende und Nachwuchskräfte zu Tools und Hardware geschaffen werden.[9]

Risiko 4: Eines der größten Risiken, welches die anderen drei Risiken weiter verstärkt, ist der Fachkräftemangel. Um den Fachkräftemangel adäquat zu adressieren, schlägt der Kooperationsbeirat folgende Maßnahmen vor:

- **Förderung der digitalen Mündigkeit in der Breite**: Bildung in der digitalen vernetzten Welt (kurz: Digitale Bildung) muss aus technologischer, gesellschaftlich-kultureller und anwendungsbezogener Perspektive in den Blick genommen werden. Digitale Kompetenzen müssen in der Breite vermittelt und zum Gegenstand lebenslangen Lernens werden. Hier sind Volkshochschulen, Institutionen der beruflichen Aus- und Weiterbildung und sogenannte dritte Lernorte gefragt. Daneben müssen in der Schule in allen Fächern, fachliche Bezüge zur Digitalen Bildung integrieren werden.
- **Stärkung der digitalen Kompetenzen im MINT-Bereich**: Damit Deutschland und Europa die erforderlichen Innovationen und Produktivitätsgewinne realisieren kann, muss die

[7] https://www.e-fi.de/fileadmin/Assets/Gutachten/2022/EFI_Kurzfassung_2022.pdf
[8] https://www.n-tv.de/shopping-und-service/Bitcoin-Hype-macht-Grafikkarten-zur-Mangelware-article22381889.html
[9] https://gi.de/meldung/webtalk-freie-und-open-source-hardware-online-verfuegbar

Stärkung der Fachkräftebasis forciert werden. Zur Verbesserung der MINT- und insbesondere der informatischen Kompetenzen empfiehlt der Kooperationsbeirat, im schulischen Bereich Lern- und Lehrmethoden auf den Prüfstand zu stellen, drohende Engpässe bei der Lehrkräfteversorgung in den MINT-Fächern aktiver zu bekämpfen und die entsprechenden Schulfächer – insbesondere im Fach Informatik – stärker auszubauen. Es muss ein eigenständiger Lernbereich für die Bezugswissenschaft der Digitalisierung eingerichtet werden, in dem die Aneignung der grundlegenden Konzepte und Kompetenzen für die Orientierung in der digitalen vernetzten Welt ermöglicht wird.[10] Dazu muss in allen Bundesländern verpflichtender Informatik-Unterricht ab der Sekundarstufe I für alle Schultypen eingeführt werden, wie es einige Länder bereits umgesetzt haben. Zudem muss der Unterricht so gestaltet werden, dass er neben der Reflektionsfähigkeit auch Offenheit und Begeisterung für digitale Technologien fördert: Schülerinnen und Schüler müssen von Konsument*innen zu Gestalter*innen der digital vernetzten Welt werden. [11] Um den enormen Bedarf an digital kompetenten Lehrkräften zu decken fordert der Wissenschaftsrat den systematischen Aufbau der Didaktik der Informatik an allen lehrkräftebildenden Universitäten mit Informatik-Fachbereichen sowie mindestens eine Graduiertenschule für Didaktik der Informatik und die Ausweitung der Zahl der möglichen Studienorte für Lehramtsstudierende der Informatik. [12]

- **Stärkung digitaler Kompetenzen in der Aus- und Weiterbildung**: Die zunehmende digitale Vernetzung, Automatisierung und Digitalisierung der Lebens- und Arbeitswelten werden zu starken Umbrüchen auf dem Arbeitsmarkt führen. Viele Tätigkeiten werden künftig von Maschinen übernommen, dafür entstehen ganz neue Beschäftigungen. Sie erfordern neue Kompetenzen und Fähigkeiten, setzen aber gleichwohl bei berufserfahrenen Beschäftigten auf der Grundlage von Ausbildung und Studium wie auch beruflichem Erfahrungswissen an. Die Weiterbildung bietet neue Chancen für berufliche Quereinstiege und eine Ergänzung vielfältiger Grundlagen. Die Weiterbildung generell und die Entwicklung digitaler Kompetenzen im Speziellen müssen in den Fokus einer die Zukunft gestaltenden Politik rücken. Die Politik muss insbesondere diejenigen in der Gesellschaft berücksichtigen, denen bisher keine zu ihrem Lebensumfeld passenden (digitalen) Weiterbildungsangebote gemacht wurden.[13]

IV. Fazit

Die Risiken für die digitale Souveränität in Deutschland sind größer denn je: Die Angreifbarkeit der kritischen IT-Systeme und -Infrastrukturen, der schleichende Verlust der Datenhoheit unserer Wirtschaft, die Abhängigkeit von Rohstoffen und Vorprodukten und der Fachkräftemangel bedrohen unseren Wohlstand und unsere Sicherheit. Deshalb ist es von großer Bedeutung, dass diese vorhandenen Risiken nun konsequent und ernsthaft behandelt werden – und zwar mit einem großen „Wumms“, um in der Sprache der Bundesregierung zu bleiben. Denn nur so wird sich die digitale Transformation in Deutschland bedarfsgerecht und damit erfolgreich gestalten lassen.

[10] https://dagstuhl.gi.de/dagstuhl-erklaerung
[11] https://informatik-monitor.de/
[12] https://www.wissenschaftsrat.de/download/2020/8675-20.pdf?__blob=publicationFile&v=9
[13] https://gi.de/fileadmin/GI/Allgemein/PDF/GI-Wahlpruefsteine_Weiterbildung_Digitale_Kompetenzen_2021-09-15.pdf

Über den Kooperationsbeirat der Charta Digitale Vernetzung e.V.

Die Charta digitale Vernetzung ist ein Kodex für die verantwortungsvolle Gestaltung der digitalen Gesellschaft. Zehn Grundsätze bilden das normative Fundament der Initiative, deren Engagement für ein gemeinsames Wertegerüst und ein nachhaltiges Verantwortungsbewusstsein in der digitalen Transformation heute mehr denn je von Bedeutung ist. Der Kooperationsbeirat hat die Aufgabe, die individuellen Maßnahmen der Mitglieder mit Vereins-/Verbandscharakter mit der Maßgabe abzustimmen, dass an den Grundsätzen der Charta ausgerichtetes gemeinsames Verständnis für den Weg in die digitale Gesellschaft bei Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft entsteht und in gemeinsamen und individuellen Maßnahmen entsprechend umgesetzt wird.

Dieses Positionspapier ist unter Mitwirkung des Bundesverbands Smart City e.V., der Gesellschaft für Informatik e.V. (GI), der ITS Germany und dem Verband Elektrotechnik Elektronik Informationstechnik e.V. (VDE) entstanden. Der Kooperationsbeirat wird geleitet von Kirsten Messer-Schmidt (Gesellschaft für Informatik e.V.).

Charta digitale Vernetzung

Impressum

Risiken für die Digitale Souveränität in Deutschland sowie Handlungsempfehlungen
– Positionspapier des Kooperationsbeirats des Vereins Charta Digitale Vernetzung e.V.

August 2022

Herausgeber:
Charta digitale Vernetzung e. V.
Torstraße 164
10115 Berlin