St. Pölten University of Applied Sciences

/informatik & security

/fh/// st.pölten

Digitale Souveränität

Herausforderungen, Probleme und die Zukunft in der öffentlichen Verwaltung

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur

eingereicht von

Kevin SCHMIDT

is191842

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer/in: FH-Prof. Mag. Dr. Simon Tjoa

Mitwirkung: -

St. Pölten, 12. September 2023

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

Fachhochschule St. Pölten GmbH, Campus-Platz 1, A-3100 St. Pölten,T: +43 (2742) 313 228, F: +43 (2742) 313 228-339, E: office@fhstp.ac.at, I: www.fhstp.ac.at

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Arbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich das Thema dieser Arbeit bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, diese Arbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z. B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, Datum *Unterschrift*

Kurzfassung

Der Prozess der Digitalisierung beschäftigt unsere Gesellschaft seit einiger Zeit. Allerdings bringt die Digitalisierung auch neue Fragestellungen hervor. Eine dieser Fragestellungen ist zum Beispiel die Frage der digitalen Souveränität. Digitale Souveränität, also die digitale Unabhängigkeit und Selbstbestimmtheit, beginnt in der heutigen geopolitischen Lage mehr und mehr an Bedeutung zu gewinnen. Es ist dabei irrelevant, ob sich die Abhängigkeiten auf Software, Halbleiter oder Technologien beziehen. In Politik und Wirtschaft wurde dieses Problem schon erkannt aber ein Konzept der digitalen Souveränität oder wie weit diese gehen muss existiert derzeit keines. Aus der EU und einigen Mitgliedstaaten kommen immer häufiger Initiativen die diese Problemstellung thematisieren und die Abhängigkeiten langsam abbauen wollen. Dies geschieht in Form von Gesetzesinitiativen wie beispielsweise die NIS-Richtlinien oder dem Chips Act oder aber durch konkrete Projekte wie des europäischen Cloudverbunds „GAIA-X“. Aber reichen solch einzelne Initiativen aus, um digital souverän zu werden? Die Antwort ist teilweise. Den Grad, der notwendigen digitalen Souveränität muss jeder Staat, jeder Wirtschaftstreibende oder jeder Mensch selbst bestimmen und in den eigenen relevanten Kontext setzen. Die Ukraine zum Beispiel hat ihre digitale Souveränität in der Zeit kurz vor dem russischen Angriff 2022 damit gesichert, indem sie die digitalen Prozesse der öffentlichen Verwaltung in die Cloud migrierte. Mitgliedstaaten der EU versuchen allerdings sich so gut es geht aus der Public Cloud aus dem EU-Ausland, zumindest für wirklich kritische Prozesse, herauszuhalten. Mit Handlungsempfehlungen wie beispielsweise einem Bekenntnis zu Open Source oder Investitionen in Forschung und Entwicklung ist es allerdings möglich, die eigene Abhängigkeit langfristig zu reduzieren. Digitale Souveränität ist also kein Konzept, welches man anwendet, sondern ein Prozess den jeder einzelne Staat, jeder Wirtschaftstreibende und jeder Mensch zu durchlaufen hat.

Abstract

The process of digitization has occupied our society for some time. However, digitization also brings up new questions. One of these questions, for example, is the issue of digital sovereignty. Digital sovereignty, i.e. digital independence and self-determination, is becoming increasingly important in today's geopolitical situation. It is not relevant whether the dependencies relate to software, semiconductors or technologies. This problem has already been recognized in politics and business, but there is currently no concept of digital sovereignty or how far this must go. Initiatives are increasingly coming from the EU and some member states to address this problem and slowly reduce the dependencies. This takes place in the form of legislative initiatives such as the NIS Directives or the Chips Act, or through concrete projects such as the European cloud network „GAIA-X". But are such individual initiatives enough to become digitally sovereign? The answer is partial. The degree of digital sovereignty required must be determined by each state, each business or each individual and placed in their own relevant context. Ukraine, for example, secured its digital sovereignty in the period shortly before the Russian attack in 2022 by migrating the digital processes of the public administration to the cloud. However, member states of the EU are trying to stay out of the public cloud from outside the EU as much as possible, at least for really critical processes. However, with recommendations for action such as a commitment to open source or investments in research and development, it is possible to reduce one's own dependence in the long term. Digital sovereignty is therefore not a concept which can be applied, but a process which every individual state, every business and every person has to go through.

Inhaltsverzeichnis

1 Einleitung

Die Digitalisierung hat in den letzten Jahrzehnten exponentiell zugenommen und verändert unser tägliches Leben in vielerlei Hinsicht. Mit dieser rasanten Entwicklung sind jedoch auch neue Herausforderungen und Fragen aufgekommen – insbesondere in Bezug auf Abhängigkeiten. Abhängigkeiten von anderen Nationen und Kontinenten gab es schon immer. So ist Österreich zum Beispiel (noch) von russischer Energie abhängig, oder von Halbleiterprodukten aus Asien oder aber auch von Soft- und Hardwareprodukten und digitalen Diensten aus den USA, Asien oder Israel. All das sind nur einzelne Beispiele, allerdings hat Österreich und die Bevölkerung die Energieabhängigkeit im Winter 2022/2023 teuer zu spüren bekommen. Bis zu diesem Zeitpunkt haben sich nur wenige Menschen aus Bevölkerung und Politik mit dem Thema „Abhängigkeiten“ beschäftigt, was sich als Fehler erwiesen hat. Um kritische Abhängigkeiten beispielsweise mittels eines risikobasierten Ansatzes bewerten zu können, um gegebenenfalls Maßnahmen zu ergreifen, muss man sich diesen Abhängigkeiten erst bewusst sein, vor allem als souveräner Staat. Eine Abhängigkeit, in der sich Österreich und Europa im Allgemeinen befindet, und welche erst seit wenigen Jahren diskutiert und beleuchtet wird, ist die digitale. Durch die Digitalisierung von immer mehr Prozessen und Vorgängen begeben sich Länder, Regierungen, die öffentliche Verwaltung, Wirtschaftstreibende oder die Bevölkerung in das Abhängigkeitsverhältnis, dass die digitale Verarbeitung von Prozessen und Daten verfügbar, integer und vertrauenswürdig sein muss. Also die drei CIA-Grundpfeiler der Informationssicherheit:

- **C**onfidentiality (Vertraulichkeit)
- **I**ntegrity (Integrität)
- **A**vailability (Verfügbarkeit)

Aber wie passt der bisher häufig genannte Begriff der „Abhängigkeit“ zum Diplomarbeitstitel „digitaler Souveränität“? Abhängigkeit bezieht sich auf den Zustand, in der eine Person oder ein Land von externen digitalen Technologien, Diensten oder Infrastrukturen ist, die von anderen Ländern oder Unternehmen bereitgestellt werden. Digitale Souveränität bezieht sich allerdings auf die Fähigkeit eines Landes oder einer Organisation, seine digitalen Angelegenheiten autonom zu steuern und zu kontrollieren. Dies bedeutet, dass sie in der Lage sind, ihre digitale Infrastruktur, Daten und Technologien unabhängig zu verwalten, ohne

von externen Quellen abhängig zu sein. Abhängigkeit und digitale Souveränität sind jedoch oft miteinander verknüpft. Wenn beispielsweise ein Land seine gesamte digitale Infrastruktur von ausländischen Unternehmen bereitstellen lässt, kann dies seine Fähigkeit zur Kontrolle und Sicherung seiner digitalen Ressourcen einschränken.

Die Motivation, das Thema der digitalen Souveränität zu meinem Diplomarbeitsthema zu machen, ergibt sich hauptsächlich aus meiner beruflichen Tätigkeit im Bereich der Informationssicherheit im Umfeld der österreichischen öffentlichen Verwaltung. Nach vierjähriger Tätigkeit in IT-sicherheitsrelevanten Themengebieten führt es weiterhin und häufig sogar im qualifizierten Kolleg:innenkreis zu umfangreichen Diskussionen, wie weit digitale Souveränität gehen darf und muss bzw. ob diese im öffentlichen Sektor ein erstrebenswerter Zustand sein sollte. Vor allem die nur noch selten aber dennoch vertretene Meinung, digitale Souveränität einzelner Staaten sei weder realistisch noch erstrebenswert motiviert mich zur genauen Darstellung dieses Themengebietes in der vorliegenden Arbeit.
Hinzu kommt mein persönliches Streben, technische Systeme vollumfänglich verstehen zu wollen und diese ohne externe Abhängigkeiten unabhängig und selbstständig betreiben zu können. Dies setze ich aktuell bereits um mit eigenen Services die im familiären und freundschaftlichen Umfeld bereitgestellt werden, um auch hier größtmögliche Souveränität und Datensicherheit zu gewährleisten.

Aus diesem Grund beschäftigt sich diese Diplomarbeit und damit auch die zu behandelnde Forschungsfrage mit der Thematik der digitalen Souveränität:

- Wie ist die Begrifflichkeiten zu definieren?
- Welche Ursachen und Formen der Abhängigkeit bestehen?
- Welche Anforderungen an digitale Souveränität existieren?
- Welche Ansätze und Initiativen wurden hierzu bisher in Österreich oder Europa zur Steigerung der digitalen Souveränität umgesetzt?

Des Weiteren geht diese Ausarbeitung auf den Begriff der Resilienz ein, und welcher Zusammenhang zwischen diesem und der digitalen Souveränität bestehen. Ebenfalls wird auf das Thema Artificial Intelligence (AI) eingegangen, da diese relativ neue digitale Technologie höchstwahrscheinlich zukunftsweisend ist und auch sie im Kontext der digitalen Souveränität zu bewerten ist. Abschließend endet diese Diplomarbeit mit Handlungsempfehlungen an Politik und Wirtschaft sowie einem Fazit und Ausblick im Sinne der digitalen Souveränität.

2 Begriffsdefinitionen

Das folgende Kapitel definiert die Hauptbegriffe dieser Arbeit und beschreibt die Verbindung zueinander.

2.1 Digital

Der Begriff „digital“ stammt aus dem lateinischen und bedeutet „Finger“. Er bezieht sich dabei auf die Verwendung einer Technologie, die Daten in einer binären Form zu verarbeiten und zu speichern. Das Cambridge Dictionary definiert das Adverb folgendermaßen:

> »*recording or storing information as a series of the numbers 1 and 0, to show that a signal is present or absent*« [1]

Diese binäre Sprache ist die Grundlage des Computers und anderer elektronischer Geräte, die digitale Signale verarbeiten. Der Begriff „digital“ ist außerdem das Gegenteil von „analog“.
In den letzten Jahrzehnten wurden vermehrt die Begriffe „Digitalisierung“ und „digitale Transformation“ verwendet, welche den Prozess einer Überführung einer analogen Welt in eine digitale Welt beschreiben. Häufig reicht es aus, ein Formular beziehungsweise einen papierbasierten Prozess im Allgemeinen durch ein IT-System oder eine technische Verarbeitung zu ersetzen, um einen Prozess zu digitalisieren. Digitalisiert sind Prozesse allerdings erst, wenn sie sich medienbruchfrei vom Anfang bis Ende digital abbilden lassen. [2] Somit ist umgangssprachlich „digital“, was in irgendeiner Weise in Verbindung mit einem Computer steht beziehungsweise sich in digitalen Geräten im Allgemeinen abbilden lässt.

2.2 Souverän

Der Begriff „souverän“ hat seinen Ursprung in der politischen Philosophie und bezieht sich auf die höchste Autorität innerhalb eines Staates oder einer Regierung. [3] Der Duden beschreibt den Begriff – bezogen auf Staaten oder Regierungen – folgendermaßen:

> »*(...) die staatlichen Hoheitsrechte ausübend; Souveränität besitzend*« [4]

Der Begriff kommt von dem lateinischen Wort „superanus“ was übersetzt „höchste“ oder „oberste“ bedeutet. Generell versteht man unter „Souveränität“ die Fähigkeit eines Staates, seine Angelegenheiten selbständig und unabhängig von außen zu regeln und seine territoriale Integrität und Unabhängigkeit zu schützen. Ein Staat gilt als souverän, wenn dieser eigenständig und unabhängig ist und nicht fremdbestimmt wird. [5]
Somit kann man „souverän“ als unabhängig von allen beziehungsweise Dritten deuten.

2.3 Resilienz

Der Begriff „resilient“ beziehungsweise „Resilienz“ hat seinen Ursprung im lateinischen „resilire“, was „zurückspringen“ oder „abprallen“ bedeutet. Der Duden definiert den Begriff folgendermaßen:

> »*psychische Widerstandskraft; Fähigkeit, schwierige Lebenssituationen ohne anhaltende Beeinträchtigung zu überstehen*« [6]

Im Kontext der Informatik beschreibt der Begriff jedoch die Fähigkeit technischer Systeme, „standzuhalten“ oder genauer: trotz massiver interner oder externer Störungen nicht vollständig auszufallen.
Es wird dabei davon ausgegangen, dass es neben dem „Normalzustand“ auch „Ausnahmefälle“ gibt, in denen ein technisches System gestört wird, es aber entweder weiterhin funktionieren oder schnell in den Normalzustand zurückkehren soll. [7]

2.4 Digitale Souveränität

Der Begriff der „digitalen Souveränität“ ist aktuell nicht einheitlich definiert. Er beschreibt das derzeitige Bestreben, sich von Abhängigkeiten in der digitalen Welt zu lösen beziehungsweise diese zu reduzieren. Hauptsächlich wird der Begriff von der öffentlichen Verwaltung oder in der Wirtschaft verwendet. Der Terminus unterscheidet dabei nicht um welche Form der Abhängigkeit es sich handelt (zum Beispiel: Hardware, Software oder digitale Dienste). Die „Schwerpunktstudie Digitale Souveränität“ [8] des deutschen Bundesministeriums für Wirtschaft und Energie aus dem Jahr 2021 hat im Anhang eine Tabelle mit 18 verschiedenen Definitionen des Begriffs „Digitale Souveränität“ gelistet, welche bis dahin durch Ministerien, Verbände oder Stiftungen geschaffen wurden. Manche der Definitionen arbeiten dabei mit dem Begriff der „technologischen Souveränität“, andere unterscheiden zwischen Nationalstaaten, Individuen oder der Wirtschaft. Die Bertelsmann Stiftung definierte den Begriff im Jahr 2020 folgendermaßen:

> »*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.« [8]

Die Mitglieder der Fokusgruppe „Digitale Souveränität in einer vernetzten Gesellschaft“ definierten am deutschen Digital-Gipfel 2018 den Begriff so:

»*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.*« [8]

Beim Digital-Gipfel 2020 wurde der Begriff dann vereinfacht definiert:

»*Digitale Souveränität wird als Teilaspekt der allgemeinen Souveränität eingeordnet und umfasst die Selbstbestimmtheit im Digitalen. Grundlagen dafür sind Vertrauenswürdigkeit von Kommunikation, Kontrolle über Datenflüsse und Möglichkeit zu selbstbestimmter Handlung und Innovation.*« [8]

Am zweckmäßigsten erscheint jedoch die Definition des deutschen „Kompetenzzentrum öffentliche IT“ des Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS) im Paper „Digitale Souveränität“:

»*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.*« [9]

Durch die Einfachheit, Zweckmäßigkeit und Offenheit orientiert sich diese Ausarbeitung an der Definition der FOKUS-Gruppe. Diese Definition ist geeignet, Anwendung auf alle Bereiche der restlichen Kapitel zu finden – unabhängig von beispielsweise Hardware, Lieferketten oder digitalen Diensten. Des Weiteren setzt diese Definition nicht die „vollständige Kontrolle“ von etwas voraus, da das Konzept bzw. der Zustand der digitalen Souveränität wahrscheinlich nicht von einzelnen Mitgliedsstaaten sondern von der Gemeinschaft der Europäischen Union abhängig ist.

Die Gemeinsamkeiten der diversen Definition sind, dass die digitale Souveränität als Teilaspekt der allgemeinen Souveränität gesehen wird. Sie stellt sozusagen einen Teilbereich der vollumfänglichen Souveränität eines Staates oder einer Institution dar. Die Definitionen unterscheiden sich im Inhalt kaum, allerdings sind manche detaillierter beschrieben und gehen auf konkrete Bereiche wie beispielsweise „Datenflüsse“ ein.

3 Bisherige Literatur

Das Ziel dieses Kapitel ist es, einen ersten Überblick zu bisherigen Publikationen im Kontext der digitalen Souveränität zu geben. Recherchiert wurde dabei in den Datenbanken der wissenschaftlichen Publikationen sowie online mittels Suchmaschinen. Die im folgendem beschriebene Literatur stellt dabei einen Auszug der gesichteten Literatur dar.

Das Buch „Digitale Souveränität: Bürger | Unternehmen | Staat“ [10] aus dem Jahr 2018 unterscheidet beginnend zwischen Bürgerinnen und Bürgern, Unternehmen und dem Staat im Hinblick auf die digitale Souveränität. Im Bereich der Bürger:innen werden im speziellen die Themen soziale Medien, digitale Partizipation und soziodigitale Souveränität näher beleuchtet und in den Kontext der digitalen Souveränität der Personen gesetzt.
Im Bereich der Unternehmen werden die wirtschaftlichen Faktoren im Kontext der digitalen Souveränität beschrieben. Des Weiteren wird dabei kritisiert, dass »trotz aller Diskussionen und Ankündigungen fehlt in Deutschland bislang jedoch eine einheitliche Definition der digitalen Souveränität (...)«. [10]
Im Bereich der Staaten werden vor allem die Herausforderungen und Abhängigkeiten im Zuge der Digitalisierung der öffentlichen Verwaltung beschrieben. Dies jedoch hauptsächlich im Bereich von digitalen Diensten. Außerdem wird dabei auf die verschiedenen Herangehensweisen der unterschiedlichen Länder und großen Organisationen wie z. B. der Europäischen Union (EU), der United Nations (UN) oder der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) eingegangen. Vor allem wird dabei die EU kritisiert, welche »(...) eher in der Rolle einer Getriebenen, die in vielfacher Weise vor allem gegenüber den USA im Hintertreffen ist«. [10] Abschließend werden auch neue Anforderungen an die digitale Souveränität beschrieben, welche sich seit den Enthüllungen von Edward Snowden aus dem Jahr 2013 entwickelt haben.

Im Paper „Das Subjekt im politischen Diskurs zu digitaler Souveränität“ [11] werden ebenfalls drei Hauptsäulen von digitaler Souveränität beschrieben. Dabei handelt es sich um eine staatliche, eine wirtschaftliche und eine individuelle Dimension. Der Hauptfokus des Papers liegt dabei auf der persönlichen digitalen Sou-

veränität der Individuen und wie diese in Verbindung mit der staatlichen sowie der wirtschaftlichen digitalen Souveränität zu betrachten ist. Außerdem geht das Paper auf den politischen Diskurs in dieser Thematik im Kontext von digitalen Diensten und der IT-Sicherheit in Verbindung mit dem Individuum ein.

Das deutsche „Kompetenzzentrum Öffentliche IT“ des FOKUS hat in den letzten Jahren einige Paper in Zusammenhang mit digitaler Souveränität veröffentlicht.
Das Paper „Digitale Souveränität“ beginnt damit, die diversen Definitionen der digitalen Souveränität in einem Satz zusammenzufassen:

> »*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.*« [9]

Im Anschluss beschreibt das Paper einige Thesen zum Thema und erklärt, dass digitale Souveränität keine Eigenschaft oder Zustand ist, sondern »aus zahlreichen Facetten« besteht. Im weiteren Verlauf beschreibt das Paper das „Maß“ an digitaler Souveränität und wie diese erreicht werden kann.
Dabei werden unter anderem Themen wie „Allgemeinbildung“, „nutzungsfreundliche Hard- und Software“ und „technische und organisatorische Maßnahmen“ vertieft. Diese Themen werden dabei in den Kontext von „individueller“ und „institutioneller“ digitaler Souveränität gesetzt und aus Sicht von IT-Produzenten und Dienstleistern abgebildet. Abschließend beschreibt das Paper Handlungsempfehlungen, welche die Bereiche *Bildung*, *rechtliche Rahmenbedingungen*, *Datenschutz* und *Standardisierung* beinhalten.

Das Paper „Digitale Souveränität als strategische Autonomie“ [12] beschreibt „Schmerzpunkte im digitalen Staat“ und warum man an Stelle von „digitaler Souveränität“ lieber von „digitaler strategischer Autonomie“ sprechen sollte. Die Arbeitsdefinition der „strategischen Autonomie im Digitalen“ ist dabei folgende:

> »*Strategische Autonomie im Digitalen umfasst die Fähigkeiten des Staates, eigene politische, gesellschaftliche und wirtschaftliche Prioritäten umsetzen zu können, ohne dabei in ungewünschtem Maße durch Abhängigkeiten in der Digitalisierung eingeschränkt zu werden.*« [12]

Des Weiteren wird im Paper beschrieben, dass die Abhängigkeiten seit langer Zeit bestehen, sie jedoch erst seit kurzem von der Allgemeinheit verstanden werden und dadurch greifbar geworden sind. In einem generischen Ansatz werden die Abhängigkeiten des „Technologie-Bündels“ in die folgenden fünf Schichten

aufgeteilt und es wird beleuchtet, dass moderne digitale Anwendungen häufig auf komplexen Verschachtelungen dieser Schichten aufbauen:

- Software
- Netze
- Hardware
- Daten
- Plattformen

Im Weiteren Verlauf definiert das Paper sieben Souveränitätsdimensionen (*Wissens-*, *Forschungs-*, *Entwicklungs-*, *Produktions-*, *Betriebs-*, *Nutzungs-* und *Transparenzsouveränität*) sowie einen Steuerungsansatz, welcher aus den Dimensionen „Relevanz“, „Spezifität“ und „Wirtschaftlichkeit“ besteht. Abschließend beschreibt das Paper grobe Lösungsansätze sowie einige Handlungsempfehlungen.

Im wirtschaftspolitischen Thesenpapier „Wie Europa seine digitale Souveränität wiederherstellen kann“ [13] wird einleitend die immer weiter entgleitende Datensouveränität der Bürgerinnen und Bürger Europas beschrieben. Das Paper beschreibt in diesem Zusammenhang auch, welchen Einfluss dabei große datengetriebene Unternehmen – häufig außerhalb der EU – in der heutigen Zeit haben. Im Anschluss wird der Begriff der „Digitalen Souveränität“ beschrieben und von *Autarkie* und *Fremdbestimmung* abgegrenzt. Ebenfalls wird die Problemlage, in welcher sich Europa im digitalen Kontext befindet, in den Fokus gerückt. Das Paper vergleicht dabei die allgemeine Wirtschaftsleistung mit dem Anteil der technologischen Entwicklung innerhalb der Märkte USA, der EU und China. Wobei die allgemeine Wirtschaftsleistung der EU zwar mit der der USA vergleichbar ist, im technologischen Bereich die USA jedoch weit vor der EU zu finden sind. Abschließend beschreibt das Paper verschiedene Lösungsansätze welche sich in Diskussion befinden und unterscheidet dabei zwischen einem *marktliberalen* und *industriepolitischen* Ansatz.

Der Report „Digital sovereignty in Europe: A first benchmark“ [14] aus dem Jahr 2020 beginnt mit Zitaten von Politikerinnen und Politikern aus dem Bereich der digitalen Souveränität. Im Anschluss beschreibt das Papier drei Dimensionen von digitaler Souveränität: eine strategische, eine im Bereich der Cybersicherheit und eine im Sinne des Datenschutzes. Im weiteren Verlauf wird näher auf die geopolitische Situation sowie deren politischer Hintergrund beleuchtet. Dabei wird exemplarisch auf das Projekt GAIA-X bzw. die europäische Debatte um 5G eingegangen. Außerdem werden am Beispiel der COVID-Pandemie die sichtbar gewordenen Abhängigkeiten zu anderen Ländern herausgearbeitet – unabhängig davon, ob es um reine

Lieferketten oder digitale Dienst geht. Im weiteren Verlauf zeigt der Report eine Übersicht der EU-Staaten sowie deren Status im Kontext von digitaler Souveränität.

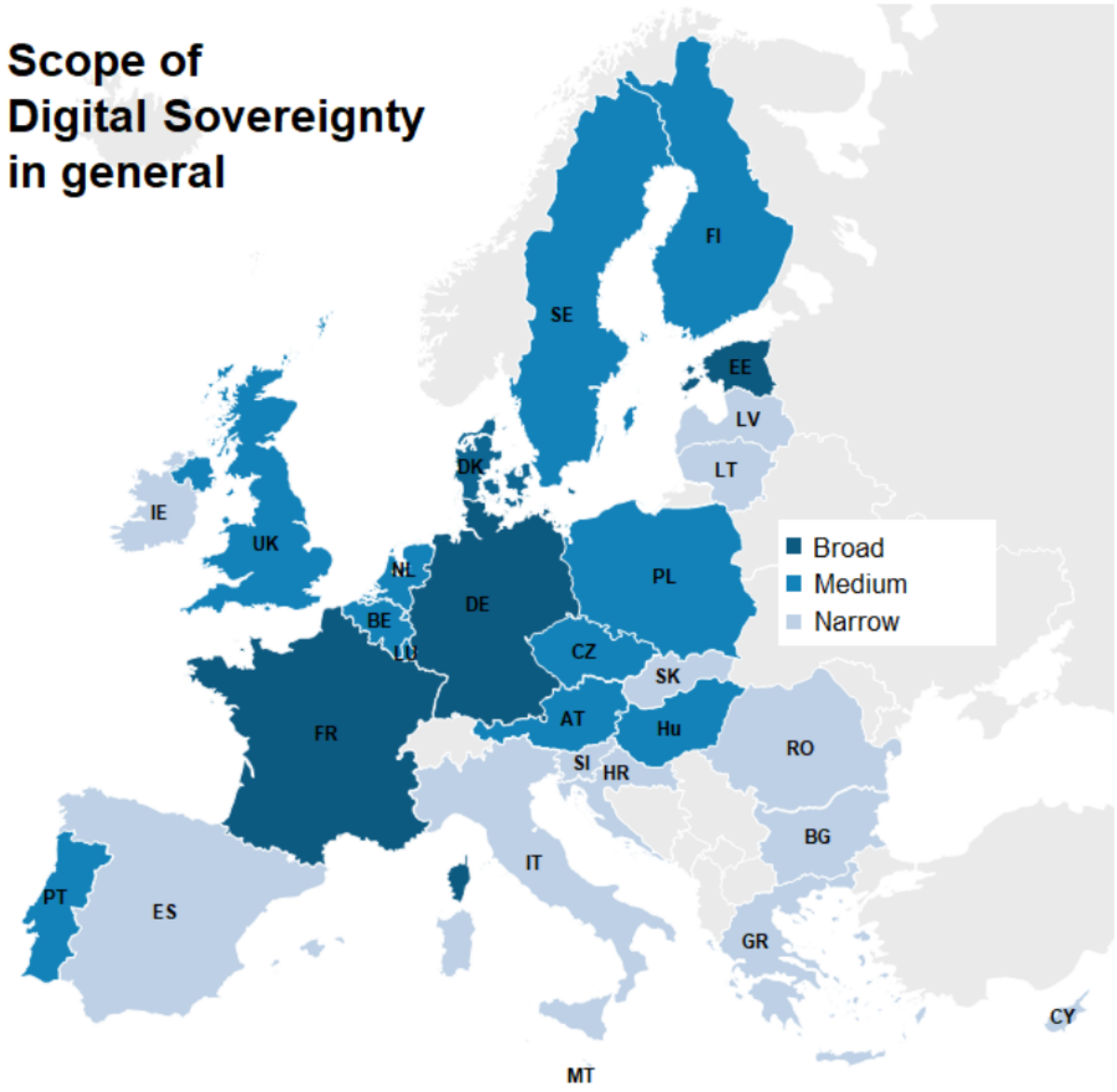

Abbildung 3.1: Ausmaß der digitalen Souveränität im Allgemeinen [14]

Der Report aus dem Jahr 2020 sieht Österreich dabei im Mittelfeld, in welchem sich die Länder den Fragen der digitalen Souveränität zwar stellen, dies jedoch eher in reaktiver Art und Weise. Außerdem wird erklärt, dass es eine dedizierte Strategie der digitalen Souveränität nur auf EU-Ebene sowie in Frankreich und Deutschland gibt. Die anderen Länder haben diese Strategie meist in anderen Strategien subsumiert. Deutschland wird dabei als größter Akteur im Kontext der digitalen Souveränität angeführt. Begründet wird

dies, da Deutschland Hauptakteur im Projekt GAIA-X ist und sich die deutsche Bundesregierung zu Informationstechnologie „Made in Germany“ verpflichtet. Der Report endet mit einem Anhang, in welchem detailliert auf jedes einzelne EU-Land eingegangen wird.

Das Paper „The fight for digital sovereignty: What it is, and why it matters, especially for the EU“ [15] beginnt mit einem Rückblick auf die COVID-Pandemie und geht auf die gescheiterten Versuche aus Deutschland und Großbritaniens ein, COVID-Tracking-Apps ohne das durch Apple und Google entwickelte Exposure Notification Framework zu entwickeln. Im Anschluss wird beispielhaft auf die Problematik bei 5G-Hardware und Social Media Apps aus China eingegangen und beschrieben, dass das alles »episodes in the fight for digital sovereignty« sind. Anschließend wird beschrieben, dass Staaten von Unternehmen digital abhängig sind und dass dies auch umgekehrt zutrifft, da Staaten die Regularien definieren. Im weiteren Verlauf wird auf die historische Entwicklung von Souveränität eingegangen und dass uns das digitale Zeitalter zwingt, diese zu überdenken. Es werden ebenfalls Formen beschrieben, wie Souveränität – analog und digital – zukünftig aussehen kann und dass vor allem die digitale Souveränität kein Thema Einzelner ist, sondern alle (Staaten, Unternehmen, Menschen) betrifft.

Abschließend lässt sich aus der Literaturrecherche zusammenfassen, dass digitale Souveränität zwar gewünscht wird und sie auch als strategisch wichtig erachtet ist, es aber ein kontinuierlicher Prozess ist, diese zu verbessern beziehungsweise zu erreichen. Der Report „Digital sovereignty in Europe: A first benchmark“ [14] aus dem Jahr 2020 beschreibt dabei am aussagekräftigsten, wie es um digitale Souveränität in Europa bestellt ist: Der Report lobt dabei explizit die Länder Deutschland, Frankreich und Estland, welche digitale Souveränität im europäischen Vergleich am besten thematisieren. Estland wird zusätzlich im Bereich der Datensouveränität gelobt, da es das einzige Land ist, das eine sogenannte „Daten-Botschaft“ (data embassy) installiert hat, in der kritische Daten als Backup in einem anderen Land aufbewahrt werden. Hervorgehoben wird dabei, dass diese „data embassy“ – vergleichbar mit einer gewöhnlichen Botschaft – unter der vollen Kontrolle des Landes steht und dieselben Rechte besitzt (beispielsweise Immunität). Da Estland mit der „e-Estonia“-Initiative eine der digitalisiertesten Verwaltungen weltweit besitzt, kann man die Notwendigkeit von „data embassy“ nachvollziehen. Andere Länder sollten im Zuge der Digitalisierung dabei ebenfalls auf solche Konzepte aufbauen.

4 Ursachen und Formen der Abhängigkeit

Im folgenden Kapitel werden die Ursachen und Formen der Abhängigkeiten im Kontext der digitalen Souveränität beschrieben. Dabei wird versucht, auf die verschiedenen Arten einzugehen und den Fokus auf Europa bzw. die EU zu legen. Dass es dabei für die Abhängigkeiten nicht eine Ursache gibt, sondern die Summe der Ursachen und Formen in Zusammenspiel stehen, wird ausführlich beleuchtet.

4.1 Ursachen

In der folgenden Sektion werden die Ursachen der Abhängigkeiten der Europäischen Union und Österreichs im Sinne der digitalen Souveränität strukturiert beschrieben. Die Untersektionen kann man dabei in technologische Abhängigkeiten sowie strukturelle Schwächen zusammenfassen. Die technologischen Aspekte der Abhängigkeiten sind dabei in Hardware, Software und digitale Dienste aufgeteilt. Die sonstigen strukturellen Schwächen beschreiben im Anschluss daran die rechtlichen Rahmenbedingungen sowie Defizite im Bereich der Bildung.

4.1.1 Hardware

Österreich und die EU haben die Abhängigkeit von Hardware in den letzten Jahren und Jahrzehnten ausgeweitet. Dabei ist es unerheblich ob von einzelnen Produkten oder von ganzen Firmenkonstellationen gesprochen wird. Beispiele hierfür gibt es zahlreiche, so wurde der deutsche Maschinenbauer „Kuka“ ab 2015 langsam von der chinesischen „Midea“ übernommen [16]. Bei den Halbleitern ist es ähnlich: 2021 schrieb das Handelsblatt noch, dass eine Abhängigkeit von China drohe. [17] Anfang 2022 stellt die Europäische Kommission dann den „EU Chip Act“ vor. Dieses Gesetz soll dabei die Wettbewerbsfähigkeit und Resilienz Europas im Kontext von Halbleitertechnologie erhöhen, da die Industrie eine Verdoppelung der Nachfrage dieser Produkte bis in das Jahr 2030 erwartet. Nach dem Vorschlag der Europäischen Kommission sollen dabei auch die Produktionskapazitäten innerhalb der EU so erweitert werden, dass bis 2030 etwa 20% der weltweiten Nachfrage gedeckt werden könnte. [18]

Die bereits erwähnten Halbleiterprodukte sind im Sinne von digitaler Souveränität jedoch nur die Basis. Die Abhängigkeit auf Hardwareebene besteht ebenfalls bei Endprodukten. Dazu zählen neben klassischen Produkten wie Computer und Smartphones auch Produkte von Netz- und Telekommunikationsausstattern. Die folgende Statistik zeigt die Anzahl der erteilten 5G-Patente der führenden Unternehmen weltweit im Jahr 2020:

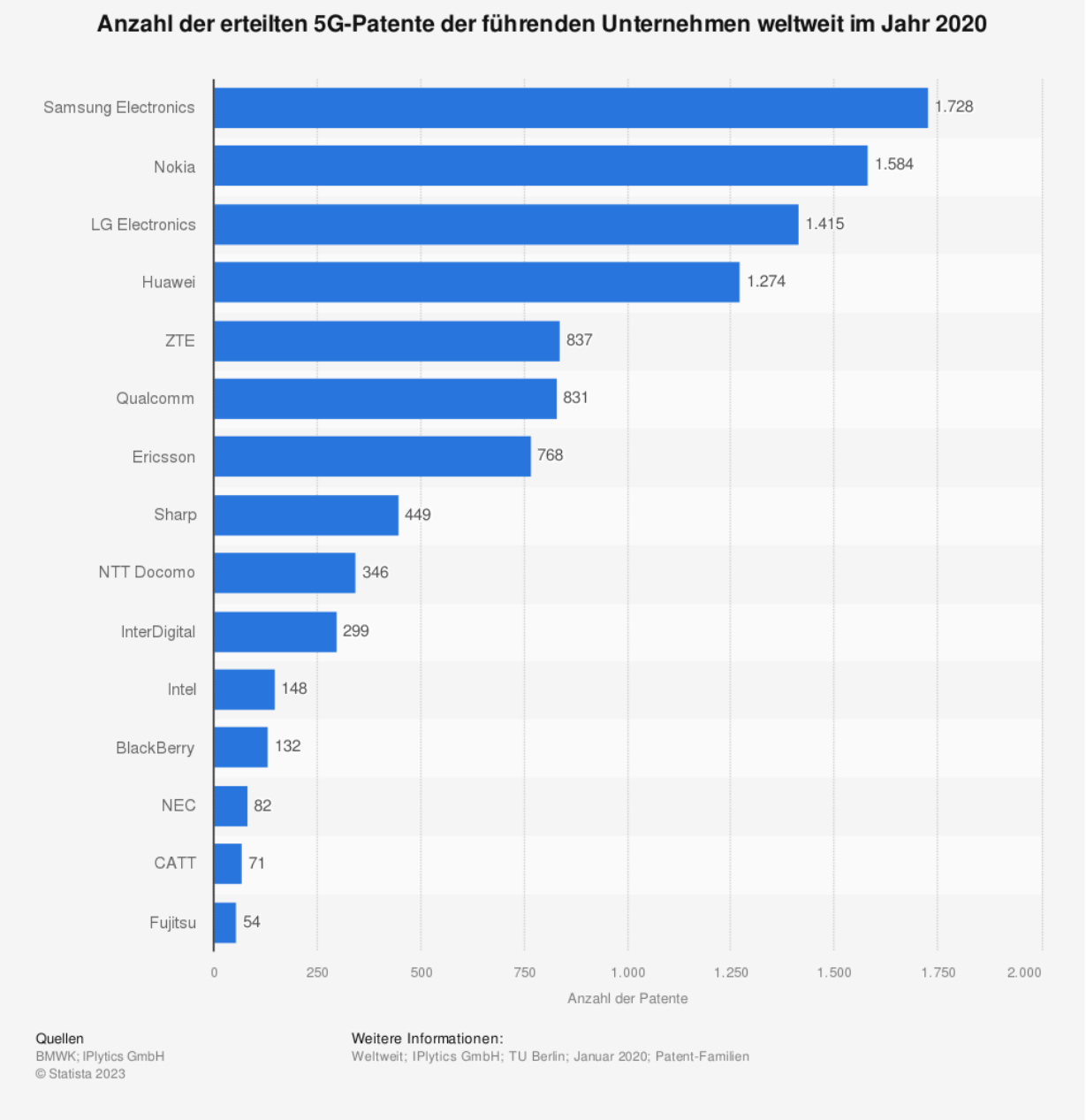

Abbildung 4.1: Anzahl der erteilten 5G-Patente der führenden Unternehmen weltweit im Jahr 2020 [19]

Wie in der Statistik zu erkennen ist, sind die meisten weltweit vergebenen Patente im Bereich 5G im asiatischen Raum angesiedelt. Mit Ericsson und Nokia sind zwar auch zwei große europäische Konzerne in der Statistik enthalten, sie zeigt aber dennoch, dass die Innovation im Bereich 5G eben nicht zu großen Teilen aus Europa kommt – und auch nicht aus den USA.

4.1.2 Software

Auch im Bereich der Software ist Europa abhängig. Ein Blick in die Büros zeigt, dass Standardsoftware für Endanwender hauptsächlich aus den USA kommt. Zu nennen sind an dieser Stelle die Betriebssysteme Windows und MacOS, aber auch Bürosoftware wie zum Beispiel MS Office. Eine Studie aus dem Jahr 2020 zeigt, dass der Marktanteil von Microsoft Office in Deutschland bei 85% lag. [20] Die folgende Statistik zeigt dazu ebenfalls die Abgeschlagenheit der Konkurrenzprodukte und, dass der Zweitplazierte (jedoch weit abgeschlagen) im Office-Umfeld die cloudbasierte Software as a Service (SaaS) Lösung von Google ist.

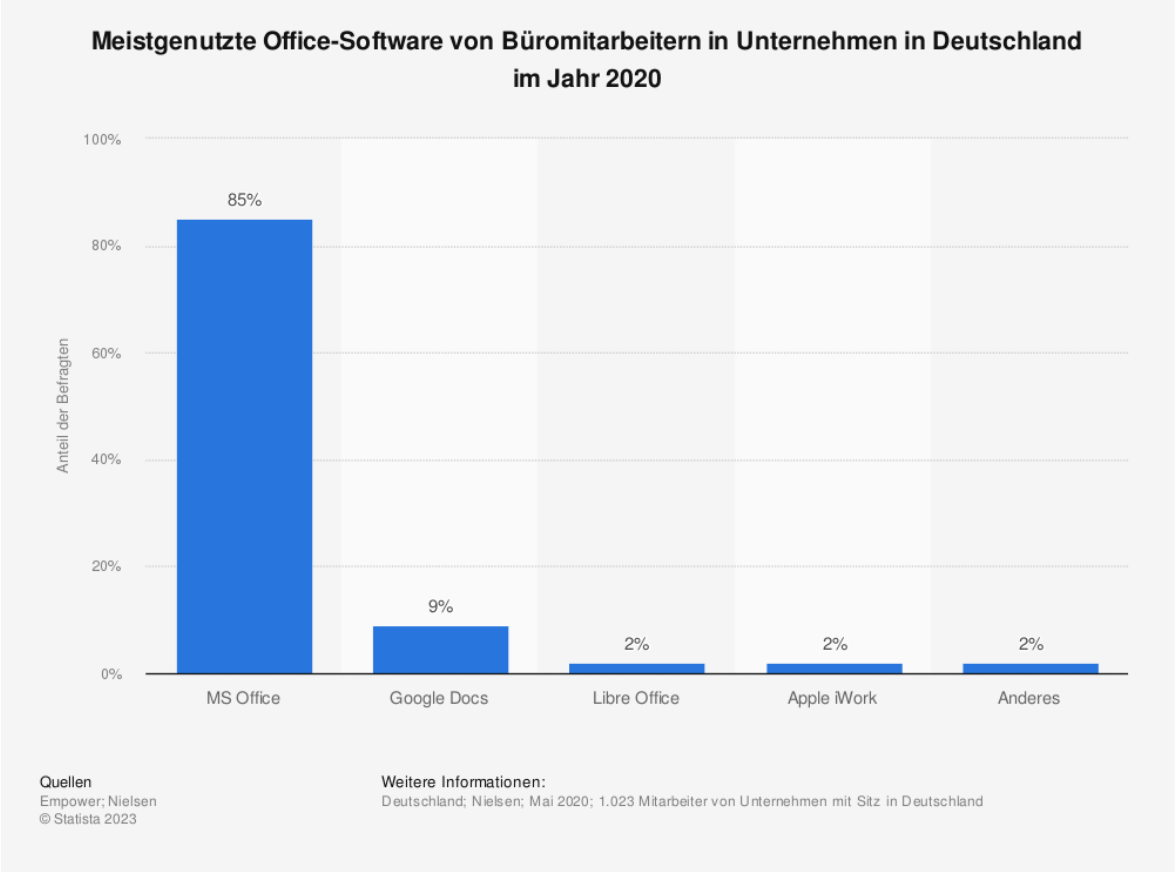

Abbildung 4.2: Meistgenutzte Office-Software von Büromitarbeitern in Unternehmen in Deutschland im Jahr 2020 [21]

Die Ursache dieser Abhängigkeit ist wahrscheinlich historisch begründet. Microsoft ist bzw. war mit den Produkten Windows und Office führend in der Innovation und konnte sich daher mangels vergleichbarer Produkte anderer Anbieter schnell weltweit etablieren.

4.1.3 Digitale Dienste

Im Kontext der digitalen Dienste ist Europa – ähnlich wie im Kapitel 4.1.2 – hauptsächlich von Nordamerika abhängig. Google, Facebook, Amazon, Netflix und Co. sind nur ein Auszug von Diensten, die in Europa und in Österreich in vielen Gesellschaftsbereichen zum Alltag gehören. Nur das chinesische Tiktok konnte sich im Kontext von Social Media bei uns etablieren und einen Markt – vor allem bei jungen Menschen – besetzen. Aktuell wird jedoch eine Debatte darüber geführt, ob Tiktok auf Dienstgeräten der öffentlichen Verwaltung installiert sein kann / soll / darf. [22] [23]
In Folgendem wird der Bereich der „Digitalen Dienste“ auf Basisdienste, Social Media und Kommunikation aufgeteilt und die Abhängigkeiten in diesen Bereichen näher beschrieben.

4.1.3.1 Basisdienste

Auch bei Basisdiensten wie z. B. DNS-Resolvern nehmen die Abhängigkeiten stets zu. Natürlich kann man Dienste wie einen DNS-Resolver selbst betreiben – Unternehmen und auch die öffentliche Verwaltung setzen aber mehrheitlich auf Kaufprodukte, die häufig aus dem EU-Ausland kommen. Im Endkundenbereich dominieren zwar die durch die Provider bereitgestellten Resolver, allerdings werden diese bei IT-affinen Menschen bei der ersten geblockten Seite durch meist US Dienste ersetzt. Der einzige wirklich große DNS-Resolver aus dem Europäischer Wirtschaftsraum (EWR) ist Quad9. Dieser wurde jedoch erst kürzlich wegen diverser Urheberrechtsverletzungen in Deutschland verurteilt. [24]
Theoretisch betrachtet ist die Abhängigkeit bei Basisdiensten lösbar. Russland hat im Jahr 2019 ein Gesetz verabschiedet, welches zusammenfassend den Aufbau eines eigenen „Internets“ vorsieht. Russische Internetdienstleister müssen durch das Gesetz sicherstellen, dass sie den Verkehr innerhalb ihrer Netze zentral kontrollieren können. [25] [26]
Praktisch betrachtet lässt sich die Abhängigkeit bei Basisdiensten nicht lösen ohne sich von der restlichen weltweiten Kommunikation zu trennen. Dies ist damit begründet, da der gesamte Aufbau des heutigen Internets bei der Internet Corporation for Assigned Names and Numbers (ICANN) organisiert ist. Diese Organisation vergibt weltweit IP-Adressen und organisiert die weltweiten DNS-Root-Server. Nachdem diese Organisation im US-Bundesstaat Kalifornien sitzt, unterliegt sie US-Recht, was im Sinne der digitalen Souveränität eine nicht lösbare Abhängigkeit darstellt. Allerdings könnte diese Abhängigkeit noch größer sein,

denn erst im Jahr 2016 übergab die US-Regierung die Internet Assigned Numbers Authority (IANA) – welche bis dahin die Verwaltung von IP-Adressen und DNS-Root-Server durchführte – an die NGO ICANN. [27]

4.1.3.2 Social Media

Auch bei Social Media ist Europa stark von den USA abhängig. Facebook, Instagram, YouTube und Co. dominieren den weltweiten Markt von Social Media. Allerdings gab es zu Beginn der Social Media Zeit auch große europäische Netzwerke. Die deutschen Netzwerke „Lokalisten“ und „StudiVZ“ entstanden in den 2005er Jahren und konnten sich am deutschen Markt durchaus etablieren. Zeitweise hatten diese Netzwerke mehr User als Facebook. [28] Allerdings wurden sie von der Internationalisierung von Facebook sowie der ständigen Weiterentwicklung der Plattform überrollt und gaben auf. [29]
Laut Angaben des österreichischen Jugend-Internet-Monitor 2023 sind fünf von sechs sozialen Netzwerken, welche von jungen Menschen genutzt werden, aus Nordamerika. Nur das chinesische TikTok kommt von außerhalb. [30]
Wieso sich europäische Netzwerke nicht durchsetzen konnten, kann nicht abschließend geklärt werden. Es ist jedoch davon auszugehen, dass die Vielzahl an Kulturen und Sprachen in Europa dazu beitrugen, dass keines der Netzwerke eine kritische Masse erreichte. In Russland beispielsweise konnte sich der lokale Facebook-Klon „VK.com“ sehr wohl etablieren, was eine Statistik aus dem Jahr 2022 zeigt. [31]

4.1.3.3 Kommunikation

Für souveräne Staaten ist Kommunikation essentiell. Dies wurde innerhalb der COVID-Pandemie deutlich. Regierungen und die öffentliche Verwaltung mussten innerhalb von sehr kurzer Zeit Dinge besprechen und die Bevölkerung anleiten. Kommunikation per se verändert sich jedoch auch. Nehmen wir beispielsweise E-Mail als Kommunikationsmedium. Ursprünglich gedacht als federierbares System ist es heute aufgrund von wenigen großen Platzhirschen kaum noch – bzw. nur mir einem erweiterten Aufwand – möglich, eigene Mailsysteme zu betreiben. [32]
Staaten bzw. die öffentliche Verwaltung sind jedoch mit Großbetrieben vergleichbar und werden auch zukünftig in der Lage sein, Mailsysteme selbst zu betreiben. Allerdings werden sie – sofern sie die Datenhoheit behalten und die Systeme weiterhin selbst betreiben – wahrscheinlich das zugrunde liegende Produkt tauschen müssen. Dies ist dem Grund geschuldet, dass in den letzten Jahren ein kontinuierlicher Druck in Richtung Cloud durch die Hersteller ausgeübt wird. Ein Beispiel eines Herstellers, welcher seine Strategie von „Cloud first“ in Richtung „Cloud only“ entwickelte, ist Atlassian. Seit dem Jahr 2021 verkauft Atlassian

keine Lizenzen für den On-Premises Betrieb der eigenen Produkte mehr und drückt damit die eigene Kundschaft in die Cloud. [33] Die Atlassian Produkte sind zwar keine Mailsysteme, dennoch ist die Tendenz auch bei anderen Herstellern erkennbar.

Für die öffentliche Verwaltung sind Cloud-basierte Kommunikationsdienste derzeit noch kaum ein Thema. Falls jedoch beispielsweise Microsoft seine Nutzungsbedingungen in eine Cloud-Richtung abändert, kann das sehr wohl die Souveränität der E-Mail-Kommunikation beeinflussen.

Neben der E-Mail-Kommunikation gibt es allerdings auch Weiterentwicklungen innerhalb der Kommunikation. Messenger-Apps haben auf so ziemlich jedem Handy Einzug gehalten – und das auch bei Regierungen. Die Chat-Affäre in Österreich, welche durch die Beschlagnahmung von Backupmedien durch die Wirtschafts- und Korruptionsstaatsanwaltschaft (WKStA) entstand, zeigt das deutlich. [34] Es gibt zwar Messenger-Systeme welche dezentral (vgl. E-Mail System) funktionieren und somit souverän betrieben werden könnten, allerdings sind diese in der Fälche eher unbekannt. Ein weiteres Thema, welches uns in Abhängigkeiten von einigen wenigen zentral – und in der Regel außerhalb von Europa – bereitgestellten Messenger-Apps getrieben hat, ist die Userbase. Netzwerke funktionieren nur erfolgreich, wenn sie eine kritische Masse von Benutzerinnen und Benutzern haben. Die folgende Statistik zeigt die Abhängigkeit Österreichs von vorwiegend US-Messenger-Apps deutlich. [35]

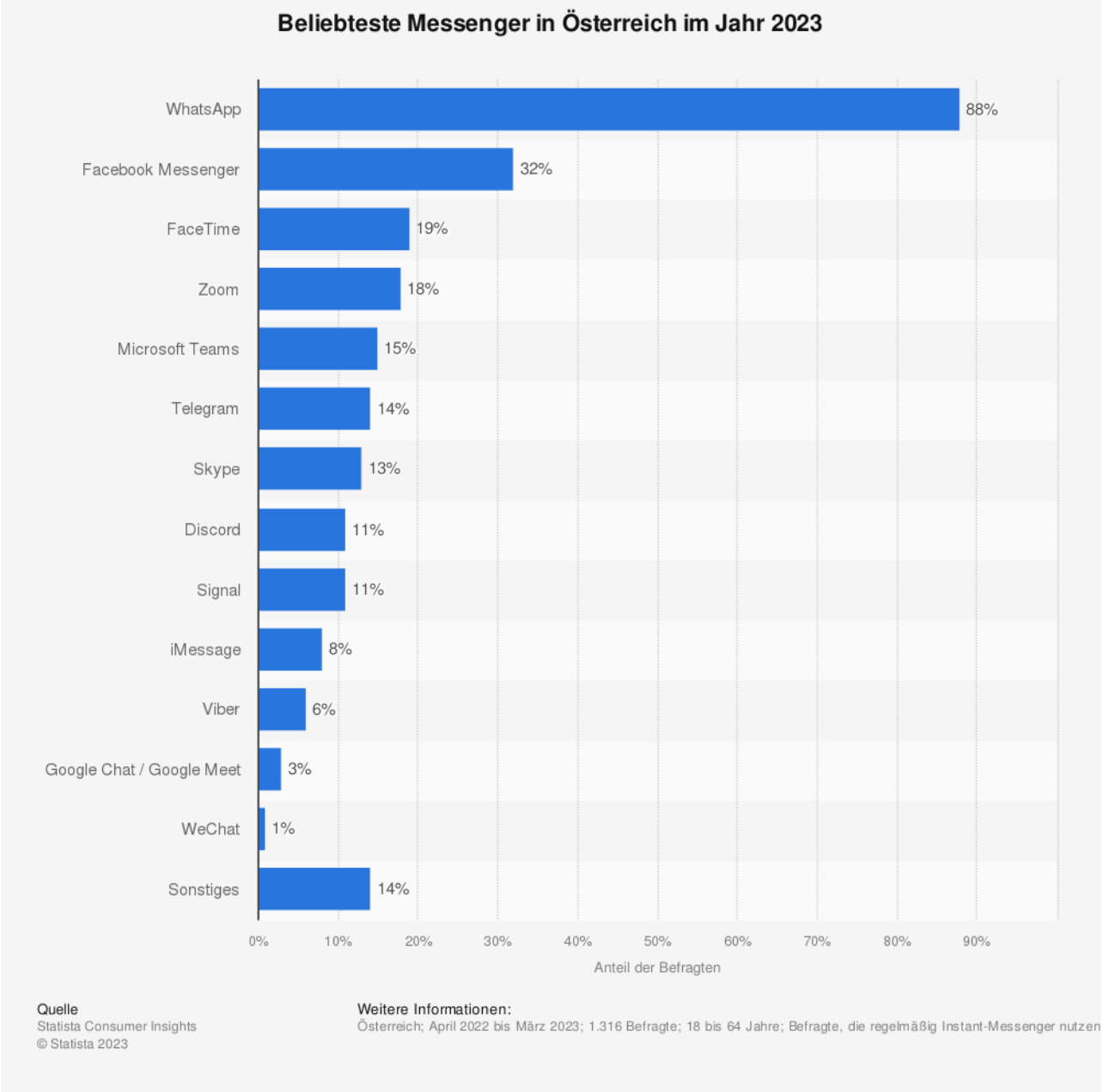

Abbildung 4.3: Beliebteste Messenger in Österreich im Jahr 2023 [35]

4.1.4 Sonstige strukturelle Schwächen

Die sonstigen strukturellen Schwächen beschreiben Querschnittsthemen, die sich jedoch auch auf Ursachen der digitalen Abhängigkeit zurückführen lassen.

Eine essentielle Ursache der derzeitigen Abhängigkeit ist im Bildungswesen verankert. Schülerinnen und

Schüler, Auszubildende oder Studentinnen und Studenten werden hauptsächlich auf Produkten von US Big-Tech-Unternehmen ausgebildet und erwarten diese Umgebungen dann auch bzw. präferieren diese als Entscheidungsträgerinnen und Entscheidungsträger im späteren Berufsleben.

Diese Problem wird – hauptsächlich im Kontext des Datenschutzes – unter anderem durch die Initiative Open Source Open Schools Austria (OSOS)[1] aufgezeigt. Der Verein setzt sich für Open Source, Datenschutz und der Unabhängigkeit von Produkten und Herstellern ein und kritisiert die erst kürzlich getroffene Entscheidung der TU Wien, die Mailboxen der Studierenden zu Microsoft 365 zu migrieren. Diese Entscheidung wurde unter anderem auch durch epicenter.works kritisiert [36]. Die TU Wien ist mit dieser Entscheidung allerdings nicht alleine. Auch die FH St. Pölten bildet ihre Studierenden indirekt an den Produkten von Microsoft aus. Dies mag für die technischen Studiengänge nicht wirklich relevant sein, alle anderen Studiengänge kennen jedoch nur diese Produkte und erwarten diese im späteren Berufsleben. Außerdem werden die heute ausgebildeten Personen zukünftig zu den Ausbilderinnen und Ausbildern der nächsten Generationen. Dadurch entsteht eine Art „Spirale“ welche bspw. die heutige Dominanz von Microsoft Produkten erklären könnte. Im Clientbereich verliert Microsoft zwar langsam Marktanteile an Apple, Open Source-Clients stagnieren allerdings, was die Abbildung 4.4 zeigt.

Interessant ist in diesem Kontext auch, dass die Mailboxen von österreichischen Lehrerinnen und Lehrern („@bildung.gv.at“) in der Microsoft-Cloud betrieben werden. [38] In Frankreich wäre dies beispielsweise nicht möglich, da dort die Nutzung von Cloud-Dienste wie Microsoft 365 oder Google Workplace verboten ist. [39]

Die strukturellen Schwächen beschränken sich nicht nur auf den Bildungsbereich. Es ist auch eine kulturelle Schwäche. Während in den USA frei nach dem Motto „try, fail and try it again“ agiert wird, ist in der europäischen Kultur das „Versagen“ negativ belastet. Dadurch wird Innovation bzw. der Prozess der Innovation erschwert. [40]

Das ist – zusammen mit einer gewissen Risikoaversion – wahrscheinlich ebenfalls ein Grund wieso die großen Tech-Unternehmen eigentlich alle in den USA sitzen.

Neben der Bildung und der kulturellen Frage sind es aber auch rechtliche Rahmenbedingungen welche zu den Ursachen zählen, dass Europa in dieser digitalen Abhängigkeit ist. Europa und die Mitgliedstaaten haben große rechtliche Regelwerke und bürokratische Prozesse, welche innovationstreibende Unternehmen abschrecken. Dadurch versuchen viele (beispielsweise Start-Ups) ihr Glück unter anderem in den USA zu suchen. Zusätzlich ist es in den USA einfacher Risikokapitalgeber:innen zu finden.

[1] `https://linux-bildung.at/` letzter Aufruf am 09.04.2023

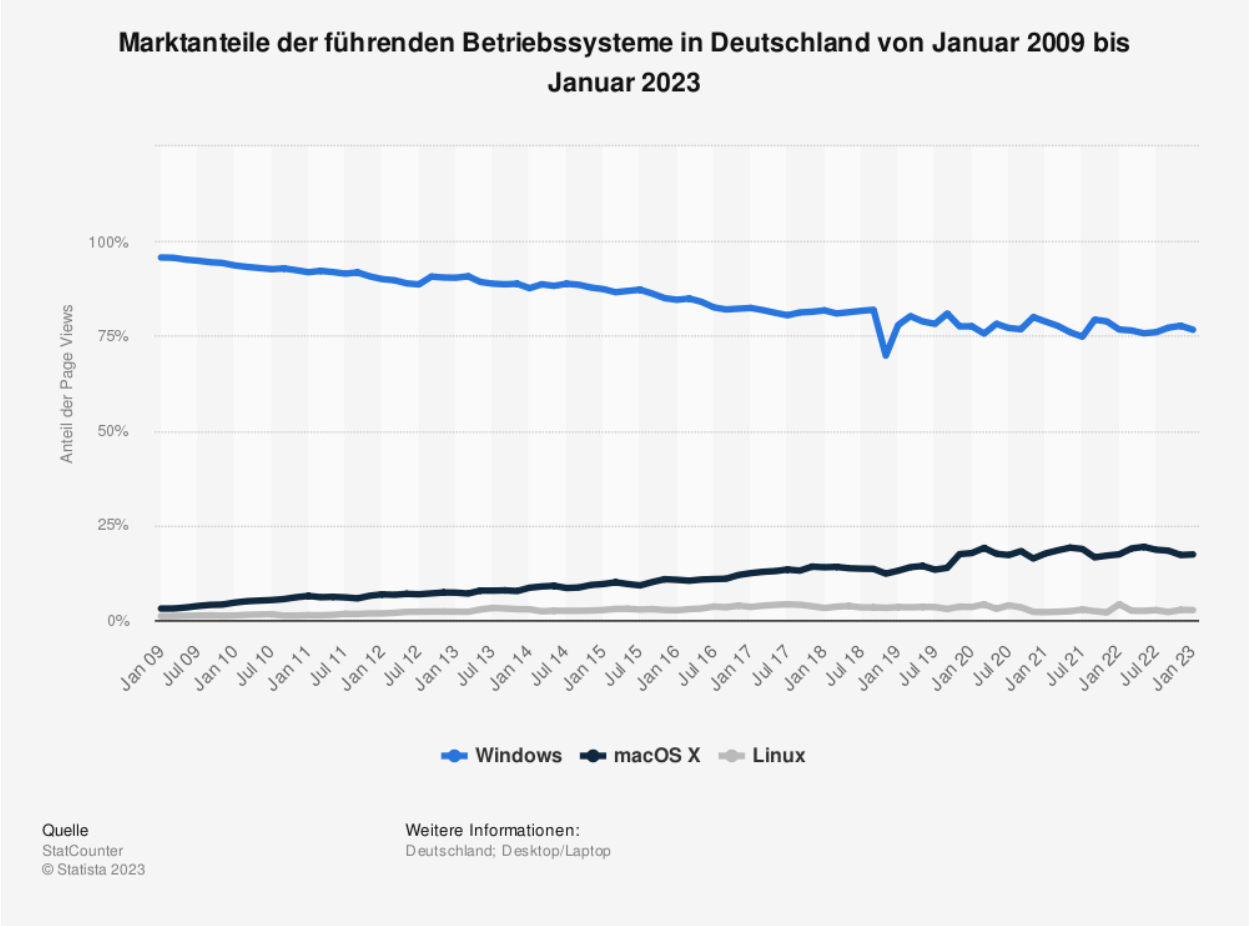

Abbildung 4.4: Marktanteile der führenden Betriebssysteme in Deutschland von Januar 2009 bis Januar 2023, Anteil der Page Views unterschieden zwischen Windows, macOS X und Linux [37]

4.2 Formen

4.2.1 Rohstoffe und Zulieferprodukte

Nicht zuletzt die Covid-19-Pandemie hat gezeigt wie abhängig Österreich und ganz Europa von funktionieren Lieferketten und einer globalisierten Handelswelt ist. Ähnlich wie damals Masken zur Mangelware wurden sind im Kontext der digitalen Souveränität wohl hauptsächlich Zulieferprodukte zu nennen. [41] Das beginnt mit Chips im Allgemeinen und endet mit kleinen Lüftern welche für die Hardware benötigt werden und hauptsächlich im asiatischen Raum produziert werden. Unabhängig davon, ob der asiatische Raum Österreich und Europa beliefert, ist eine weitere Form der Abhängigkeit bei den Lieferketten zu erkennen. Die Blockade des Suezkanals durch den Containerfrachter „Ever Given“ im Jahr 2021 hat deutlich gezeigt, wie abhängig Europa und die Welt von globalen Lieferketten ist. [42] Diese Form der Abhängigkeit

hat allerdings einen entfernten Bezug zur und nur mittelbaren Einfluß auf die digitale Souveränität.

4.2.2 Zahlungsdienstleister

Zahlungsdienstleister bzw. die Zahlungsabwickler sind ein Paradebeispiel für eine Abhängigkeit im Kontext digitaler Dienste. Wenn man mit der eigenen Bankkarte ein Produkt oder eine Dienstleistung digital bezahlen will, wird diese Abrechnung von einem der wenigen aber durchaus großen Zahlungsabwicklern verarbeitet. Für Mitteleuropa sprechen wir hier vor allem von den Firmen Visa und MasterCard. Beide sind amerikanische Unternehmen, die allein durch ihre Stellung im Markt in Europa auf Knopfdruck das bargeldlose Bezahlen bei uns abschalten könnten. [43]

4.2.3 Bildung

Auch im Bildungsbereich lässt sich eine Form der Abhängigkeit erkennen. Ausbildende vermitteln Auszubildenden stets das Wissen, das sie selbst verinnerlicht haben. Aus diesem Grund sind in einem Großteil der Bildungseinrichtungen beispielsweise Produkte von Microsoft etabliert. Der gemeinnützige Verein Open Source Open Schools Austria (OSOS) will dazu beitragen, dass das »Österreichische Bildungssystem digital souverän in die Zukunft geführt wird und unsere SchülerInnen bzw. deren Daten nicht amerikanischen Software-Monopolisten ausgeliefert werden«. [44]

4.2.4 Suchmaschinen

Eine weitere Form der Abhängigkeit stellen Suchmaschinen dar. Suchmaschinen sind das Mittel der Wahl um in einer digitalisieren Welt an Informationen zu kommen. Eine Statistik (Abbildung 4.5) aus dem Jahr 2023 zeigt auch hier die deutliche Abhängigkeit von hauptsächlich US-amerikanischen Konzernen. Die einzige europäische Suchmaschine in der Statistik ist die Berliner Firma „Ecosia“, welche allerdings ökologische Ziele verfolgt und Suchergebnisse von Microsofts Bing-Suchmaschine ausliefert. [45]
Eine – einst erfolgreiche – europäische Suchmaschine fehlt allerdings in der Statistik. Die tschechische Suchmaschine „seznam.cz“ war bis im Jahr 2011 die meistgenutzte Suchmaschine Tschechiens mit einem Marktanteil von über 50%. [47] Die Suchmaschine konnte sich jedoch ab diesem Zeitpunkt nicht mehr gegen den Konkurrenten Google behaupten und hatte im Jahr 2020 „nur“ noch einen Marktanteil von knapp 25%. [48] Auch wenn die tschechische Abhängigkeit bei Suchmaschinen bei weitem geringer ist als im restlichen Europa, hat sie doch auch dort spürbar zugenommen. Allerdings ist die lokale Alternative vorhanden und kann daher auch jederzeit wieder genutzt werden.

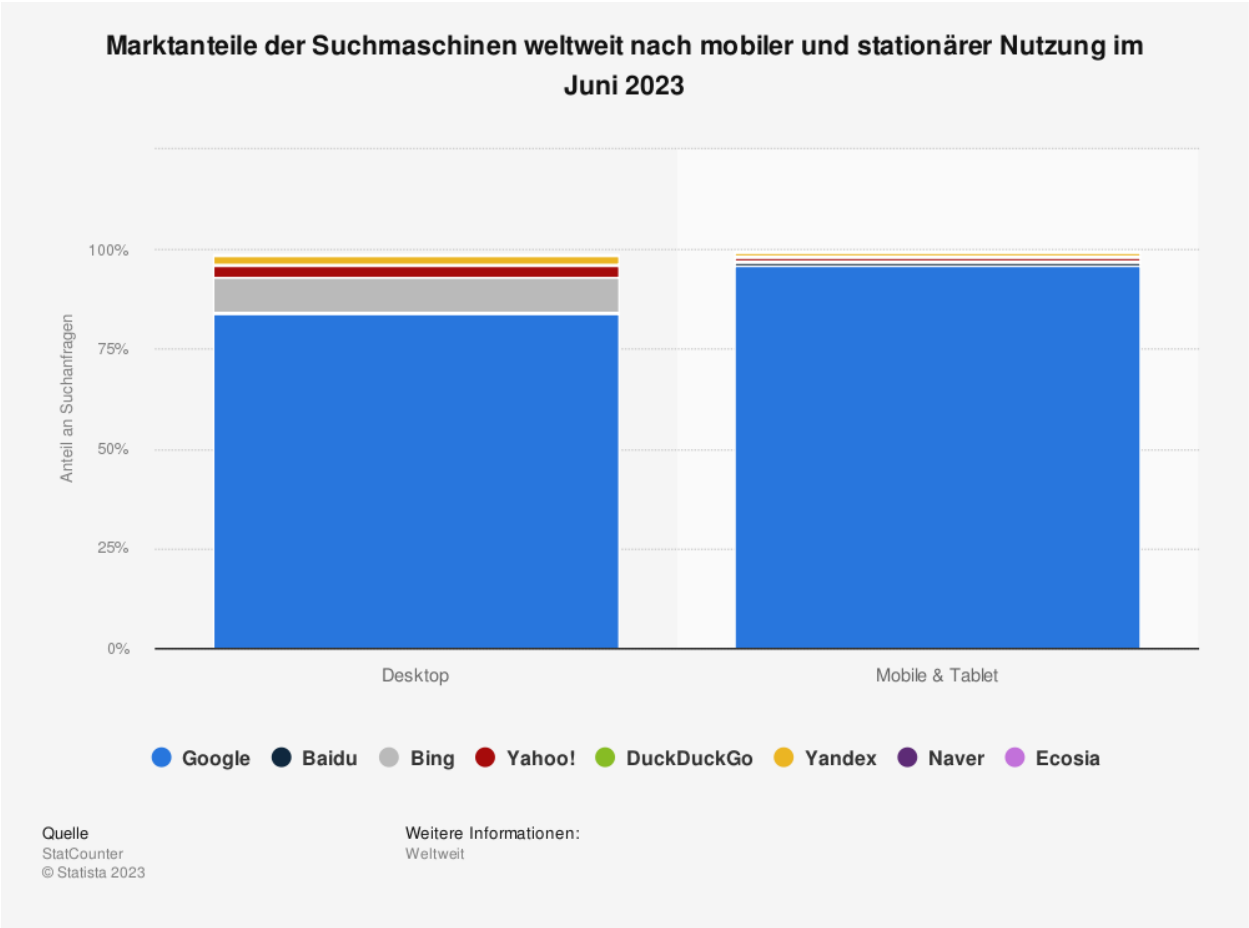

Abbildung 4.5: Marktanteile der Suchmaschinen weltweit nach mobiler und stationärer Nutzung im Juni 2023 [46]

5 Anforderungen an (digitale) Souveränität und Resilienz

In diesem Kapitel werden die Anforderungen an die digitale Souveränität und Resilienz beschrieben. Dabei werden die Anforderungen im Sinne eines souveränen Staats bzw. aus dem Blickwinkel der öffentlichen Verwaltung beachtet. Die folgenden sechs Anforderungen stellen dabei eine Ausgangsbasis dar, ohne die sich digitale Souveränität nicht vollständig umsetzen lässt.

5.1 Bildung und Kompetenz

Die (Grund)Ausbildung im Kontext von digitaler Kompetenz ist essentiell. Beispiele wie Microsoft zeigen, dass es sich lohnt in eine (Produkt)Ausbildung zu investieren. Bildungseinrichtungen können deren Produkte häufig kostenfrei oder zu vergünstigten Konditionen nutzen und bilden damit indirekt Auszubildende an diesen Produkten aus. Dies führ dazu, dass es für Unternehmen – oder aber auch die öffentliche Verwaltung – um ein Vielfaches einfacher ist solche Produkte einzuführen und deren Nutzer:innen daran weiterzuentwickeln. Nicht zuletzt aus diesen Gründen ist das Thema „Bildung und Kompetenz“ ein essentielles. Allerdings ist diese Thematik auch eine Querschnittsmaterie welche sich durch die weiteren Kapitel durchzieht.

Die Anforderungen an die Bildung sind vielseitig. Die Ausbildung sollte dabei die notwendigen digitalen Skills vermitteln und die grundlegende Technik. Im Beispiel „E-Mail“ sollte dabei nicht die Produktausbildung (z. B. Microsofts Outlook oder Googles Gmail) im Vordergrund stehen, sondern die Vermittlung der Grundlegenden Funktionsweise sowie die (offenen) Standard auf welchem alles aufsetzt.

Der Begriff „Digital Literacy“ beschreibt dieses Vorgehen. Wörtlich übersetzt bedeutet es „digitale Alphabetisierung“ und beschreibt dabei die Vermittlung von digitalem Grundwissen an die Menschen. Wie bei der Alphabetisierung wird es immer deutlicher wie wichtig digitale Grundkenntnisse sind. Die American Library Association (ALA) definiert das dabei folgendermaßen:

> »*the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills.*« [49]

5.2 Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen stellen eine weitere essentielle Anforderung an digitale Souveränität dar. Die aktuelle Situation – vor allem mit Anbieterinnen und Anbietern aus den USA – zeigt, dass es ohne eine rechtliche Handhabe nicht möglich ist eigene Souveränität im digitalen Sinn durchzusetzen. Beispiele sind hierbei der Clarifying Lawful Overseas Use of Data Act (CLOUD-Act), welcher für US-Behörden die rechtliche Handhabe schafft um auf Daten innerhalb von Public Clouds zugreifen zu können. Dabei wird nicht unterschieden ob es sich um Daten eines souveränen Staats oder aus der Wirtschaft handelt. Ebenfalls ist es irrelevant wo sich die Daten physikalisch befinden.
Ein vergleichsweise kleines Land wie Österreich wird es allerdings nicht schaffen, die digitale Souveränität in Verbindung mit lokalen Anbietern und der lokalen rechtlichen Situation abzusichern. Aus diesem Grund ist das Kapitel „Zusammenarbeit und Partnerschaft“ (5.5) ein essentieller und relevanter Punkt für die ganze EU. Auf europäischer Basis wurden dabei auch die rechtlichen Rahmenbedingungen geschaffen, welche Unternehmen aufgrund der europäischen Größe auch berücksichtigen. Einiges an relevanten rechtlichen Rahmenbedingungen, die im Sinne der digitalen Souveränität wirken, wurde dabei schon geschaffen.
Die Datenschutzgrundverordnung (DSGVO) beispielsweise regelt den Schutz von personenbezogenen Daten innerhalb der EU. Sie hat dabei das Ziel, die Souveränität der Bürger:innen im Kontext der eigenen personenbezogenen Daten sicherzustellen. Ein weiteres Beispiel ist der „EU Cybersecurity Act“ auf dessen Basis die European Network and Information Security Agency (ENISA) gegründet wurde. Ein weiterer Rechtsakt der im Sinne der digitalen Souveränität wirkt, sind die NIS-Richtlinien die seit der Überarbeitung beispielsweise die ganze öffentliche Verwaltung mit einschließt und sie dadurch zwingt, sich an Minimalanforderungen für Cybersicherheit und Resilienz zu halten. Was in diesem Kontext ebenfalls noch essentiell ist, ist der Standort. Dieser ist im Kontext der rechtlichen Rahmenbedingungen relevant, um Rechtsakte durchsetzen zu können.

5.3 Standort

Wie auch im Kapitel 5.2 erwähnt, ist die Wahl des Standorts für die (digitale) Souveränität essentiell. Ein souveräner Staat kann diese Souveränität am besten innerhalb des eigenen Staatsgebiet ausüben. Theoretisch wäre es zwar möglich, den Standort außerhalb des eigenen Staatsgebiets zu wählen, die Unsicherheiten sich

vollumfänglich auf die rechtliche Durchsetzung eines Partnerstaates zu verlassen wären jedoch wahrscheinlich zu riskant. Auch wenn das innerhalb der EU eigentlich keine Probleme machen sollte, ist es dennoch einfacher sich im eigenen souveränen Terrain zu bewegen. Das Beispiel Ungarn zeigt derzeit, dass Partner oder Verbündete sich auch im heutigen Zeitalter in eine Richtung entwickeln können, welche der eigenen Philosophie widerspricht. Im europäischen Parlament wird Ungarn in diesem Kontext sogar als „Wahlautokratie“ bezeichnet. [50]

Natürlich kann man die Standort-Frage auch differenzierter behandeln. Digitale Dienste und Services welche nicht zwingend für den Erhalt der eigenen (staatlichen) Souveränität wichtig sind, können sicherlich außerhalb des eigenen Territoriums genutzt werden. Einer solchen Entscheidung kann man sich mit den in der Informationssicherheit üblichen „Confidentiality, Integrity, Availability (C I A)“ Schutzzielen annähern. Falls der Schutzbedarf eines Services oder einer Anwendung niedrig ist, und es nicht zu erwarten ist, dass sich dieser grundlegend ändern wird, ist die Wahl des Standortes für den Betrieb eigentlich unbedeutend. Als Beispiel kann man hier eine Webseite nennen, welche ausschließlich Informationen bereitstellt, was bei einer Nichtverfügbarkeit dieser Website jedoch trotzdem keinerlei Auswirkungen hätte.

Manchmal ist die Wahl des Standorts aber auch ein zweitrangiger Faktor welche durch andere Prioritäten verdrängt wird. In Österreich konnte man das am Beispiel der COVID-bedingten „Pre Travel Clearence“ feststellen, welche man zeitweise in der Pandemie zur Anmeldung der Einreise nutzen musste. Das Web-Frontend, in welchem die personenbezogenen Daten einzugeben waren, war unter der URL „https://entry.ptc.gv.at“ erreichbar. Historische DNS-Daten zeigen, dass dieses Frontend auf der Microsoft Azure Cloud betrieben wurde[1]. Die in diesem Zusammenhang versendeten E-Mails wurden jedoch durch einen deutschen Service Provider verschickt.

Auch nach der COVID-Pandemie gab es im Zuge der Teuerung 2022 und 2023 Bürger:innen-Services welche über die Azure Cloud bereitgestellt wurden. Als Beispiel kann man hier den Energiekostenausgleich der Bundesregierung nennen, welcher unter „https://www.energiekostenausgleich.gv.at“ betrieben wurde. Auch hier zeigen historische DNS-Daten, dass das Frontend für die Bürgerinnen und Bürgern auf der Microsoft Azur Cloud Plattform betrieben wurde.[2].

Die Aussagekraft der Nutzung von Azure IP-Adressen ist allerdings stark begrenzt und sagt auch nichts darüber aus, wie die personenbezogenen Daten innerhalb dieser Anwendungen verarbeitet wurden. Man

[1] `https://dnshistory.org/dns-records/entry.ptc.gv.at` Letzter Aufruf am 21.05.2023

[2] `https://dnshistory.org/dns-records/www.energiekostenausgleich.gv.at` Letzter Aufruf am 21.05.2023

kann an dieser Stelle nur spekulieren, dass die notwendige Geschwindigkeit zur Bereitstellung der beiden Beispiel-Applikationen dazu beigetragen haben diese in einem Cloud-Service bereitzustellen. Weitere österreichische Bürger:innen-Services welche über Public-Clouds betrieben werden sind derzeit nicht bekannt.

Für sensiblere Daten wie beispielsweise Daten aus dem Identitätsdokumentenregister (IDR) oder dem Zentrales Melderegister (ZMR) kann man sich eine Datenverarbeitung mittels public Cloud Services oder außerhalb der eigenen souveränen Grenzen nicht vorstellen. Die COVID-Pandemie hat dies an einem grob vergleichbaren Beispiel deutlich gemacht: Grenzen zwischen den Ländern wurden geschlossen. Würde man so ein Szenario ins Digitale überführen, wäre das mit dem Blockieren eines ganzen Landes vergleichbar. Für essentielle und wichtige Dienste eines souveränen Staats wäre dies wohl der Supergau.
Nicht zuletzt aus diesen Gründen werden und sollten souveräne Staaten auch in Zukunft eigene Rechenzentren betreiben und sich nicht vollständig von Unternehmen abhängig machen.

Zusammenfassen kann man sagen, dass die Wahl des Standorts – sowohl im Sinne der digitalen Souveränität als auch im Kontext der Resilienz – eine entscheidende ist. Nur bei Standorten auf dem eigenen Hoheitsgebiet bzw. bei Partnerstaaten kann der physische Zutritt eingefordert werden wodurch Resilienz und digitale Souveränität gestärkt werden können.

5.4 Infrastruktur und Technologie

Infrastruktur und Technologie sind essentielle Themenbereiche um die digitale Souveränität zu erhöhen. Nur wer Infrastruktur selbst betreibt ist unabhängig und hat die Kontrolle über diese. Dadurch ergeben sich einige Vorteile wie beispielsweise Sicherheitsanforderungen bzw. Maßnahmen selbst zu definieren und diese auch kontrollieren und überwachen zu können. Eine gut ausgebaute Infrastruktur unterstützt nicht nur die eigene digitale Souveränität, sie unterstützt auch andere Bereiche wie bspw. die Wirtschaft und den Wirtschaftsstandort generell. Des Weiteren bietet eigene Infrastruktur innerhalb der Landesgrenzen die Möglichkeit, die rechtlichen Rahmenbedingungen selbst zu gestalten und zu kontrollieren und bietet daher Schutz vor politischer Einflussnahme von Drittstaaten. So kann zum Beispiel Datenschutz und Datensicherheit besser gewährleistet werden. Insgesamt ist eine robuste, zuverlässige und kontrollierte digitale Infrastruktur von zentraler Bedeutung für die digitale Souveränität. Sie ermöglicht es einem Land oder einer Organisation, ihre technologische Zukunft aktiv zu gestalten, unabhängig zu agieren und die eigene Sicherheit und Privat-

sphäre zu schützen.

Ähnlich zur Infrastruktur ist es mit dem Themenbereich Technologie gelagert. Wer eigene Technologie besitzt, verschafft sich Unabhängigkeit und Kontrolle über diese. Mit (eigener) Technologie und Infrastruktur ist es möglich, digitale Dienste selbst anzubieten und so unabhängig die Digitalisierung weiter zu stärken. Auch die Themenbereiche Datensicherheit und Datenschutz sind bei technologischer Führerschaft oder offenen Technologien besser zu kontrollieren. Zusätzlich zu den genannten Punkten bietet das mehr Anpassungsfähigkeit und Flexibilität. Eine selbst entwickelte Technologie erlaubt es, schnell auf sich ändernde Anforderungen und Bedrohungen zu reagieren. Man ist nicht länger von der Geschwindigkeit und Entscheidungsfähigkeit ausländischer Technologiekonzerne abhängig. Und das wiederum fördert die eigene Wettbewerbsfähigkeit.

Insgesamt trägt technologische Souveränität dazu bei, dass ein Land oder eine Organisation ihre digitale Zukunft in die eigenen Hände nehmen kann, anstatt von anderen Staaten oder Unternehmen abhängig zu sein. Dies ist besonders wichtig in einer zunehmend vernetzten und digitalisierten Welt, in der die Kontrolle über Technologie eine Schlüsselrolle für die nationale Sicherheit, wirtschaftliche Stabilität und den Schutz der Privatsphäre spielt.

5.5 Zusammenarbeit und Partnerschaft

Im Kapitel „Zusammenarbeit und Partnerschaft“ werden die – vor allem für kleiner Länder – relevanten Anforderungen für die digitale Souveränität beschrieben. Länder wie beispielsweise Österreich können die digitale Souveränität in Verbindung mit den heutigen Möglichkeiten der Digitalisierung nicht erreichen. Allerdings können Partnerschaften helfen die Risiken zumindest zu reduzieren bzw. besser zu verteilen. Eine der wahrscheinlich wichtigsten Partnerschaften ist in diesem Kontext die Europäische Union. Durch sie tritt Europa als großer Markt bzw. einheitliche Entität auf, welche sich dadurch im Weltgeschehen besser behaupten kann. Außerdem schafft die EU verlässliche Rechtssicherheit, um Technologien oder Dienste anderer Mitgliedstaaten auch in einem souveränen Kontext nutzen zu können. Durch Zusammenarbeit und Partnerschaft kann aber auch die Effizienz – auch im Sinne der digitalen Souveränität – gesteigert werden. Es ist nicht nötig, dass alle Länder mit vergleichbaren Prozessen vieles parallel erledigen. Ein Beispiel kann hier der Bundesmessenger sein, den Deutschland längst entwickelt hat. Diesen könnten beispielsweise andere Länder nutzen oder weiterentwickeln und den eigenen Bedürfnissen anpassen ohne von vorne beginnen zu müssen.

Zusammenarbeit und Partnerschaft ist aber auch wichtig, da es unmöglich ist alles – von Know-how, über

Technologien, bis hin zu Ressourcen – selbst zu besitzen bzw. verfügbar zu machen. Ein zentrales Beispiel aus Österreich zeigt das deutlich: Die Pensionierungswelle und der weiter steigende Fachkräftemangel.
Wie man an diversen Militärbündnissen erkennen kann, sind Partnerschaft und Zusammenarbeit nicht nur im Digitalen Kontext relevant. Durch diese Bündnisse steigt die Macht, die man am Weltgeschehen hat. Dies ist eins zu eins auf den Scope der digitalen Souveränität übertragbar.

5.6 Offene Datenstandards

Durch offene Datenstandards und Interoperabilität lassen sich zukunftsfähige Systeme und Anwendungen entwickeln, bei denen man sich nicht einem Anbieter ausliefern muss. Dies unterstützt beispielsweise auch der Vorbeugung eines sogenannten „Vendor-Lock-In“. Des Weiteren unterstützen offene Schnittstellen und Datenstandards die weitere Digitalisierung und den Zusammenschluss verschiedenster Systeme. Unternehmen, welche beispielsweise ein Enterprise Resource Planning (ERP)-System vollständig etabliert haben, setzen in der Regel auf ein System. Würden sie dieses System austauschen wollen, geht das häufig nur mit kostspieligen Großprojekten und dauert eine lange Zeit. Wenn es hierbei aber offene Datenstandards gibt mit offene Schnittstellen, wäre ein solcher Austausch einfacher und günstiger abzubilden. Alleine schon aus dem Grund, weil es keinen Big-Bang braucht, sondern einzelne Teile peu à peu ausgetauscht werden könnten. Ebenfalls ein wichtiger Aspekt in Bezug zu offenen Datenstandards ist die langfristige Verfügbarkeit und Zugänglichkeit. Angenommen, man setzt auf Tools oder digitale Dienste mit proprietären Dateiformaten, so besteht immer die Abhängigkeit zum Hersteller. Falls dieser das Produkt einstellt, es nicht mehr weiter beschaffbar ist oder nicht mehr existiert, ist man mit kostspieligen Großprojekten konfrontiert um das Produkt zu tauschen. Auch die Bereiche „Innovation und Wettbewerb“ werden durch offene Standards gefördert, da vorhandene Daten so leichter anderen Systemen für eine ggf. neue Verwendung zugeführt werden können.
Aus Sicht von Herstellern, die eigentlich einen Vendor-Lock-In begrüßen, mag die Thematik anderes zu bewerten sein. Aus der Sicht von souveränen Staaten gilt es jedoch, solche Lock-In-Effekte bestmöglich zu verhindern, um sich nicht abhängig zu machen.

6 Ansätze und Initiativen

In diesem Kapitel werden ausgewählte Ansätze und Initiativen, die die digitale Souveränität fördern und bekräftigen beschrieben. Dabei werden neben spezifischen Projekten auch Ansätze beschrieben, wie Europa die digitale Souveränität stärken könnte.

6.1 LiMux

Die LiMux-Initiative aus München ist bzw. war ein Ansatz der Stadtverwaltung die rund 15.000 Arbeitsplatzrechner nach dem Ablauf des Windows NT4-Support 2003 mit freier Software zu betreiben. Der Initiative ging eine Studie voraus, die die technischen, strategischen und wirtschaftlichen Aspekte von kommerziellen Systemen, Open Source und Mischformen aus diesen Welten beleuchtete. [51] [52] Im Anschluss an diese Studie – bei welcher zwei Alternativen gleichauf waren – entschied sich eine Mehrheit des Stadtrats für eine herstellerunabhängige IT-Strategie auf freier Basis. Im Sinne der digitalen Souveränität war dieses Vorgehen lobenswert und zu begrüßen.
Im Jahr 2013 gab Microsoft bekannt, seinen deutschen Firmensitz aus dem Münchner Vorort Unterschleißheim ins Münchner Stadtgebiet zu verlegen. Kurz darauf debattierte man in München eine Rückkehr zu Microsoft. Schlussendlich beschloss der Stadtrat im Jahr 2017 wieder auf Microsoft Windows und Office zu setzen um mit „marktüblichen Standardprodukten“ zu arbeiten. Im Jahr 2020 folgte dann der erneute Strategiewechsel: München möchte – zumindest bei selbst entwickelter Software – »unter Berücksichtigung aller relevanten und rechtlichen Faktoren als Open Source Lösungen und beschafft priorisiert Open-Source-Lösungen, wo immer technisch und finanziell sinnvoll« [52] einsetzen.

Im Sinne der digitalen Souveränität war diese Initiative durchaus begrüßenswert. Wäre das Projekt gelungen, wären wahrscheinlich auch andere Städte und Gemeinden dem Münchner Weg gefolgt. Durch den politisch motivierten Rückbau des Projekts ist es wahrscheinlich, dass ähnliche Initiativen und Vorhaben zukünftig abgewürgt wurden, was sicherlich nicht im Sinne der digitalen Souveränität zu werten ist.

6.2 Airbus

Die Geschichte des heutigen Airbus-Konzern startete Ende der 1960er Jahre als Großbritannien, Frankreich und Deutschland in einem Übereinkommen die Zusammenarbeit auf dem Gebiet der Luftfahrttechnologie formulierten. Sie beschrieben darin, dass sie ohne ein solches Programm hinter den Amerikanern zurückbleiben würden.

> »*(...) without a joint programme of aircraft development and production, Europe would be left trailing in the wake of the Americans (...)*« [53]

Im Anschluss startete die Konzeption und der Bau eines ersten Flugzeugs (A300), welcher im Oktober 1972 seinen ersten Flug absolvierte. In den nächsten Jahren startete Airbus eine weltweite Verkaufstour, um Airlines von dem europäischen Produkt zu überzeugen. In den Folgejahren konnte Airbus eine Technologieführerschaft verzeichnen und entwickelte weitere Flugzeuge. Durch die Technologieführerschaft konnte Airbus immer mehr Airlines von den eigenen Produkten überzeugen und startete als tatsächliche Konkurrenz zu den US-Herstellern durch. [54]
Heute ist Airbus aus der Sparte der Großraumflugzeuge nicht mehr wegzudenken und bildet mit der amerikanischen Konkurrenz Boeing das wohl größte und bekannteste Duopol der Welt.

Airbus per se hat freilich nichts mit einem Ansatz der digitalen Souveränität Europas zu tun. Allerdings kann man den Konzern vielleicht als Vorbild für Ansätze in eine ähnliche Richtung nutzen. So könnte man sich in einem Gedankenspiel vorstellen, dass sich – ähnlich wie bei der Gründung von Airbus – europäische Technologiekonzerne zusammenschließen und eine europäische Konkurrenz zu Microsoft, Amazon und Google bilden. Der Vergleich zu Airbus hinkt natürlich. Airbus musste sich damals ausschließlich darauf konzentrieren, ein konkurrenzfähiges Flugzeug herzustellen. Im Sinne der digitalen Souveränität wäre hier jedoch nicht nur die Erstellung von Alternativprodukten zu sehen, man müsste auch die Gesellschaft dazu bringen, solche Alternativen zu nutzen.

6.3 Gaia-X

Gaia-X ist eine europäische Initiative zur Entwicklung einer sicheren und vertrauenswürdigen Cloud- und Dateninfrastruktur. Sie wurde ursprünglich von Deutschland und Frankreich ins Leben gerufen und hat sich mittlerweile zu einem europaweiten Projekt entwickelt, an dem mehrere Länder und Unternehmen beteiligt sind.

Das Hauptziel von Gaia-X besteht darin, eine souveräne europäische Cloud- und Dateninfrastruktur aufzubauen, um die Abhängigkeit von großen amerikanischen und chinesischen Cloud-Anbietern zu verringern. Dennoch arbeiten Unternehmen wie Microsoft, Google, Amazon und Alibaba im Projekt mit, was auch zu deutlicher Kritik führt. [55] Ziel des Projekts Gaia-X ist es nicht, einen eigenen Hyperscaler zu schaffen, sondern durch die Vernetzung von vielen kleinen (Cloud-)Anbietern Alternativen zu den großen, meisten amerikanischen Anbietern zu etablieren. [56]
Ob Gaia-X der europäische „Gamechanger“ im Public-Cloud-Sektor sein wird, wird die Zukunft zeigen.

6.4 Europäische Union

Auch die Europäische Union als Ganzes kann man als einen Ansatz sehen um die digitale Souveränität in Europa zu stärken. Die EU, mit ihren Anfängen als Wirtschaftsgemeinschaft, mit dem Ziel, als großer Markt den Wohlstand zu steigern, stellt heute eine Großmacht dar. Durch die wirtschaftliche Leistung sowie der Größe der Bevölkerung hat die EU einen internationalen Stellenwert, den einzelne Mitgliedstaaten wohl selbstständig nicht erreichen hätten können. Durch diesen Stellenwert hat die EU auch Möglichkeiten, internationalen politischen Druck für eine Steigerung der digitalen Souveränität aufzubauen.
Des Weiteren verfolgt die EU verschiedene Initiativen und Strategien, um die technologische Unabhängigkeit und Wettbewerbsfähigkeit Europas im digitalen Bereich zu fördern. Projekte wie Gaia-X (siehe 6.3) oder rechtliche Rahmenbedingungen wie die NIS-Richtlinien (siehe 6.5), der AI-Act (siehe 8.3), der Cyber Resilience Act (siehe 6.6) oder der Chip-Act (siehe 6.10) zeigen das deutlich.

6.5 NIS Richtlinie

Die NIS-Richtlinie und die NIS2-Richtlinie sind europäische Rechtsvorschriften, die sich mit der Cybersicherheit von Informationsnetzwerken befassen. NIS steht für „Network and Information Security“. Die Richtlinien zielen darauf ab, die Widerstandsfähigkeit und den Schutz kritischer Infrastrukturen und digitaler Dienste in der Europäischen Union zu verbessern.
Die NIS-Richtlinie wurde im Jahr 2016 eingeführt und war die erste EU-weite Rechtsvorschrift auf dem Gebiet der Cybersicherheit. Sie legt Anforderungen an Betreiber wesentlicher Dienste und digitale Diensteanbieter fest und fordert von den Mitgliedstaaten die Festlegung nationaler Strategien und die Einrichtung nationaler Behörden zur Gewährleistung der Cybersicherheit. [57]
Die NIS2-Richtlinie – die überarbeitete Version der bisherigen Richtlinie – wurde im Jahr 2022 verab-

schiedet. Sie soll die Effektivität und Resilienz des Cybersicherheitsrahmens der EU weiter verbessern. Die NIS2-Richtlinie erweitert den Anwendungsbereich der Richtlinie, um neue Sektoren und Dienstleistungen einzubeziehen, und stärkt die Zusammenarbeit zwischen den Mitgliedstaaten, insbesondere bei grenzüberschreitenden Cybersicherheitsvorfällen. Sie sieht auch höhere Anforderungen an Sicherheitsmaßnahmen und Meldepflichten vor. [58] Dadurch, dass es sich um eine EU-Richtlinie handelt ist sie nicht direkt in den Ländern anwendbar und muss von den Mitgliedstaaten erst in nationales Recht übernommen werden. Bis dahin gilt weiterhin die NIS1-Regelung, welche in Österreich im „Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz - NISG)“ abgebildet ist. [59]

Ein wesentlicher Unterschied von NIS1 zu NIS2 ist, dass die gesamte öffentliche Verwaltung sowie alle Anbieter von Rechenzentrumsdienstleistungen unter die Vorschrift fallen werden. Bisher konnte die öffentliche Verwaltung selbst definieren ob ein IT-Service NIS-Pflichtig ist oder nicht.

6.6 Cyber Resilience Act

Der Cyber Resilience Act (CRA) ist eine im Jahr 2022 von der Europäischen Kommission vorgeschlagene Cybersicherheitsverordnung. Die Verordnung zielt darauf ab, Cybersicherheitsverpflichtungen für alle Produkte mit digitalen Elementen aufzuerlegen, deren beabsichtigte und vorhersehbare Verwendung eine direkte oder indirekte Datenverbindung zu einem Gerät oder Netzwerk umfasst. Dabei sollen Grundsätze wie „(Cyber-)Sicherheit by Design“ und „by Default“ eingeführt werden. Des Weiteren sollen durch den CRA eine Sorgfaltspflicht für den Lebenszyklus von Produkten vorgeschrieben werden. [60]

Durch eine solche Sorgfaltspflicht müssen beispielsweise Produkte wie Handys oder sonstige Netzwerkkomponenten über einen definierten Zeitraum mit Sicherheitsupdates versorgt werden. Solche Vorgaben wirken sich dadurch indirekt auf die digitale Souveränität in Europa aus, da man zumindest davon ausgehen kann, dass Schwachstellen erkannt und behoben werden.

Der Vorschlag wird jedoch auch kritisch betrachtet, da die Möglichkeit besteht, dass die selben Anforderungen, welche an Unternehmen gestellt werden, auch an die Open Source Community gestellt werden könnten. [61] Da Open Source Projekte teilweise nur aus wenigen einzelnen Menschen oder gemeinnützigen Organisationen bestehen, und einen wichtigen Teil für den Weg in Richtung digitale Souveränität bedeuten, ist es nicht zielführend diese mit den selben Haftungsthemen zu konfrontieren wie Unternehmen. [62]

Falls die Haftungsfragen, vor allem im Bereich von Open Source, in der jetzigen Formulierung bleiben, könnte der CRA tatsächlich mittelfristig auch eine Schwächung der digitalen Souveränität in Europa bedeuten.

6.7 Matrix in öffentlichen Verwaltungen

Das Kommunikationsprotokoll „Matrix“ ist ein quelloffenes Protokoll zur Echtzeitkommunikation in föderierten Umgebungen. Durch das Protokoll lassen sich Instant Kommunikation wie Textnachrichten und Videotelefonie in einer Ende-zu-Ende-verschlüsselten Form abwickeln. Als Ausgangsbasis nutzt Matrix dabei die selben Ansätze und Algorithmen wie sie zum Beispiel auch in der Signal-App vorkommen. Allerdings in einer angepassten Form um diese für größere Gruppenräume mit sehr vielen Geräten praktikabel zu halten. [63]
Im Sinne der digitalen Souveränität gab es im 2018 einen Ansatz aus Frankreich, das Protokoll als Basis in der öffentlichen Verwaltung einzusetzen. In Verbindung mit der „Riot“-App will man so direkte Kommunikation innerhalb und zwischen Behörden ermöglichen und eine sichere und lokal betriebene Alternative zu WhatsApp und Telegram bieten. [64] [65]
Im Jahr 2020 verkündete die BMI GmbH – der IT-Dienstleister der deutschen Bundeswehr – ein ähnliches Vorhaben und veröffentlichte den auf Matrix basierenden Messenger für Angehörige der deutschen Streitkräfte. [66] Ein Fork, also eine Weiterentwicklung des für die Bundeswehr entwickelten Messengers, mit dem Namen „BundesMessenger“ befindet sich seit Ende 2022 in einer Betaphase und soll zukünftig in der öffentlichen Verwaltung Deutschlands eingesetzt werden. [67]

Solche begrüßenswerten Initiativen tragen durch den Open-Source-Ansatz und der Möglichkeit eines Eigenbetriebs dazu bei, die eigene digitale Souveränität – egal ob für Staaten, Unternehmen oder Bürgerinnen und Bürger – zu verbessern.

6.8 Social Media

Auch im Bereich von Social Media gibt es Initiativen, sich aus Abhängigkeiten lösen zu wollen. Spätestens seit der Übernahme von „X“ (vormals als Twitter bekannt) durch Elon Musk ist vielen Menschen klar, dass in relativ kurzer Zeit und ohne eigene Mitwirkung sich Plattformen aus dem Bereich Social Media grundlegend verändern können. So wurden im Beispiel von „X“ unter anderem die Nutzung der beliebten

Oberfläche „X Pro“ (vormals bekannt als Tweetdeck) an einen kostenpflichtigen Account geknüpft und im allgemeinen ein Abo-Modell für von „verifizierten“ Accounts eingeführt. [68]. Es ist dabei allerdings unerheblich, ob sich die Anpassungen auf Policies beziehen oder sich die Preisgestaltung bei der Nutzung des Application Programming Interface (API) oder des Services selbst ändert. Die Abhängigkeit von Social Media Diensten wurde dabei einer breiten Masse aufgezeigt, was einer dezentralen X-Alternative namens „Mastodon“ zu einem Höhenflug verhalf. [69]
Mastodon ist ein freies Open-Source Softwareprodukt welches heute auf dem „ActivityPub“ Protokoll des World Wide Web Consortium (W3C) basiert. Das Ziel der Software ist es, einen dezentralen und verteilten Micro-Blogging Dienst als Alternative zu Twitter bereitzustellen.
Durch die Twitter-Übernahme von Elon Musk und das folgende Chaos, bei welchem u.a. Journalistinnen und Journalisten willkürlich blockiert wurden, entschlossen sich manche Unternehmen und Behörden eigene Instanzen des verteilten Netzwerks aufzubauen. So startete beispielsweise der Medienkonzern „DerStandard“ eine eigene Instanz. [70] Behördlich betriebene Instanzen wie beispielsweise „social.bund.de“ und „social.network.europa.eu“ gab es im Kontext des Datenschutzes schon vor der Twitterübernahme. Allerdings wurden diese aufgrund der steigenden Nutzungszahlen im Netzwerk erheblich relevanter. [71]
Neben Mastodon betreibt beispielsweise die EU auch eine dezentrale Videoplattform Namens „EU Video“ welche auf Basis der freien Software „PeerTube“ bereitgestellt wird und ebenfalls auf dem „ActivityPub“ Protokoll beruht. Diese Plattform soll eine Alternative zu Googles YouTube sein. [72]

Auch wenn die genannten Initiativen eigentlich aus Datenschutzgründen entstanden sind, sind sie dennoch Beispiele dafür wie man im Bereich von Social Media auch die digitale Souveränität stärken kann.

6.9 Galileo

Galileo ist ein globales Satellitennavigationssystem, das von der Europäischen Union entwickelt und betrieben wird. Es wurde konzipiert, um eine präzise Positionsbestimmung, Navigation und Zeitmessung für verschiedene Anwendungen auf der ganzen Welt zu ermöglichen. Das Galileo-System besteht aus einer Konstellation von Satelliten im Weltraum, Bodenstationen und Empfängern, die von Benutzern verwendet werden, um ihre genaue Position zu bestimmen. Ursprünglich war Galileo ausschließlich für die zivile Nutzung bestimmt. [73] Im Jahr 2008 änderte das Europäische Parlament jedoch die Meinung und gab die militärische Nutzung mit großer Mehrheit frei. [74] Diese Freigabe zeigt deutlich, dass die EU dabei die eigene Souveränität stärken wollte und sich – vor allem – von der amerikanischen Abhängigkeit befreien

wollte.
Galileo ist die europäische Antwort auf das US-System „GPS“, das russische System „GLONASS“ oder das chinesische System „Beidou“.

6.10 Chips Act

Der European Chips Act ist eine EU-Rechtsverordnung mit dem Ziel, die lokale Halbleiterindustrie zu fördern und zu stärken, um sich von asiatischen Lieferländern und amerikanischen Konzernen im Kontext von Halbleiterprodukten unabhängiger zu machen. Die Gesetzesinitiative wurde nach grob zweijähriger Vorbereitung im zweiten Halbjahr 2023 verabschiedet. Ein konkretes Ziel des Chips Act ist es, möglichst viel von dem, was zur Produktion von Mikrochips notwendig ist, wieder nach Europa zu holen. Dabei soll bis 2030 der Anteil der in Europa produzierten Chips auf 20 Prozent verdoppelt werden. [75]
Die Verabschiedung des Chips Act ist unter anderem für Deutschland und Polen sehr wichtig. Deutschland und das Bundesland Sachsen-Anhalt planen seit längerem den Konzern Intel beim Bau eines neuen Halbleiterwerks in Magdeburg zu unterstützen, konnten dies allerdings nicht, da Wettbewerbsverzerrungen befürchtet wurden. Der Chips Act räumt diese nun aus dem Weg und schafft die Möglichkeit, den Bau mit knapp 10 Milliarden Euro zu subventionieren. [76] Vergleichbar zu dem geplanten Werk in Deutschland plant Intel ebenfalls ein Werk in Polen zu bauen. Dabei will Polen mit ca. 4 Milliarden Dollar, welche auch durch den Chips Act ermöglicht wurden, subventionieren. [77]

Durch die Möglichkeit, dediziert die Halbleiterproduktion in Europa zu stärken, stellt der Chips Act auch eine Initiative zur Verbesserung der Unabhängigkeit und somit zur Stärkung der digitalen Souveränität da.

7 Zusammenhang Resilienz und digitale Souveränität

Digitale Souveränität bezieht sich auf die Fähigkeit eines Landes oder einer Organisation, ihre digitalen Angelegenheiten eigenständig zu kontrollieren und zu gestalten, ohne dabei von externen Akteuren abhängig zu sein. Dies umfasst den Schutz digitaler Infrastrukturen, die Entwicklung und den Einsatz eigener Technologien sowie die Kontrolle über Daten und Informationen.
Resilienz hingegen bezieht sich auf die Fähigkeit eines Systems, Störungen oder Bedrohungen zu widerstehen, sich anzupassen und im Idealfall schnell zurück in den Regelbetrieb zu gehen. Im digitalen Kontext bedeutet dies, dass ein Land oder eine Organisation widerstandsfähig gegenüber Cyberangriffen, Datenverlust, technologischen Störungen oder anderen digitalen Bedrohungen sein sollte.
Digitale Souveränität trägt somit zur Resilienz bei, indem sie eine unabhängige Kontrolle über Systeme und Technologien ermöglicht. In der heutigen Zeit sind Systeme nur so resilient, wie es von den Herstellern und Anbietern vorgesehen ist. Nutzt ein Anbieter oder Hersteller das Abhängigkeitsverhältnis – welches aus der derzeitigen digitalen Unsouveränität resultiert – aus, ist damit auch sofort die Resilienz bedroht.

Zusammenfassend lässt sich sagen, dass digitale Souveränität und Resilienz eng miteinander verbunden sind. Eine starke digitale Souveränität unterstützt die Resilienz, indem sie die Kontrolle und den Schutz digitaler Infrastrukturen ermöglicht und die Abhängigkeit von externen Akteuren verringert. Dies stärkt die Widerstandsfähigkeit gegenüber digitalen Bedrohungen.

8 Artificial Intelligence

Im folgenden Kapitel wird versucht im Speziellen auf das Thema Artificial Intelligence (AI) einzugehen. Aber welchen Zusammenhang hat AI mit digitaler Souveränität? Die Technologie Artificial Intelligence steckt aktuell noch in den Kinderschuhen. Allerdings ist derzeit schon absehbar, dass sie das nächste große „Ding“ in der IT und im Kontext der Digitalisierung darstellen wird. Daher stellt sich die Frage, ob Österreich oder die EU auch bei der nächsten Technologie wie AI abhängig sein werden und somit nicht souverän agieren können.

8.1 Was ist AI?

AI steht für künstliche Intelligenz (englisch: Artificial Intelligence). Es handelt sich um ein Teilgebiet der Informatik, das sich mit der Entwicklung von Systemen befasst, die menschenähnliche Intelligenz aufweisen sollen. Künstliche Intelligenz ermöglicht es Computern, Aufgaben auszuführen, die normalerweise menschliche Intelligenz erfordern würden, wie zum Beispiel Spracherkennung, Bildverarbeitung und Entscheidungsfindung. [78]

Eine der Geburtsstunden der KI liegt in den 1950er Jahren mit Alan Turings Paper „Computing machinery and intelligence“. [79] Anstatt die Frage „Können Maschinen denken?“ zu stellen, stellte er die Frage, ob Maschinen ein Spiel, das „Imitation Game“, gewinnen können. An diesem Spiel nimmt ein Mensch, ein Computer und eine Schiedsrichterin bzw. ein Schiedsrichter teil. Die Schiedsrichter:innen stellen dabei Fragen, sowohl an den am Spiel teilnehmenden Menschen sowie an den Computer. Beide antworten. Und die Schiedsrichter:innen müssen entscheiden, wer Mensch und wer Computer ist.

Seit den 1950er Jahren hat sich AI aber bedeutend weiterentwickelt und es gibt unterschiedliche Herangehensweisen bei der Definition der AI-Ziele: [78]

- Starke AI
- Schwache AI

Von einer **schwachen AI** wird gesprochen, wenn die Ausführung einer Aufgabe auf menschlichem Niveau erfolgt. Dabei geht es hauptsächlich darum, konkrete Anwendungsprobleme zu meistern und die Aufga-

benerfüllung effizienter zu Gestalten als es beispielsweise mit menschlichen physischen Möglichkeiten der Fall ist. Eine **starke AI** beschreibt Systeme, die eigenständig und intuitiv ein komplexes Aufgabenspektrum ausführen können, das menschliche und, im weiteren Sinne, emotionale Intelligenz erfordert.
Beispiele für eine schwache AI sind derzeit unterstützende Systeme wie Amazons Alexa oder Google Assistant. Eine starke AI existiert gegenwärtig (noch) nicht. [80]
Aktuell sind die Menschen schon häufig mit AI konfrontiert, merken es aber oftmals nicht. Beispielsweise bei Systemen beim Onlineeinkauf. Anzeigen wie „Sie haben das im Warenkorb, es kann sein, dass Ihnen das auch gefällt“ oder die schon erwähnten Sprachassistenten existieren in großer Zahl.

8.2 Problemstellung

Aber wo genau ist nun die Problemstellung von AI in Verbindung mit digitaler Souveränität? Auf den ersten Blick ist diese eher nicht zu erkennen, da es sich bei AI um trainierte Modelle handelt die auch in Europa oder in Österreich trainiert werden könnten. Allerdings braucht es für ein gutes Training von solchen Systemen auch entsprechende Daten – sowohl bezüglich Masse als auch Qualität. Beim Thema „Daten“ wird es in Europa im Vergleich z. B. den USA schon etwas komplexer. Daten sind häufig personenbezogen und unterliegen dann beispielsweise in der EU der DSGVO. Es gibt aber auch noch andere rechtliche Regularien die die Verwendung von Daten regeln. Beispielsweise unterliegen Bankdaten dem Bankgeheimnis.
Aber bleiben wir beim Datenschutz: Diskussionen, dass Datenschutz beispielsweise Digitalisierung und Innovation verhindert gab und gibt es seit der Einführung der DSGVO im Jahr 2018. Ob das tatsächlich so ist, ist wahrscheinlich Ansichtssache. Die Bitkom, der Branchenverband der deutschen IT-Branche, schrieb im Jahr 2020 in einer Presseaussendung, dass »Bei mehr als jedem zweiten Unternehmen (56 Prozent) (...) neue, innovative Projekte aufgrund der DS-GVO gescheitert« sind. [81] Das Ziel der DSGVO ist allerdings nicht, Innovation zu verhindern, sondern individuelle personenbezogene Daten zu schützen und Menschen mit Rechten auszustatten, diesen Schutz auch durchsetzen zu können.
Eine vergleichbare Diskussion entwickelt sich derzeit auch in Verbindung mit AI. Spätestens seit Italien OpenAI untersagte, personenbezogene Daten von italienischen Bürgerinnen und Bürgern in ChatGPT zu verwenden. [82] Daten, egal welcher Art, sind jedoch essentiell zum Training solcher AI-Systeme. Daher steht die Befürchtung im Raum, dass die europäischen rechtlichen Rahmenbedingungen die Entwicklungen in diesem Bereich in Europa ausbremsen könnten.

Neben rechtlichen Rahmenbedingungen gibt es noch ein zweites Problem mit Daten. Ein Großteil der Daten,

die in den letzten Jahrzehnten generiert wurden, sind bei US-Technologieunternehmen unter Verschluss. Google, Facebook und all die anderen Big-Tech-Konzerne sitzen auf riesigen Datenbergen, welche für das eine oder andere AI-Training mit Sicherheit wertvoll ist.

Es gibt aber auch heute schon erfolgreiche AI-Dienste in Europa. Das Übersetzungstool DeepL mit Sitz in Köln existiert seit 2018. DeepL nutzt AI um eine möglichst akkurate Übersetzung in diverse Sprachen durchzuführen. Nach eigenen Angaben ist es dabei drei Mal akkurater als die Konkurrenz wie beispielsweise Google. [83]

Dass Daten und auch personenbezogene Daten der Schlüssel zu erfolgreicher AI sind, zeigt derzeit ein Fall in den USA. Dort wird der Betreiber von ChatGPT, die Firma OpenAI, aktuell verklagt. Die Klagenden werfen der Firma vor, private Daten und urheberrechtlich geschützte Informationen zum Training verwendet zu haben. [84]

8.3 AI Act

Der sogenannte AI Act ist ein Vorschlag einer EU-Verordnung der Europäischen Kommission. Ähnlich wie bei der Datenschutzgrundverordnung, hat er das Ziel, Risiken und Nachteile Einzelner zu verhindern und »einen Rechtsrahmen für eine vertrauenswürdige KI zu schaffen«. [85] Neben der Schaffung von Rechtssicherheit sollen durch den AI-Act auch ethische Themen und die Wahrung der Grundrechte und Werte der EU verordnet werden. Der AI Act sieht auch Anforderungen an verschiedene AI-Anwendungen vor. Dabei sollen mittels einem risikobasierten Ansatz AI-Anwendungen in vier Kategorien unterteilt werden um die Anwendungen entsprechend zu regulieren: [86]

- Nicht akzeptables Risiko (z.B. Social Scoring)
- Hohes Risiko (z.B. Bewerbungen oder medizinische Produkte)
- AI mit spezifischen Transparenzverpflichtungen
- Minimales oder kein Risiko

Für Systeme mit minimalem oder keinem Risiko werden dabei keine Anforderungen gestellt. Für „normale AI“, also AI-Systeme mit spezifischen Transparenzverpflichtungen wird u. a. die Anforderung gestellt, den Nutzenden darüber zu informieren, dass dieser mit einem AI-System arbeitet. In die Kategorie AI-Systeme mit hohem Risiko fallen unter anderem Systeme mit folgenden Zwecken bzw. Einsatzorten: [86]

- Sicherheits- oder regulierte Produkte
- Biometrische Identifikation von natürlichen Personen
- Management oder Betrieb von kritischer Infrastruktur

- Bildung im Allgemeinen
- Arbeitnehmerinnen-/Arbeitnehmermanagement
- Strafverfolgung, Migration und Asylwesen

An AI-Anwendungen dieser Kategorie sollen dabei spezielle Anforderungen gestellt werden. Unter anderen an die Qualität der Trainingsdaten, der Dokumentation und des Loggings, an die Transparenz, die Robustheit, Genauigkeit und Cybersicherheit.

Neben den genannten Anforderungen soll durch den AI-Act aber auch die Innovation unterstützt werden. So genannte KI-Reallabore, welche durch die Mitgliedstaaten oder die EU eingerichtet werden, sollen dabei »kontrollierte Umgebungen, um die Entwicklung, Erprobung und Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme nach einem spezifischen Plan zu erleichtern«. [85]

Ob der AI-Act in seiner jetzigen Form auch tatsächlich kommen wird bleibt abzuwarten. Viele Unternehmen und Forschende kritisieren diesen derzeit scharf. Er sei zwar mit »guten Intentionen gestartet worden, schieße aber an manchen Stellen am Ziel vorbei«. [87]

8.4 Ausblick

Artificial Intelligence ist in jedem Fall eine äußerst vielversprechenden Technologie und wird die Welt noch einige Zeit begleiten. Die Fortschritte dieser Technologie haben in den vergangen Jahren rasant zugenommen und das Potential ist sicherlich erst zu einem Bruchteil ausgeschöpft. Auch bei der Entwicklung von Anwendungsfällen sind der Kreativität keine Grenzen gesetzt. Ob im medizinischen Umfeld oder bei der Landwirtschaft, AI-Systeme werden zukünftig weiter an Relevanz gewinnen. Ob man durch die Regulierungsvorhaben der EU AI im Allgemeinen im Keim erstickt oder aber vielleicht ein relevantes Rahmenwerk für die Welt schafft, bleibt abzuwarten. In jedem Fall steht AI noch in den Kinderschuhen und wird immer relevanter werden.

Ebenso bleibt abzuwarten, ob man AI im Kontext von digitaler Souveränität auch aus Österreich und Europa weiterentwickelt und fördert. Oder ob sich diese in anderen Teilen der Welt ansiedeln wird. Der AI Act zum Beispiel hat großes Potential, Bürgerinnen und Bürger zu schützen. Andererseits kann dieser womöglich auch die eine oder andere Innovation in Europa blockieren. In jedem Fall ist die EU ein großer Markt,

welcher eigentlich von keinem Gewerbetreibenden ausgelassen werden will. Aus diesem AI Act kann sich vielleicht ein weltweit anerkanntes Rahmenwerk für den Einsatz von AI-Systemen entwickeln.
Ein weiterer großer Punkt im Kontext von digitaler Souveränität und AI sind die Daten zum Trainieren. Dies wird an der einen oder anderen Stelle sicherlich zu einer Herausforderung werden, innovative AI-Systeme mit den derzeit in europäischen Datenpools vorhandenen Daten, zu trainieren. Die USA haben an dieser Stelle, mit dem dortigen Sitz der Big-Tech-Unternehmen, einen nicht zu verachtenden Vorsprung.

9 Handlungsempfehlungen an Politik und Wirtschaft

Im folgenden Kapitel werden Handlungsempfehlungen an die Politik und Wirtschaft beschrieben, welche die derzeitigen Abhängigkeiten mindern können und dadurch die digitale Souveränität stärken. Dabei wird der Fokus nicht auf einzelne Nationen sondern auf die Europäische Union gelegt. Dies ist dadurch begründet, dass einzelne oder kleine Länder die digitale Souveränität nicht in einem solchen Ausmaß herstellen können werden, wie eine starke und geeinte EU es kann. Dies soll jedoch nicht heißen, dass die im weiteren beschriebenen Themen nicht auch in den Mitgliedstaaten Anwendung finden sollen. Manche dieser Themen müssen sogar auf nationaler Ebene eingebracht werden, um sie anwendbar zu machen.

9.1 Bekenntnis zu Open Source & offenen Standards

Durch ein klares Bekenntnis zu Open Source und offenen Standards wird die digitale Souveränität gestärkt. Das plakative Beispiel mit der Einführung der „Office Open XML“ Formate zeigt deutlich, dass man mit offenen Standards ein Stück mehr digitale Souveränität zurückerlangen kann. Vor der Einführung dieses Standards konnten beispielsweise Microsoft Office Dokumente ausschließlich vom Produkt Microsoft Office verarbeitet werden. Durch die sehr große Verbreitung dieses Produktes war man de facto gezwungen, es selbst ebenfalls einzusetzen um am alltäglichen Austausch teilzunehmen. Dies galt sowohl für Unternehmen – aber auch für die öffentliche Verwaltung und auch für die einzelnen Bürgerinnen und Bürger. Heute ist es mit diesem offenen Standard kein Problem mehr, sich für Alternativprodukte oder gar für Open Source Produkte zu entscheiden. Bürgerinnen und Bürger sind beispielsweise nicht mehr genötigt Microsoft Office Lizenzen zu erwerben, sondern können auf kostenfreie Open Source Alternativen zurückgreifen.

An dieser Stelle gilt es zu erwähnen, dass Open Source nicht pauschal kosten- oder lizenzfrei bedeutet. Auch öffentlich Zugängliches kann kosten- oder lizenzpflichtig sein. Beispielhaft kann man hier Paten-

te nennen, welche man kaufen oder lizenzieren muss wenn man sie verwenden will. Open Source ist auch nicht zwingend immer Software. Es können auch Beispiele wie Vektorgrafiken, Schriftarten, Druckvorlagen oder Baupläne sein. Des Weiteren sind die Bedenken, dass man bei Open Source keine Herstellerunterstützung bekommt oder keine Wartungsverträge abschließbar sind, falsch. Dies ist häufig der Grund, wieso Unternehmen sich für proprietäre Produkte entscheiden.

Open Source und offene Standards können also die digitale Souveränität eines Staates oder der Wirtschaft verbessern. Außerdem können Open Source und offene Standards auch ein Gewinn für die Sicherheit sein. So ist man nicht etwas Geheimen ausgeliefert, was nicht unabhängig überprüfbar ist. Die Handlungsempfehlung an Politik und Wirtschaft lautet daher klar, Open Source und offene Standards zu fördern und zu nutzen. Langfristig ist es dabei nicht zielführend, die vorhandene Open Source Community mit ungeklärten Haftungsfragen – wie derzeit beim Cyber Resilience Act (CRA) (siehe 6.6) – zu schwächen. Des Weiteren sollten Initiativen wie beispielsweise Open Source Open Schools Austria (OSOS) gefördert und ein „Open Source First“ Mindset entwickelt werden.

9.2 Langfristig Denken

Ein weiterer wichtiger Punkt zur Stärkung der digitalen Souveränität ist langfristiges Denken und Handeln. Mit langfristigem Denken ist gemeint, Entscheidungen nicht ausschließlich bis zur nächsten Legislaturperiode oder einer Vertragsverlängerung zu bedenken. Wichtig ist, sich bei Entscheidungen auch die Frage zu stellen, was in zehn oder zwanzig Jahren ist. Natürlich kann man nicht alle Eventualitäten bedenken und vor allem nicht selbst beeinflussen, jedoch sollte man vorbereitet sein – zumindest soweit es möglich ist. Die Preiserhöhungen der Microsoft Cloud vom Jahr 2022 und 2023 erzeugen derzeit Unmut in viele Unternehmen. Entscheidungen, möglicherweise einer Cloud-only Strategie zu folgen, werden derzeit wahrscheinlich von manchen Unternehmen bereut. Allerdings hätte man die Thematik, dass man sich in ein Abhängigkeitsverhältnis begibt, auch bei der damaligen Entscheidung zu einer solchen Strategie schon sehen können. Es ist nicht auszuschließen, dass damals kurzfristiges Denken – beispielsweise wegen Kostenreduzierung – dazu geführt hat, sich für eine solche Strategie zu entscheiden. Natürlich kann es sein, dass die Risiken bei einer vergangenen Entscheidung berücksichtigt wurden und für akzeptierbar gehalten worden sind. Dies ersetzt aber nicht die Erstellung einer Strategie, wie mit schlagend gewordenen, also eingetretenen, Risiken umzugehen ist. Wahrscheinlich gibt es Unternehmen, die für die derzeitigen Preiserhöhungen auch die entsprechenden Exitstrategien haben, das sind aber wahrscheinlich die wenigsten.

Natürlich gibt es auch Entwicklungen, die man auch beim langfristigen Denken nicht erkennen wird. Den Brexit zum Beispiel hätte vor 2016 wohl kaum jemand für möglich gehalten. Dadurch, dass der Brexit unvorhergesehen kam, haben viele Unternehmen Entscheidungen in Bezug auf Großbritannien erneut evaluiert und ggf. neue Risiken identifiziert. Diese Reevaluierung von Entscheidungen sollte jedoch regelmäßig wiederholt werden. Auch im Bezug der Fragestellungen ob man sich abhängig macht und wie es um den Status der – vor allem digitalen – Souveränität bestellt ist.

Durch langfristiges Denken und der Fragestellung von digitaler Souveränität und Abhängigkeiten im Allgemeinen sowie der regelmäßigen Reevaluierung von Entscheidungen kann die digitale Souveränität erhöht werden. Dies gilt sowohl für die Wirtschaft als auch für die Politik.

9.3 Richtlinien zur Beschaffung überdenken

Ein wesentlicher Punkt der Steigerung von digitaler Souveränität steckt auch in der Beschaffung bzw. im Beschaffungsrecht. Und auch im Umgang mit beschafftem. Man stelle sich vor, eine Behörde möchte ein neues Softwareprodukt zur Videotelefonie und Chatnachrichten einführen. So ist es – zumindest in Österreich – an das Bundesvergabegesetz (BVergG) gebunden, welches Schwellwerte und Arten der verschiedenen Vergaben definiert.

Die heutigen Beschaffungsrichtlinien sind jedoch oft auf die Auswahl von Technologien und Dienstleistungen aus wirtschaftlichen Gründen ausgerichtet. Kostenersparnis und Effizienz sind zweifellos wichtige Faktoren, jedoch sollten auch Aspekte der Sicherheit, Kontrolle und Souveränität in Betracht gezogen werden. Zu oft werden Technologien und Dienstleistungen aufgrund ihrer niedrigen Kosten oder etablierten Marktposition ausgewählt, ohne ausreichend die potenziellen Risiken für die digitale Souveränität zu berücksichtigen.

Ebenfalls kann es durch die heutigen Beschaffungsrichtlinien vorkommen, dass alternative Ansätze, Open Source Projekte oder auch Technologien im eigenen nationalen Einfluss, welche womöglich die eigenen Werte am besten verkörpert, ausgeschlossen werden.

Neue Ansätze in der Beschaffung könnten zum Beispiel sein, neue Auswahlkriterien oder anders gestaltete Markterkundungsverfahren zu etablieren. Man könnte die Einbeziehung von Sicherheitsbewertungen und -standards als wesentlichen Bestandteil der Auswahlkriterien festsetzen oder durch Förderung von Forschung und Entwicklung lokaler Technologien und Dienstleistungen Anreize schaffen, dass diese Konkurrenzfähig werden.

Insgesamt ist entscheidend, dass das strategische Ziel von digitaler Souveränität in Beschaffungsrichtlinien eingearbeitet wird, um eine bessere Kontrolle über mögliche Abhängigkeiten, in die man sich begibt, zu haben.

9.4 Investition in Forschung und Entwicklung

Investitionen in Forschung und Entwicklung stellen einen Schlüssel zur Schaffung von digitaler Souveränität dar. Die digitale Transformation hat eine neue Ära der Abhängigkeit von Technologie und Daten eingeläutet in dem Europa im Sinne von Forschung und Entwicklung nicht immer vorne dabei ist. Aus diesem Grund ist Europa in vielen Bereichen abhängig von Technologien, welche in der Regel aus dem amerikanischen und asiatischen Kontinent kommen. Um diese Abhängigkeiten zu minimieren wäre es wichtig, in eine Innovationsführerschaft zu kommen was Europa beispielsweise in anderen Industriezweigen geschafft hat. Um eine solche Vorreiterrolle zu übernehmen, braucht es jedoch Innovation, welche durch Forschung und Entwicklung und mit Investitionen in diese womöglich erreicht werden kann. Neben der Steigerung der digitalen Souveränität unterstützen Investitionen in F&E auch die wirtschaftliche Stärke, welche dadurch auch selbst mehr investieren kann und auf dem Arbeitsmarkt attraktiver wird. Häufig arbeiten Pioniere in Unternehmen, welche es ihnen ermöglichen den Pioniergeist auszuleben und zu fördern. Derzeit sind das bei digitalen Technologien allerdings häufig Unternehmen außerhalb Europas.

9.5 Investition bei der Bildung

Auch die Investition in Bildung ist eine Schlüsselrolle zur Stärkung der digitalen Souveränität. Bildung ist der Schlüssel zur Entwicklung einer technologisch versierten Bevölkerung und zur Förderung von Innovation und kritischem Denken. Eine gut ausgebildete Gesellschaft verfügt über das Wissen und die Fähigkeiten, um eigene Technologien zu entwickeln, zu verwalten und zu sichern. Dies ist entscheidend, um digitale Abhängigkeiten von externen Anbietern zu reduzieren und die Kontrolle über die eigenen digitalen Ressourcen zu behalten. Ebenfalls vermittelt Bildung grundlegende technologische Kompetenzen, welche nötig sind um komplexe Zusammenhänge, Abhängigkeiten oder Risiken zu verstehen. Diese Kompetenzen sind auch notwendig um sich in einer digitalisieren Welt zurecht zu finden und Produkte, Systeme oder Dienstleistungen kritisch zu hinterfragen. Bildung fördert außerdem Innovation und Kreativität, welches beides notwendig ist, um zu forschen und zu entwickeln und dadurch die digitale Souveränität positiv beeinflussen kann.
Investitionen in Bildung sind eine langfristige Strategie zur Stärkung der digitalen Souveränität. Sie tragen dazu bei, eine Bevölkerung zu schaffen, die nicht nur technologisch versiert ist, sondern auch in der Lage

ist, die Herausforderungen und Chancen der digitalen Welt aktiv zu gestalten und zu nutzen.
Im Thema Bildung sollte allerdings die allgemeine Bildung im Vordergrund stehen, und nicht beispielsweise Produktausbildungen an vermeintlich marktüblichen Systemen, wie es derzeit häufig an Bildungseinrichtungen der Fall ist. (vgl. Kap 4.1.4)

9.6 Investition bei der Infrastruktur und Technologieunternehmen

Investitionen in Infrastruktur und Technologieunternehmen bilden das Rückgrat zur Schaffung bzw. Stärkung der digitalen Souveränität. Investitionen in digitale Infrastruktur, wie Breitbandnetze, Rechenzentren und Cloud-Plattformen sind grundlegend, um die Grundlagen für eine starke digitale Souveränität zu legen. Durch den Aufbau eigener Infrastruktur kann ein Land oder eine Ländergemeinschaft die Kontrolle über wichtige Daten und Dienste behalten, anstatt von ausländischen Anbietern abhängig zu sein. Dies reduziert nicht nur potenzielle Sicherheitsrisiken oder Datenschutzbedenken, sondern ermöglicht auch die Schaffung von Arbeitsplätzen und technologischem Fortschritt. Technologieunternehmen sind die treibende Kraft hinter Innovationen und Fortschritten im digitalen Bereich. Investitionen in diese Unternehmen sind nicht nur eine Möglichkeit, von neuen Technologien zu profitieren, sondern auch die digitale Souveränität zu stärken. Durch gezielte Investitionen kann ein Land oder ein Staatenverbund sicherstellen, dass Schlüsseltechnologien und Know-how im eigenen Land bzw. Kontinent vorhanden sind. Dies verhindert, dass strategisch wichtige Technologien in die Hände ausländischer Unternehmen fallen, was die Kontrolle über die eigene digitale Zukunft gefährden könnte. Der Ausbau von Breitbandnetzen kann dabei auch die eigene Bevölkerung unterstützen die digitale Souveränität des eigenen Landes zu stärken. Durch den Ausbau solcher Netze wäre es beispielsweise möglich, dass das Volk auf eigene Technologien setzen bzw. die heimische Wirtschaft unterstützen kann, ohne sich beispielsweise Satelliteninternet mit ausländischen Wurzeln zulegen zu müssen.
Eine gut ausgebaute Infrastruktur ist auch ein Schlüsselaspekt für Technologieunternehmen, welche diese voraussetzen. Ohne diese Voraussetzungen ist es wahrscheinlich für solche Unternehmen nicht möglich sich anzusiedeln bzw. sich entsprechend groß zu entwickeln. Dass Europa in manchen technologischen Bereichen kaum mit innovativen Produkten vertreten ist, zeigt die Sparte der (Cyber-) Sicherheitsprodukte. Ausnahmsweise ist dieser Wirtschaftszweig jedoch nicht durch US-Unternehmen dominiert, sondern wird durch israelische Unternehmen besetzt. Nicht zuletzt, da Israel den Technologiesektor „Cybersecurity“ massiv fördert. Solche Förderungen in Technologieunternehmen und -sektoren könnte ein „Gamechanger“ für die Gewinnung bzw. Stärkung der digitalen Souveränität in Europa werden.

10 Fazit und Ausblick

Der Themenbereich der digitalen Souveränität ist ein sehr junges Feld, welcher erst in Verbindung mit der digitalen Transformation an Bedeutung gewonnen hat. Erst seit Verwaltungsakten oder Prozesse bzw. der menschliche Alltag im Allgemeinen digitalisiert sind, gewinnt das Thema der digitalen Souveränität an Bedeutung. Natürlich gab es vor der Digitalisierung auch technologische Abhängigkeiten, diese hatten jedoch bei weitem nicht die Größe der heutigen und zukünftigen. Beispielsweise Technologien der Telekommunikationsinfrastruktur oder aus dem Bereich Automotive hätten diesen Themenkomplex auch vorantreiben können, kamen jedoch teilweise bzw. hauptsächlich aus Europa, wodurch man sich als Mitgliedsstaat der Europäischen Union in Sicherheit wog. Jetzt, im Zuge der Digitalisierung nahezu aller Anwendungen im täglichen Umfeld, zeigt sich, dass Information Technology (IT) eine Schlüsselrolle hat. Und diese IT kommt häufig aus dem Ausland wodurch man sich als souveräner Staat oder Staatengemeinschaft verwundbar machen kann. Man stelle sich im Zuge der geopolitischen Lage im Jahr 2023 in einem Gedankenspiel vor, die Firma Microsoft und dessen Produkte kämen nicht aus Amerika, sondern aus Russland. Was das für souveräne Staaten weltweit bedeuten würde, bzw. wie dessen Sicherheit gefährdet sein könnte, kann man sich kaum vorstellen. Das Beispiel der russischen Anti-Schadsoftwarefirma „Kaspersky“ zeigt das auf einer deutlich kleineren Ebene. Die Firma, dessen Produkte durchaus genutzt und geschätzt wurden, kam erstmal 2017 in die mediale Berichterstattung, nachdem der damalige US-Präsident Donald Trump verkündet hatte, dass die Softwareprodukte dieser Firma nicht mehr bei US-Behörden genutzt werden dürfen. Als Grund wurde damals die Nähe des Unternehmens zum russischen Staat angegeben. Damals hatte das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) keinen Grund für diesen Vertrauensentzug gesehen. Das Unternehmen selbst startete daraufhin eine Transparenzinitiative, um das vorhandene Misstrauen auszuräumen. Nach dem russischen Angriff auf die Ukraine im Februar 2022 ändert schließlich das BSI nur Wochen später seine Meinung zum Unternehmen Kaspersky und warnte im März 2022 davor, Software von diesem Hersteller zu verwenden. Diese Warnung wurde kontrovers diskutiert, da die Sicherheitsforschenden von Kaspersky einen exzellenten Ruf der Community genossen bzw. diesen noch immer genießen. Allerdings haben Sicherheitsprodukte wie Antivirensysteme auf Betriebssystemen tiefsitzende Rechte und da die

Software aufgrund von regelmäßigen und schnellen Aktualisierungen häufig mit Serversystemen des Unternehmens Daten austauschen muss, wurde die Angst begründet, dass Daten abfließen könnten oder durch die Software selbst Malware oder Backdoors in Systeme implementiert werden können. [88]
Der Firma Kaspersky konnte zwar bis dato nicht nachgewiesen werden, dass die Software das ihr Unterstellte ausführt, allerdings kann man sich ausmalen welche Möglichkeiten der Kompromittierung der digitalen Souveränität bestünden, wenn sie es doch tun würde. Das Repertoire reicht hier von Datenabfluss strategischer wichtiger Informationen, der Manipulation dieser oder bis hin zu der kompletten Stilllegung von ganzen Systemen.
Man stelle sich vor, was das allein beim Beispiel von Kaspersky, wäre es tatsächlich so gewesen, hätte bedeuten können. Kommunikationswege von Regierungen, Streitkräften, Wirtschaftstreibenden und der öffentlichen Verwaltung hätten gestört oder deren Integrität hätte nicht sichergestellt werden können. Welche geopolitischen Folgen ein solcher Vorfall hätte haben können, kann man sich wohl ausschließlich in einem Weltuntergangsszenario vorstellen.

Dass Macht über IT-Systeme bzw. auch über Operational Technology (OT)-Systeme die eigenen oder auch die globalen sicherheitspolitischen Interessen beeinflussen bzw. sicherstellen kann, das zeigt auch der Stuxnet Vorfall, der im Jahr 2010 bekannt wurde. Bei diesem Vorfall wurden gezielt IT-Systeme mit einem Wurm infiziert, um damit OT-Systeme zu manipulieren. Im konkreten Fall von Stuxnet war das Ziel nach heutiger Erkenntnis ein speziell konfiguriertes Supervisory Control and Data Acquisition (SCADA)-System des deutschen Hersteller Siemens, welches es ermöglicht Industrieprozesse zu überwachen und zu steuern. Bei Stuxnet waren die Ziele Frequenzumrichter einzelner Firmen, welche unter anderem die Geschwindigkeiten von Zentrifugen steuern und bei denen man davon ausging, dass diese im Iran zur Urananreicherung genutzt wurden. Nach heutiger Erkenntnis erreichte Stuxnet sein Ziel, indem der Iran bei der Urananreicherung um einige Jahr zurückgeworfen wurde. Bis heute ist nicht abschließend geklärt, welches Land hinter diesem Angriff steckt bzw. es wird vermutet, dass neben den USA und Israel auch Großbritannien und Deutschland unterstützt haben. [89] [90]
Dass ein solcher gezielter Angriff ausschließlich durch staatliche Akteure ausgeführt werden kann, ist in der Security-Community unumstritten. Nur diese haben die nötigen – vor allem finanziellen – Ressourcen so gezielt und über Jahre hinweg, um ein solches Vorgehen zu koordinieren und zu steuern. Dass staatliche Souveränität auch in einer digitalen Form untergraben werden kann, beweist das genannte Beispiel deutlich. Und dass SCADA-Systeme bei industrialisierten Nationen häufig in Verwendung sind, ist ebenfalls allgemein bekannt. Dabei muss man nicht unterscheiden ob mit solchen Systemen Kraftwerke gesteuert

werden oder Industrieprozesse die Wirtschaft am Laufen halten. Man stelle sich vor, was es für Ausmaße haben kann, wenn beispielsweise die in Österreich wichtige Automotive-Industrie über Tage oder vielleicht Wochen nicht produzieren kann. Für die österreichische Wirtschaftsleistung wäre das eine Herausforderung welche sich nach kurzer Zeit auch auf Nachbarländer auswirken würde, da diese ohne die nötigen Zulieferungen ebenfalls den Produktionsprozess – beispielsweise in der Auto-Industrie in Deutschland – drosseln oder gar ganz einstellen müssen.

Nicht zuletzt aufgrund der beiden Beispiele wird die stetig steigende Notwendigkeit digitaler Souveränität deutlich und rückt immer weiter in den Fokus des politischen Diskurses bzw. der Öffentlichkeit. Menschen aller Art, seien es Privatpersonen oder politische Entscheidungsträger, beschäftigen sich immer häufiger mit diesem Thema und hinterfragen beispielsweise Systeme oder Apps. Allerdings stehen wir heute beim Thema der digitalen Souveränität erst am Beginn – sowohl in der Diskussion als auch bei den zu setzenden Maßnahmen.

Nachdem die Wichtigkeit der digitalen Souveränität erst langsam erkannt wird, wird auch die Abhängigkeit, in der sich Österreich und Europa im Allgemeinen befindet, nur langsam deutlich. Das ist auch dem Grund geschuldet, dass es sich bei digitaler Souveränität um ein komplexes Themenfeld handelt welches sich durch sehr viele Bereiche zieht – auch Bereiche die man in einem ersten Gedanken wohl kaum erkennen würde. Auf europäischer Ebene werden zwar schon erste Maßnahmen wie der „Chips Act“ zur Verringerung der Abhängigkeiten in der Halbleiterindustrie (vgl. Kap. 6.10), das Projekt „GAIA-X“ zur Reduzierung der US-Dominanz im Cloud-Sektor (vgl. Kap. 6.3) oder die NIS-Richtlinien zur Stärkung der Resilienz für Betreiber wesentlicher Dienste (z.B. Kraftwerke oder Lebensmittelversorgung, vgl. Kap. 6.5) vorangetrieben, allerdings beschäftigen sich diese Beispiele nur mit den offensichtlichsten Themenfeldern. Nichtsdestotrotz sind die Projekte wichtig und signalisieren das neu gewonnene Verständnis, sich von externen und wenig beeinflussbaren Faktoren unabhängiger bzw. sich resilienter machen zu wollen.

Dass Abhängigkeiten Länder schnell in kritische Zustände bringen können, zeigen auch die Ereignisse rund um die russischen Energielieferungen nach Europa, auf welche man sich im Zuge des russischen Angriffs auf die Ukraine im Winter 2022/2023 nicht mehr vollumfänglich verlassen konnte. Diese Abhängigkeit ist zwar keine Abhängigkeit im Sinne der digitalen Souveränität, allerdings hätte auch diese einen Einfluss auf die digitalisieren Prozesse unserer Zeit haben können, falls es beispielsweise einen Stromnotstand gegeben hätte und digitalisierte Systeme nicht mehr verfügbar gewesen wären. Auch am Beispiel dieser Energielieferungen ist die Tragweite und die Komplexität von Souveränität und auch digitaler Souveränität deutlich zu erkennen.

Digitale Souveränität bedeutet aber nicht zwingend alle Abhängigkeiten aufzulösen, alle Dienste selbst zu betreiben oder gar Autarkie herzustellen. Man kann digitale Souveränität auch herstellen, indem man gezielt Unterstützung von Verbündeten nutzt. Ein weiteres Beispiel aus der überfallenen Ukraine macht das deutlich: Um den Betrieb der .ua-Country Code Top-Level Domain (ccTLD) – und vor allem die gov.ua-Zone – zu gewährleisten, »evakuierten« sie einige System in die public Cloud außerhalb des eigenen Territoriums. [91] Auch in der ukrainischen öffentlichen Verwaltung änderte der beginnende Krieg die Prioritäten der digitalen Souveränität. Bis kurz vor Kriegsbeginn gab es in der Ukraine ein Datenschutz- bzw. Datensicherheitsgesetz, welches die Nutzung von public Cloud-Diensten untersagte. Das bedeutete, dass Dienste in Rechenzentren innerhalb des eigenen Territoriums betrieben werden mussten. Nur sieben Tage vor Kriegsbeginn änderte das ukrainische Parlament diese Gesetze, um eine Evakuierung von Daten und Diensten zu Cloud-Services zu ermöglichen. Dass diese Strategie sehr sinnvoll war, stellte sich schnell heraus, da einige Bomben Rechenzentren der öffentlichen Verwaltung trafen. [92] Dieses Beispiel zeigt deutlich, dass digitale Souveränität nicht ausschließlich bedeutet Abhängigkeiten zu anderen zu vermeiden, sondern diese fallweise auch die digitale Souveränität stützen können. Nichtsdestotrotz wird die Ukraine nach Kriegsende – vermutlich – versuchen die eigene digitale Souveränität – unabhängig von Drittstaaten – wiederherzustellen. Vor allem wegen zwei relevanten US-Gesetzen: dem US Foreign Intelligence Surveillance Act (FISA) und dem US Clarifying Lawful Overseas Use of Data Act (CLOUD-Act). FISA regelt unter anderem die Überwachung in der Auslandsaufklärung und der CLOUD-Act ermöglicht es für US-Behörden auch dann auf Daten von US-IT-Dienstleistern zuzugreifen, wenn diese nicht physisch auf US-Territorium gespeichert werden. Diese Rechtsgrundlagen in Verbindung mit den Enthüllungen von Edward Snowden bzgl. der globalen digitalen Überwachung durch die US National Security Agency (NSA), macht es für souveräne Staaten eigentlich unmöglich digitale US-Dienste zu nutzen, da sowohl die Vertraulichkeit als auch die Integrität der zu verarbeitenden Daten kaum zu gewährleisten sind.

Wie man sicherlich erkennen kann, ist digitale Souveränität kein Konzept, das man anwendet, um dieses Thema zu erledigen. Es ist mehr ein Prozess, den jeder souveräne Staat zu durchlaufen hat, um die eigenen lokalen Bedürfnisse in den Kontext der digitalen Souveränität zu stellen. Natürlich sind die europäischen Bedürfnisse häufig sehr ähnlich zueinander, was es für den Staatenbund einfacher macht sich gemeinsam diesem Thema zu widmen. Und natürlich wird Europa und auch Österreich die bestehenden Abhängigkeiten in einer globalisierten Welt kurz- und mittelfristig nicht auflösen können. Aber genauso selbstverständlich wird sich die Welt diesem Thema mehr und mehr stellen müssen. Die Initiativen einzelner europäischer Mitgliedstaaten bzw. der Europäischen Union sind die ersten Schritte innerhalb des Prozesses der digitalen

Souveränität. Es werden aber auch nicht die letzten sein die es umzusetzen gilt. Digitale Souveränität wird in Zukunft ein Querschnittsthema sein, welches in allen Bereichen mitgedacht werden muss – und das nicht nur auf einer technischen Ebene. Unabhängig davon, ob man in Zukunft das Bildungswesen modernisiert, Richtlinien zu Beschaffung aktualisiert, Budget für Forschung und Entwicklung bereitstellt oder aber tatsächlich technische Systeme einführt: digitale Souveränität wird thematisch immer mitbehandelt werden müssen.

Abschließend kann man zusammenfassen, dass wir Abhängigkeiten wohl nie vollständig auflösen werden können. Wir werden aber zukünftig ein entsprechendes Risikobewusstsein haben um diese Abhängigkeiten – auch im Kontext der digitalen Souveränität – besser bewerten zu können. Dadurch ergibt sich auch die Möglichkeit die Resilienz digitaler Systeme besser in Business Continuity Management (BCM)-Prozessen mit (besseren) Notfallplänen abbilden zu können. Nur wer die Abhängigkeiten innerhalb der digitalen Souveränität kennt, kann sich auf entsprechende (worst case) Szenarien vorbereiten und damit die eigene (digitale) Souveränität schützen.

Abbildungsverzeichnis

Akronyme

AI	Artificial Intelligence
ALA	American Library Association
API	Application Programming Interface
BCM	Business Continuity Management
BMBWF	Bundesministerium für Bildung, Wissenschaft und Forschung
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
bzw.	beziehungsweise
C I A	Confidentiality, Integrity, Availability
ccTLD	Country Code Top-Level Domain
CLOUD-Act	US Clarifying Lawful Overseas Use of Data Act
CLOUD-Act	Clarifying Lawful Overseas Use of Data Act
CRA	Cyber Resilience Act
DNS	Domain Name Service
DSGVO	Datenschutzgrundverordnung
ENISA	European Network and Information Security Agency
ERP	Enterprise Resource Planning
EU	Europäischen Union
EWR	Europäischer Wirtschaftsraum

FISA	US Foreign Intelligence Surveillance Act
FOKUS	Fraunhofer-Institut für Offene Kommunikationssysteme
ggf.	gegebenenfalls
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IDR	Identitätsdokumentenregister
IT	Information Technology
NGO	Non-Governmental Organisation
NIS	Network and Information Systems
NSA	US National Security Agency
OSOS	Open Source Open Schools Austria
OSS	Open Source Software
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
OT	Operational Technology
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
UN	United Nations
USA	United States of America
W3C	World Wide Web Consortium
WKStA	Wirtschafts- und Korruptionsstaatsanwaltschaft

ZMR Zentrales Melderegister

Literatur

[1] Cambridge Dictionary, *Meaning of digital in English*. Adresse: https://dictionary.cambridge.org/dictionary/english/digital (besucht am 16. 07. 2023).

[2] Roland Heuermann, Andreas Engel, Jörn Von Lucke, Roland Heuermann, Roland Heuermann, Roland Heuermann, Roland Heuermann, Roland Heuermann, Andreas Engel, Jörn von Lucke u. a., „Digitalisierung: Begriff, Ziele und Steuerung“, in *Digitalisierung in Bund, Ländern und Gemeinden: IT-Organisation, Management und Empfehlungen*, Springer, 2017, S. 9–50.

[3] Friedrich Balke, „Figuren der Souveränität“, in *Figuren der Souveränität*, Brill Fink, 2019.

[4] Der Duden, *Wörterbuch: souverän*. Adresse: https://www.duden.de/node/169140/revision/1237263 (besucht am 16. 07. 2023).

[5] Julia Pohle, „Digitale Souveränität“, in *Handbuch Digitalisierung in Staat und Verwaltung*, Tanja Klenk, Frank Nullmeier und Göttrik Wewer, Hrsg. Wiesbaden: Springer Fachmedien Wiesbaden, 2020, S. 1–13, ISBN: 978-3-658-23669-4. DOI: 10.1007/978-3-658-23669-4_21-1. Adresse: https://doi.org/10.1007/978-3-658-23669-4_21-1.

[6] Der Duden, *Wörterbuch: Resilienz*. Adresse: https://www.duden.de/node/121204/revision/1274751 (besucht am 16. 07. 2023).

[7] Benjamin Scharte und Klaus Thoma, „Resilienz–Ingenieurwissenschaftliche Perspektive“, *Multidisziplinäre Perspektiven der Resilienzforschung*, S. 123–150, 2016.

[8] Dr. Mareike Seifried; Prof. Dr. Irene Bertschek, „Schwerpunktstudie Digitale Souveränität, Bestandsaufnahme und Handlungsfelder“, Bundesministerium für Wirtschaft und Energie (BMWi), 2021. Adresse: https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.html (besucht am 26. 01. 2023).

[9] Gabriele Goldacker, „Digitale Souveränität“, Kompetenzzentrum Öffentliche IT / Fraunhofer FOKUS, 2017. DOI: 10.24406/publica-fhg-298824. Adresse: https://publica.fraunhofer.de/handle/publica/298824 (besucht am 26. 01. 2023).

[10] Volker Wittpahl, *Digitale Souveränität: Bürger | Unternehmen | Staat*. Springer Nature, 2018.

[11] Julia Pohle, Leo Thüer, Finn Dammann und Jan Winkler, „Das Subjekt im politischen Diskurs zu digitaler Souveränität“, in *Handbuch Digitalisierung und politische Beteiligung*, Norbert Kersting, Jörg Radtke und Sigrid Baringhorst, Hrsg. Wiesbaden: Springer Fachmedien Wiesbaden, 2020, S. 1–23, ISBN: 978-3-658-31480-4. DOI: 10.1007/978-3-658-31480-4_12-1. Adresse: https://doi.org/10.1007/978-3-658-31480-4_12-1.

[12] Resa Mohabbat Kar und Basanta E.P. Thapa, „Digitale Souveränität als strategische Autonomie, Umgang mit Abhängigkeiten im digitalen Staat“, Kompetenzzentrum Öffentliche IT / Fraunhofer FOKUS, 2020. DOI: 10.24406/publica-fhg-300498. Adresse: https://publica.fraunhofer.de/handle/publica/300498 (besucht am 10. 02. 2023).

[13] Stephan Kreutzer und Manuel Molina Vogelsang, „Wie Europa seine digitale Souveränität wiederherstellen kann“, Fraunhofer-Zentrum für Internationales Management und Wissensökonomie IMW, 2022. DOI: 10.24406/publica-85. Adresse: https://publica.fraunhofer.de/handle/publica/418023 (besucht am 18. 02. 2023).

[14] Dajan Baischew, Peter Kroon, Stefano Lucidi, Christian Märkel und Bernd Sörries, „Digital sovereignty in Europe: A first benchmark“, WIK-Consult Report, 2020. Adresse: http://hdl.handle.net/10419/251539 (besucht am 18. 02. 2023).

[15] Luciano Floridi, „The fight for digital sovereignty: What it is, and why it matters, especially for the EU“, *Philosophy & technology*, Jg. 33, S. 369–378, 2020.

[16] „Chinesen wollen nur 49 Prozent von Kuka“, *Spiegel Online*, Adresse: https://www.spiegel.de/wirtschaft/unternehmen/kuka-chinesischen-wollen-nur-49-prozent-von-roboterfirma-a-1097487.html (besucht am 08. 06. 2023).

[17] Dana Heide, „Experten warnen vor drohender Abhängigkeit von China bei Halbleitern“, *Handelsblatt Online*, Adresse: https://www.handelsblatt.com/technik/forschung-innovation/chipbranche-experten-warnen-vor-drohender-abhaengigkeit-von-china-bei-halbleitern/27869926.html (besucht am 08. 06. 2023).

[18] Europäische Kommission, *Europäisches Chip-Gesetz*. Adresse: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_de (besucht am 07. 06. 2023).

[19] Statista, *Anzahl der erteilten 5G-Patente der führenden Unternehmen weltweit im Jahr 2020*, 2023. Adresse: https://de.statista.com/statistik/daten/studie/967168/umfrage/anzahl-der-5g-patente-der-fuehrenden-unternehmen-weltweit/ (besucht am 09. 06. 2023).

[20] empower GmbH, *Die grosse Office-Software Studie*, 2020. Adresse: https://www.empowersuite.com/de/wissen/office-studie-deutschland (besucht am 09. 06. 2023).

[21] Statista, *Meistgenutzte Office-Software von Büromitarbeitern in Unternehmen in Deutschland im Jahr 2020*, 2023. Adresse: https://de.statista.com/statistik/daten/studie/77226/umfrage/internetnutzer-verbreitung-von-office-software-in-deutschland/ (besucht am 09. 06. 2023).

[22] Peter Zellinger, „Politische Schockstarre in Österreich vor möglichem Tiktok-Verbot“, *Der Standard Online*, Adresse: https://www.derstandard.at/story/2000144312960 (besucht am 24. 03. 2023).

[23] „TikTok-Verbot auf Diensthandys“, *Tagesschau Online*, Adresse: https://www.tagesschau.de/ausland/eu-kommission-tiktok-101.html (besucht am 24. 03. 2023).

[24] Monika Ermert, „Störerhaftung für DNS-Resolver: Quad9 verliert vor Landgericht gegen Sony“, *Heise Online*, Adresse: https://heise.de/-6280566 (besucht am 09. 06. 2023).

[25] „Putin schafft sich ein “souveränes“ Internet“, *Deutsche Welle Online*, Adresse: https://www.dw.com/de/russlands-pr%C3%A4sident-putin-schafft-sich-ein-souver%C3%A4nes-internet/a-51080505 (besucht am 09. 06. 2023).

[26] Philipp Bovermann, „Hinterm Eisernen Software-Vorhang“, *Süddeutsche Zeitung Online*, Adresse: https://sz.de/1.5553286 (besucht am 09. 06. 2023).

[27] Monika Ermert, „Analyse: USA gibt ihre Wächterrolle im DNS ab“, *Heise Online*, Adresse: https://heise.de/-3339640 (besucht am 09. 06. 2023).

[28] „Aus für Studi-VZ: Ihre Erinnerungen an die Plattform“, *Der Standard Online*, Adresse: https://www.derstandard.at/story/2000134717435 (besucht am 09. 06. 2023).

[29] Claudia Frickel, „Wie Facebook die Welt eroberte“, *Focus Online*, Adresse: https://www.focus.de/digital/internet/facebook/wie-facebook-die-welt-eroberte-von-den-anfaengen-bis-zum-boersengang_id_2416737.html (besucht am 09. 06. 2023).

[30] Saferinternet.at, *Jugend-Internet-Monitor*, 2023. Adresse: https://www.saferinternet.at/services/jugend-internet-monitor (besucht am 09. 06. 2023).

[31] Statista, *Leading social media platforms in Russia in 3rd quarter 2022, by monthly penetration rate*, 2022. Adresse: https://www.statista.com/statistics/867549/top-active-social-media-platforms-in-russia/ (besucht am 09. 04. 2023).

[32] Monika Ermert, „Es ist was faul im E-Mail-Land: Zwischen Komplexität und ungleichen Machtverhältnissen“, *Heise Online*, Adresse: https://heise.de/-4259518 (besucht am 23. 07. 2023).

[33] Merlin Schumacher, „Atlassian stellt Verkauf von Serverlizenzen ein. Die Zukunft gehört der Cloud.“, *Heise Online*, Adresse: https://heise.de/-4931264 (besucht am 23. 07. 2023).

[34] Thomas Cik, Georg Renner, Maximilian Miller und Jonas Binder, „Das Handy des Thomas S.“, *Kleine Zeitung Online*, Adresse: https://interaktiv.kleinezeitung.at/handy-thomas-schmid/ (besucht am 23. 07. 2023).

[35] Statista, *Beliebteste Messenger in Österreich im Jahr 2023*, 2023. Adresse: https://de.statista.com/prognosen/1000264/oesterreich-beliebteste-messenger (besucht am 29. 07. 2023).

[36] „TU Wien macht sich lächerlich mit ihrer Entscheidung für Microsoft“, *epicenter.works*, Adresse: https://epicenter.works/content/tu-wien-macht-sich-laecherlich-mit-ihrer-entscheidung-fuer-microsoft (besucht am 09. 04. 2023).

[37] Statista, *Marktanteile der führenden Betriebssysteme in Deutschland von Januar 2009 bis Januar 2023*, 2023. Adresse: https://de.statista.com/statistik/daten/studie/158102/umfrage/marktanteile-von-betriebssystemen-in-deutschland-seit-2009/ (besucht am 09. 04. 2023).

[38] Open Source Open Schools Österreich, *Microsoft Ausfall - nichts geht mehr*. Adresse: https://linux-bildung.at/2023/01/microsoft-ausfall-nichts-geht-mehr/ (besucht am 11. 06. 2023).

[39] Rene Schwarzinger, Thomas Gatterer und Thomas Kruppa, „Datenschutz an Österreichs Schulen: Freie Open Source Software: Ein Beitrag von Open Source Open Schools Austria (Rene Schwarzinger, Thomas Krupa, Thomas Gatterer)“, *Medienimpulse*, Jg. 61, Nr. 1, 12–Seiten, 2023.

[40] Reinhold Karner, *Europe's failure to deal with failure*. Adresse: https://www.rmk.org/de/blog/europes-failure-deal-failure (besucht am 11. 06. 2023).

[41] Michael Kröger, „Mangelware Masken“, *Spiegel Online*, Adresse: https://www.spiegel.de/wirtschaft/mangelware-masken-a-a4540a5f-9db2-45ac-99ac-ed859ba3e062 (besucht am 29. 07. 2023).

[42] Mischa Ehrhardt, „Der blockierte Suezkanal und die Weltwirtschaft“, *Deutsche Welle Online*, Adresse: https://www.dw.com/de/der-blockierte-suezkanal-und-die-weltwirtschaft/a-56989523 (besucht am 29. 07. 2023).

[43] Benedikt Nabben und Sabina Wolf, „Deutschlands Abhängigkeit von den USA“, *Bayerischer Rundfunk Online*, Adresse: https://www.br.de/fernsehen/das-erste/sendungen/report-muenchen/europa-abhaengigkeit-usa-100.html (besucht am 29. 07. 2023).

[44] Open Source Open Schools Österreich, *OSOS Austria*. Adresse: https://linux-bildung.at/osos-austria/ (besucht am 11. 06. 2023).

[45] Microsoft News Center, *Mit Suchen die Wüste aufforsten – Ökologisch inspirierte Webseite Ecosia setzt auf Bing*, 2016. Adresse: https://news.microsoft.com/de-de/oekologisch-webseite-ecosia-bing/ (besucht am 29. 07. 2023).

[46] Statista, *Marktanteile der Suchmaschinen weltweit nach mobiler und stationärer Nutzung im Juni 2023*, 2023. Adresse: https://de.statista.com/statistik/daten/studie/222849/umfrage/marktanteile-der-suchmaschinen-weltweit/ (besucht am 29. 07. 2023).

[47] Till Janzer, „Internetsuchmaschinen: Google in Tschechien erstmals vor Seznam“, *Radio Prague International Online*, Adresse: https://deutsch.radio.cz/internetsuchmaschinen-google-tschechien-erstmals-vor-seznam-8379544 (besucht am 29. 07. 2023).

[48] Jörn Brien, „Seznam: Tschechische Suchmaschine verklagt Google auf 345 Millionen Euro“, *t3n Online*, Adresse: https://t3n.de/news/suche-seznam-verklagt-google-1344600/ (besucht am 29. 07. 2023).

[49] American Library Association (ALA), *Digital Literacy*. Adresse: https://literacy.ala.org/digital-literacy/ (besucht am 07. 06. 2023).

[50] Pressemitteilung Europäisches Parlament, *Ungarn: Zerfall der Demokratie, der Rechtsstaatlichkeit und der Grundrechte*. Adresse: https://www.europarl.europa.eu/news/de/press-room/20220909IPR40137/ (besucht am 07. 06. 2023).

[51] Unilog Integrata Unternehmenberatung GmbH, *Clientstudie der Landeshauptstadt München*, 2003. Adresse: https://web.archive.org/web/20120724021042/http://osalliance.com/portfolio/migration/clientstudie_kurz.pdf (besucht am 09. 04. 2023).

[52] Ulrich Bantle, „Stadt München setzt auf Open-Source-Lösungen“, *Linux Magazin Online*, Adresse: https://www.linux-magazin.de/news/stadt-muenchen-setzt-auf-open-source-loesungen/ (besucht am 09. 06. 2023).

[53] Airbus SAS, *Commercial Aircraft History, Early days (1967)*. Adresse: https://www.airbus.com/en/who-we-are/our-history/commercial-aircraft-history/early-days-1967 (besucht am 30. 07. 2023).

[54] Airbus SAS, *Commercial Aircraft History*. Adresse: https://www.airbus.com/en/who-we-are/our-history/commercial-aircraft-history (besucht am 30. 07. 2023).

[55] Jonas Volkert, „EU-Cloud: Gaia-X “lediglich ein weiteres Bürokratiemonster““, *Heise Online*, Adresse: https://heise.de/-6273961 (besucht am 11. 06. 2023).

[56] „Europäisches Datenprojekt Gaia-X nimmt Fahrt auf“, *Austria Presse Agentur*, Adresse: https://science.apa.at/power-search/14475582107082791308 (besucht am 11. 06. 2023).

[57] Europäische Kommission, *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union*. Adresse: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32016L1148 (besucht am 30. 07. 2023).

[58] Europäische Kommission, *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)*. Adresse: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555 (besucht am 30. 07. 2023).

[59] Rechtsinformationssystem des Bundes (RIS) Republik Österreich, *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*. Adresse: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536 (besucht am 30. 07. 2023).

[60] Think Tank | European Parliament, *EU cyber-resilience act*. Adresse: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739259 (besucht am 13. 06. 2023).

[61] Stefan Krempl, „Cyber Resilience Act: "Cybersicherheit geht die ganze Gesellschaft an"", *Heise Online*, Adresse: https://heise.de/-7265080 (besucht am 13. 06. 2023).

[62] Jan Mahn, „Cyber Resilience Act CRA: EU-Gesetzentwurf gefährdet Open Source", *Heise Online*, Adresse: https://heise.de/-8983416 (besucht am 13. 06. 2023).

[63] Matrix.org Foundation, *Mainpage*. Adresse: https://matrix.org/ (besucht am 07. 06. 2023).

[64] Matrix.org Foundation, *Matrix and Riot confirmed as the basis for France's Secure Instant Messenger app*. Adresse: https://matrix.org/blog/2018/04/26/matrix-and-riot-confirmed-as-the-basis-for-frances-secure-instant-messenger-app (besucht am 07. 06. 2023).

[65] Hauke Gierow, „Frankreichs Whatsapp-Alternative setzt auf Matrix und Riot", *golem.de*, Adresse: https://glm.io/134115 (besucht am 11. 06. 2023).

[66] BWI GmbH, *Open-Source: "Matrix" ist einheitlicher Messenger-Standard für die Bundeswehr*. Adresse: https://www.bwi.de/magazin/artikel/open-source-matrix-ist-einheitlicher-messenger-standard-fuer-die-bundeswehr (besucht am 07. 06. 2023).

[67] Moritz Tremmel, „Wie der Bwmessenger Behörden verändern soll", *golem.de*, Adresse: https://glm.io/169472 (besucht am 11. 06. 2023).

[68] „Tweetdeck ab sofort nur noch für zahlende X-Nutzer", *Kronen Zeitung Online*, Adresse: https://www.krone.at/3088084 (besucht am 18. 08. 2023).

[69] Andreas Proschofsky, „Twitter-Chaos beschert Mastodon Explosion der Nutzerzahlen", *Der Standard Online*, Adresse: https://www.derstandard.at/story/2000140635465 (besucht am 12. 06. 2023).

[70] „Twitter-Alternative: DER STANDARD ist jetzt auch auf Mastodon", *Der Standard Online*, Adresse: https://www.derstandard.at/story/2000141364458 (besucht am 12. 06. 2023).

[71] „Kelber: Bund soll eigene Social-Media-Instanz betreiben", *Süddeutsche Zeitung Online*, Adresse: https://sz.de/dpa.urn-newsml-dpa-com-20090101-230315-99-963424 (besucht am 12. 06. 2023).

[72] „“EU Voice“ und “EU Video“: Die EU testet eigene Alternativen zu Youtube und Twitter“, *Der Standard Online*, Adresse: https://www.derstandard.at/story/2000135329259 (besucht am 09. 06. 2023).

[73] Bärbel Deisting und Günter W Hein, „GALILEO–ein europäisches Projekt von internationaler Bedeutung“, *ZfV-Zeitschrift für Geodäsie, Geoinformation und Landmanagement*, Nr. zfv 5/2006, 2006.

[74] Peter-Michael Ziegler, „EU-Parlament segnet militärische Nutzung von Galileo ab“, *Heise Online*, Adresse: https://heise.de/-185619 (besucht am 08. 07. 2023).

[75] Günther Strobl, „Mikrochips statt Kartoffelchips: In Österreich beginnt das Ringen um Geld“, *Der Standard Online*, Adresse: https://www.derstandard.at/story/3000000178716 (besucht am 05. 08. 2023).

[76] Mark Mantel, „Grundlage für Intels Magdeburg-Werke geschaffen: EU Chips Act verabschiedet“, *Heise Online*, Adresse: https://heise.de/-9213258 (besucht am 05. 08. 2023).

[77] Stephan Finsterbusch, „Intel baut neue Chipfabrik in Polen“, *Frankfurter Allgemeine Zeitung Online*, Adresse: https://www.faz.net/-gqi-bajtd (besucht am 05. 08. 2023).

[78] Ralf T Kreutzer, Marie Sirrenberg u. a., *Künstliche Intelligenz verstehen*. Springer, 2019.

[79] Alan M Turing, *Computing machinery and intelligence*. Springer, 2009.

[80] Sonja Cechak, „Schwache KI, Starke KI & Superintelligenz“, *AIHubYou, Universität für Weiterbildung Krems*, Adresse: https://imbstudent.donau-uni.ac.at/aihubyou/ai-grundlagen/schwache-ki-starke-ki-superintelligenz/ (besucht am 30. 06. 2023).

[81] „Jedes 2. Unternehmen verzichtet aus Datenschutzgründen auf Innovationen“, *Bitkom e. V., Presseaussendung*, Adresse: https://www.bitkom.org/Presse/Presseinformation/Jedes-2-Unternehmen-verzichtet-aus-Datenschutzgruenden-auf-Innovationen (besucht am 30. 06. 2023).

[82] Oliver Schonschek, „Verhindert der Datenschutz eine erfolgreiche KI?“, *Security Insider Online*, Adresse: https://www.security-insider.de/verhindert-der-datenschutz-eine-erfolgreiche-ki-a-b34a0ec681ee1ffb7dc6d3f60078687a/ (besucht am 30. 06. 2023).

[83] DeepL SE, *The world's most accurate and nuanced machine translation*. Adresse: https://www.deepl.com/en/whydeepl (besucht am 30. 06. 2023).

[84] Eva-Maria Weiss, „Diebischer ChatGPT: Klage gegen OpenAI und Microsoft“, *Heise Online*, Adresse: https://heise.de/-9202510 (besucht am 01. 07. 2023).

[85] Europäische Kommission, *Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION*. Adresse: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52021PC0206 (besucht am 01. 07. 2023).

[86] Lucilla Sioli, „A European Strategy for Artificial Intelligence“, *CEPS webinar-European approach to the regulation of artificial intelligence*, Jg. 23, 2021.

[87] Stefan Mey, „AI Act der EU als Gefahr für freie KI-Software in Europa“, *Der Standard Online*, Adresse: https://www.derstandard.de/story/3000000174724 (besucht am 03. 07. 2023).

[88] Eva Wolfangel, „Vertrauen ist gut, aber Kontrolle hilft auch nicht immer“, *Die Zeit Online*, Adresse: https://www.zeit.de/digital/datenschutz/2023-07/kaspersky-antivirensoftware-russland-sicherheitsfirma-datenschutz/ (besucht am 20. 08. 2023).

[89] Frank Rieger, „Der digitale Erstschlag ist erfolgt“, *Frankfurter Allgemeine Zeitung Online*, Adresse: https://www.faz.net/-gsi-xua1 (besucht am 20. 08. 2023).

[90] Yossi Melman, „Israel Finally Moving to Define National Policy on Iran“, *Haaretz Online*, Adresse: https://www.haaretz.com/2011-03-10/ty-article/israel-finally-moving-to-define-national-policy-on-iran/0000017f-e2d7-d38f-a57f-e6d7fdb80000 (besucht am 20. 08. 2023).

[91] Monika Ermert, „Wie die ukrainische Top Level Domain .ua in Zeiten des Kriegs funktioniert“, *Heise Online*, Adresse: https://heise.de/-6611226 (besucht am 24. 03. 2023).

[92] Brad Smith, „Defending Ukraine: Early Lessons from the Cyber War“, Microsoft. Adresse: https://aka.ms/June22SpecialReport (besucht am 24. 03. 2023).