LIONS

Funded by
dtec.bw

Funded by
the European Union
NextGenerationEU

Digitale Souveränität

Handlungsempfehlungen

Manfred Hofmeier – Martha Klare – Isabelle Fries – Kai Weeber

Universität der Bundeswehr München

LIONS – Ledger Innovation and Operation Network for Sovereingty

Das interdisziplinär ausgerichtete Forschungsprojekt LIONS baut eine Forschungsplattform für die Erforschung von Distributed-Ledger-Technologie (DLT) als eine Technologie der Digitalisierung zur Erhöhung von Resilienz und Digitaler Souveränität auf.

LIONS baut technische und analytische Kompetenzen auf, stellt eine Laborumgebung mit Infrastruktur für DLT realistischer Größe bereit und baut eine Community aus Bundeswehr, Behörden und Privatwirtschaft auf. Es werden Indikatoren und Instrumente für Analyse, Design und Implementierung von DLT-basierten Informationssystemen und ihrem Beitrag zu Resilienz und digitaler Souveränität entwickelt und dabei drei Analyseperspektiven berücksichtigt: (1) Individuum, (2) Supply Chain und (3) Gesellschaft.

LIONS wird gefördert durch dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.

➔ https://dtecbw.de

Digitale Souveränität - Handlungsempfehlungen

Manfred Hofmeier[1], Martha Klare[2], Isabelle Fries[3], Kai Weeber[4]

[1]Universität der Bundeswehr München, Fakultät für Informatik
[2]BWI GmbH, Center of Excellence Consulting
[3]Universität der Bundeswehr München, Fakultät für Staats- und Sozialwissenschaften
[4]Universität der Bundeswehr München, Fakultät für Humanwissenschaften

Neubiberg 2024

Institut für Schutz und Zuverlässigkeit
Fakultät für Informatik
Universität der Bundeswehr München

Werner-Heisenberg-Weg 39
85577 Neubiberg

1 Hintergrund und Ziel

Das interdisziplinäre Forschungsprojekt LIONS hat als zentrales Ziel, die Digitale Souveränität auf den Ebenen Staat, Organisation und Individuum zu verbessern. Nachdem sich das Projektkonsortium aus den Perspektiven verschiedener Fachdisziplinen lange Zeit intensiv mit Digitaler Souveränität beschäftigt hat, wurden am 14. Mai 2024 in einem Workshop die aus Sicht des Projektkonsortiums wichtigsten Handlungsempfehlungen für Entscheider und Entscheiderinnen zusammengetragen. Die Ergebnisse wurden für die hier vorliegenden Handlungsempfehlungen analysiert und aufbereitet. Der diskursive Entstehungsprozess prägt die multiperspektivische Qualität der konkreten Empfehlungen. Sie verbinden fachliche Expertise, Erfahrung und Praxisbezogenheit. Im Ergebnis können sie Digitale Souveränität auf den genannten drei Ebenen (Staat, Organisation und Individuum) stärken.

Eine konkrete Empfehlung kann sich dabei ambivalent zeigen. Zumindest potenziell kann sie auch Nachteile bzw. Nebeneffekte beinhalten, die je nach Fall von den jeweiligen Entscheidern und Entscheiderinnen abgewogen werden müssen. Gleichzeitig sind aber auch Synergieeffekte der Maßnahmen für andere Bereiche sichtbar, beispielsweise für Bürokratie, Digitalisierung oder Bildung.

In den nachfolgenden Abschnitten werden die Handlungsempfehlungen zugunsten Digitaler Souveränität vorgestellt. Das Dokument ist unterteilt in eine kurze Erläuterung des zugrunde liegenden Verständnisses von Digitaler Souveränität (siehe Kapitel 2), Empfehlungen für Organisationen (siehe Kapitel 3) und Empfehlungen für politische Entscheider und Entscheiderinnen (siehe Kapitel 4).

2 Digitale Souveränität – was wir damit meinen

Angela Merkel verwendete 2021 den Begriff der Digitalen Souveränität, um auf die Schwächen Europas in Bezug auf Innovation, technologische Fähigkeit und Beschaffung von Software und Hardware aufmerksam zu machen. Es finde „Innovation in erheblichem Umfang außerhalb Europas statt", heißt es im Schreiben von Angela Merkel an die EU-Kommissionschefin[1]. Damit begleitet der Souveränitätsbegriff ein politisch wahrgenommenes Defizit hinsichtlich wirtschaftlicher Konkurrenzfähigkeit einerseits und einen Wunsch nach technologischer Unabhängigkeit andererseits. Digitale Souveränität wird zum erstrebten Zielzustand, um Missstände beispielsweise im Blick auf die IT-Supply-Chain zu reduzieren. Im Koalitionsvertrag der Ampel-Regierung wird am Ziel der Erhöhung Digitaler Souveränität festgehalten, ebenso wie am Hinweis, dass Digitale Souveränität maßgeblich von europäischen Rahmenbedingungen abhinge[2].

Wir lehnen uns an dieses Verständnis an, wenn wir über Digitale Souveränität sprechen. Noch weiter gefasst verstehen wir unter Digitaler Souveränität allerdings ein selbstbestimmtes Handeln im digitalen Raum. Das beinhaltet, dass mit Digitaler Souveränität beispielsweise die Reduzierung von Abhängigkeiten bei der Beschaffung von Hardware aus Asien oder Software aus den Vereinigten Staaten einhergeht. Auf wissenschaftlicher Ebene schließt sich aber auch die Erforschung der Frage an, in welche zukunftsfähigen Innovationsbereiche Europa investieren sollte. Selbstbestimmtes Handeln zielt wiederum auch auf Befähigung und damit den Bereich der Bildung, sei es im schulischen Kontext oder einer Mitarbeitenden-Qualifizierung im Unternehmenskontext. Wir gehen davon aus, dass der gezielte Einsatz von Schlüsseltechnologien wie Blockchain oder Künstlicher Intelligenz auf Basis europäischer Werte zu den verschiedenen Dimensionen Digitaler Souveränität beitragen kann. In den genannten emergenten Technologien sehen wir allerdings keine Selbstläufer, die ein gewünschtes Ergebnis garantieren könnten. Deshalb setzen wir zugleich auf begleitende Handlungsempfehlungen, um Individuen, Organisationen und Staat im Blick auf eine souveräne Technologieentwicklung und einen souveränen Technologiegebrauch, aber auch allgemein im Blick auf souveränes Handelns im digitalen Raum zu befähigen.

Im Forschungsprojekt LIONS wurde ein Modell entwickelt, das Digitale Souveränität im Dreiklang Staat bzw. supranationale Institution, Organisation und Individuum betrachtet, und dabei auch die wechselseitigen Einflüsse berücksichtigt[3]. Die hier vorgelegten Handlungsempfehlungen fußen auf dem dort detaillierter beschriebenen Verständnis von Digitaler Souveränität. Insbesondere wird der systemische Ansatz, der jeweilige Ebenen nicht

[1] Merkel, A., Kallas, K., Frederiksen, M., Marin, S. (2021). Appell von vier Regierungschefinnen an die EU: »Europa muss seine digitale Souveränität stärken«, in: Handelsblatt, https://www.handelsblatt.com/meinung/gastbeitraege/digi talisierung-appell-von-vier-regierungschefinnen-an-die-eu-europa-muss-seine-digital e-souveraenitaet-staerken/26962398.html

[2] Mehr Fortschritt wagen: Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit. Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/ Die Grünen und den Freien Demokraten (FDP) (2021, 24. November). https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf

[3] Fries, I., Greiner, M., Hofmeier, M., Hrestic, R., Lechner, U., & Wendeborn, T. (2023). Towards a layer model for digital sovereignty: A holistic approach. In B. Hämmerli, U. Helmbrecht, W. Hommel, L. Kunczik, & S. Pickl (Eds.), Critical information infrastructures security (pp. 119–139). Cham: Springer Nature Switzerland.

isoliert, sondern organisch ineinandergreifend versteht, mit den hier präsentierten Handlungsempfehlungen weiterverfolgt.

Mit den vorgelegten Handlungsempfehlungen adressieren wir Entscheider und Entscheiderinnen und somit vorwiegend die Ebenen Organisation und Staat bzw. supranationale Institution (hier die EU).

3 Empfehlungen für Entscheider und Entscheiderinnen in Unternehmen

3.1.1 Empfehlungen für die Beschaffung

Auf dem Weg zu Digitaler Souveränität in Organisationen stellt die Beschaffung einen wichtigen Bereich dar, der Weichenstellungen ermöglicht. Beim Einkauf von Produkten (z.B. IT-Komponenten) und Dienstleistungen sollten dabei folgende Punkte berücksichtigt werden.

Redundanz: Für jedes eingekaufte Produkt sollten mehrere Zulieferer gewählt werden, sodass bei Wegfall eines Zulieferers noch Kapazitäten vorhanden sind. Dabei sollten auch reelle oder potenzielle geopolitische Spannungen einbezogen werden. Zulieferer sollten deshalb aus unterschiedlichen Regionen und, falls realisierbar, möglichst lokal gewählt werden. Bei Komponenten, die in risikobehafteten Regionen deutlich günstiger produziert werden können, und daher aus wirtschaftlichen Gründen nur von dort bezogen werden können (z.B. bestimmte Halbleiter), kann es hilfreich sein, zumindest einen kleineren Prozentsatz aus näheren Regionen zu beziehen. So bleiben die betreffenden Unternehmen und damit das Know-how in der Region erhalten, und es kann im Krisenfall darauf zurückgegriffen werden.

Austauschbarkeit: Komponenten sollten einfach gegen Komponenten anderer Hersteller austauschbar sein. Auch Provider-Services wie beispielsweise Cloud-Services sollten einfach austauschbar sein. Hier sollte vor allem geprüft werden, ob sich die Daten aus dem betreffenden Service in eine andere (ggfs. konkurrierende) Lösung migrieren lassen.

Recht auf Quelldaten: Bei der Beauftragung von Entwicklungsleistungen sollte sich die beauftragende Organisation das Recht auf die Quelldaten (z.B. Quellcode bei Softwareprojekten) sichern. So kann ein Lock-in bei Folgeaufträgen vermieden werden und die Unabhängigkeit gewahrt werden.

Plattformunabhängigkeit: Softwareprodukte sollten nach Möglichkeit so ausgewählt bzw. zur Entwicklung beauftragt werden, dass sie plattformunabhängig sind. So bleibt die Wahl des darunterliegenden Betriebssystems frei bzw. wird ermöglicht.

3.1.2 Empfehlungen für das Management

Bildung: Das staatliche Bildungssystem kann in erster Linie Kinder und Jugendliche für eine Bildung im Blick auf Digitale Souveränität erreichen. Eine verpflichtende Erwachsenenbildung kann dagegen nicht gewährleistet werden. Somit ist es die Aufgabe des betrieblichen Schulungswesens, Mitarbeitende hinsichtlich Digitaler Souveränität weiterzubilden. Das kann über betriebliche Fortbildungs- und Sensibilisierungsmaßnahmen erreicht werden.

Risikomanagement: Bei der Ausgestaltung der Infrastruktur sollten eindimensionale Abhängigkeiten von Technologien sowie Überkomplexität vermieden werden. Daneben sollte eine regelmäßige Bestandaufnahme und Risikobewertung in Bezug auf Digitale Souveränität stattfinden. Herfür kann das Thema der Digitalen Souveränität ggfs. in das bestehende Risikomanagement eingebettet werden.

Verantwortung: Es kann hilfreich sein, einen Beauftragten für Digitale Souveränität in der Organisation zu benennen, analog zur Rolle des Datenschutzbeauftragten. Daneben kann ein betriebliches Vorschlagswesen (ggfs. mit Anreizsystemen) etabliert werden, um Ideen und Innovationskraft der Belegschaft einzubeziehen.

3.1.3 Empfehlungen für die Schlüsseltechnologien Blockchain und KI

Blockchain: Mittels Blockchain kann die Datensouveränität aufgrund hoher Manipulationssicherheit und Unveränderlichkeit der Daten unterstützt werden. Ein weiterer Vorteil der Blockchain-Implementierung liegt in der ermöglichten Daten-Transparenz, die zum Beispiel innerhalb einer Lieferkette Nutzen schafft und in einem Krisenfall Handlungsmöglichkeiten beschleunigen und die Resilienz erhöhen kann.

Künstliche Intelligenz: Insbesondere im Blick auf Explainable AI sind europäische Innovationen gefragt. Vor allem in der Integration europäischer Werte in KI-basierte Technologien liegt ein ausbaufähiges Potenzial. Bislang gibt es nur wenige Anbieter aus Asien und Amerika, die Erklärbarkeit und Nachvollziehbarkeit von KI als Nische adressieren. Die Fokussierung auf EU-wertebasierter Explainable AI kann somit einen strategischen Wettbewerbsvorteil mit sich bringen. Gerade hier wäre es möglich, gute Anwendungsszenare zu entwickeln.

3.1.4 Empfehlungen für die Gewährleistung von mehr IT-Sicherheit

Strategie zur Digitalen Souveränität: Erhöhte Digitale Souveränität setzt die Auseinandersetzung mit dem Thema IT-Sicherheit aus politisch-technischer Perspektive voraus. Um IT-Sicherheit im Horizont Digitaler Souveränität in eine Gesamtstrategie einzubetten, empfehlen wir, Experten zum Thema IT-Sicherheit und Innovation zusammenzubringen, um eine unternehmensspezifische Strategie auszuarbeiten. Da sich technische Systeme, betriebliche Prozesse und Bedrohungslagen stetig verändern, ist auch das dazugehörige Consulting als dauerhafter Prozess zu behandeln anstatt als einmalige Maßnahme.

Resilienz: Trotz sorgfältiger Vorkehrungen kann ein Restrisiko für Sicherheitsvorfälle nie ausgeschlossen werden. Aus diesem Grund sollten Unternehmen strategisch planen, wie IT-Systeme abgesichert und schnell wiederaufgebaut werden können.

IT-Sicherheit als Unternehmenswert: Unternehmensprozesse und technische Systeme sind nur so sicher wie die nutzenden Beschäftigten. Auch wenn Beteiligte Wissen über IT-Sicherheit erwerben sollten z.B. im Rahmen von Schulungen, verhalten sie sich nicht unbedingt dementsprechend. Gelebte Unternehmenskultur bezüglich IT-Sicherheit, wie beispielsweise die Aufnahme des Themas in das betriebliche Vorschlagswesen mit dazugehörigem Anreizsystem, kann entsprechende Motivation bieten.

4 Empfehlungen für Entscheider und Entscheiderinnen in der Politik

4.1.1 Bildung

Schulsystem: Das Bildungssystem ist zentral für die Förderung der digitalen Kompetenzen zugunsten Digitaler Souveränität der einzelnen Individuen. Damit ist es auch mittelbar ausschlaggebend für Organisationen, in denen Individuen wirken. Digitale Souveränität sollte explizit als Lernziel definiert und in die Lehrpläne von Schulen, Hochschulen und Universitäten integriert werden. Dabei sollten neben dem sicheren Umgang mit IT auch begleitende Fähigkeiten und Wissen vermittelt werden, wie etwa ein Verständnis für Algorithmen (z.B. Feed), Quellenüberprüfung und Filterblasen. Das Fördern und Fordern entsprechender Qualifizierung von Lehrkräften stellt dafür die Basis.

Lebenslanges Lernen: Gleichzeitig ist ein Bewusstsein um einen Digital Divide unverzichtbar: Verschiedene Faktoren führen dazu, dass konkrete Bildungsstandards, Nutzungsbereitschaft im Blick auf Technologien oder auch ein technologie-bezogenes Risikobewusstsein unterschiedlich stark ausgeprägt sind. Auch im Blick auf ein lebenslanges Lernen ist es deshalb wichtig, Formate zu fördern, die Menschen jeden Alters, jedes Geschlechts und jeder sozialer Herkunft – Menschen in ihrer Diversität – im Blick auf Digitale Souveränität befähigen. Die Aus- und Weiterbildung digitaler Kompetenzen in der Breite mit entsprechenden Nutzen für die jeweiligen Arbeitsbereiche einer digital kompetenten Gesamt-Bevölkerung fördert nicht zuletzt auch die Wettbewerbsfähigkeit mit anderen Ländern.

4.1.2 Schaffung rechtlicher Vorgaben

Durch rechtliche Vorgaben kann die politische Sphäre Einfluss auf Digitale Souveränität in öffentlichen Einrichtungen oder bestimmten Unternehmen (z.B. Kritische Infrastrukturen) nehmen. Das kann sich durch Kaskadeneffekte auch auf weitere Unternehmen übertragen.

Vorgaben zur Beschaffung: Für öffentliche Einrichtungen oder Kritische Infrastrukturen (nach dem IT-Sicherheitsgesetz) sind Vorgaben für die Beschaffung denkbar. Beispielsweise könnten Organisationen verpflichtet werden, bei Beschaffungen zwingend Faktoren zugunsten Digitaler Souveränität zu prüfen, sowohl technischer Art (z.B. Modularität, offene Schnittstellen) als auch betriebswirtschaftlicher Art (z.B. Multi-Sourcing, Vermeidung langer Vertragslaufzeiten). Das sollte nicht zu Lasten von Innovationen gehen. Daher kann es bedeutsam sein, den Organisationen Freiräume zu lassen, in welcher Form Souveränitätsaspekte geprüft werden und welche Faktoren dabei definiert werden.

Open Source und Plattformunabhängigkeit: Allgemein könnten für Ausschreibungen der öffentlichen Hand für Neuentwicklungen von Software sowohl Quelloffenheit (Open Source) als auch Plattformunabhängigkeit vorgeschrieben werden. Dies hätte auch einen Einfluss über den öffentlichen Bereich hinaus, da so auch das Software-Ökosystem zugunsten Open Source und Plattformunabhängigkeit beeinflusst würde. Um Open-Source-Projekte zu fördern und zudem dafür zu sorgen, dass sie für die öffentlichen Interessen gut nutzbar sind, müssten relevante Projekte durch Finanzhilfen oder Personal (als Kontributoren) unterstützt werden.

4.1.3 Förderung von Arbeitsumgebungen zugunsten Digitaler Souveränität

Innovationsförderung: Um im internationalen Vergleich konkurrenzfähig zu sein, braucht es Innovationen. Dass es politisch geförderte Programme gibt, die Innovationsgeist fördern, ist deshalb begrüßenswert. In freiem und kreativem Think-Tank-Rahmen ermöglichen sie Erfindungsgeist mit Start-up-Kultur. Im Blick auf Digitale Souveränität können bereits bestehende Programme verlängert und dezidiert thematisch fokussiert werden. Um langfristige Perspektivität und Nachhaltigkeit zu garantieren, ist die Verstetigung dieser meist befristeten Programme mit Projektcharakter eine wichtige Voraussetzung. Ausbaufähig ist auch die Innovationsförderung innerhalb öffentlicher Einrichtungen (agile Strukturen, kurze Kommunikationswege oder Hands-On-Mentalität im Blick auf digitale Lösungen unter Abbau bürokratischer Hürden).

Forschungsförderung: Zur Konkurrenzfähigkeit im internationalen Vergleich ist zudem eine starke Forschung Voraussetzung. Auch dass es politisch geförderte Programme gibt, die die Wissenschaft zugunsten Digitaler Souveränität fördern, ist deshalb begrüßenswert. Außen- wie innenpolitische Entwicklungen zeigen: Die Themen Sicherheit und Souveränität nehmen an Relevanz noch zu. Es ist wichtig, diese Entwicklungen durch die professionellen Kompetenzen von Forscherinnen und Forschern verschiedener Disziplinen zu beobachten, reaktive Prozesse zu begleiten und wissenschaftsfundierte Weichenstellungen für die Zukunft anzustoßen. Damit Nachhaltigkeit und die stetige Weiterentwicklung freier wissenschaftlicher Kompetenz in öffentlicher Hand möglich sind, braucht es langfristige Finanzierungssicherheit von Forschung und Stellen. Entscheider und Entscheiderinnen in der Politik können durch Verstetigung von Projekten und damit einhergehender Entfristung von Stellen sowohl nachhaltige Forschung als auch öffentliche Zukunftsfähigkeit durch Forschung sichern.

Entlohnung von Fachkräften: Um öffentliche Einrichtungen im Zeichen Digitaler Souveränität auszurichten, braucht es Fachkräfte zur strategischen Entwicklung, Umsetzung und langfristigen Gewährleistung. Es lässt sich beobachten: Oft bleiben Stellen im IT-Bereich von öffentlichen Einrichtungen – auch in der Wissenschaft und im wissenschaftsstützenden Bereich – vakant, weil keine wettbewerbsfähige Entlohnung oder Perspektive angeboten werden kann. Eine krisenresiliente IT-Infrastruktur fußt auf qualifiziertem und engagiertem Personal. Deshalb ist es wichtig, in eine auch gegenüber der Wirtschaft im eigenen Land konkurrenzfähige Bezahlung zu investieren und mehr Planstellen im Blick auf Digitale Souveränität zu schaffen.

4.1.4 Kommunikation in Partei und Parlament

Konkretion und Beharrlichkeit: In der Parlaments- und Parteiarbeit könnte die Thematisierung Digitaler Souveränität stärker inhaltliche Wirkung entfalten. Konkrete Vorhaben zugunsten Digitaler Souveränität könnten Eingang in Parteiprogramme finden. Das Thema könnte auch in ergebnissichernder Regelmäßigkeit als Tagesordnungspunkt auf Agenden aufgenommen werden. Eine praxisbezogene und inhaltlich konkrete Füllung von „Digitaler Souveränität“ durch Entscheider und Entscheiderinnen in der Politik würde zur Entmythologisierung des Begriffs und damit auch im öffentlichen Diskurs zu einem besseren Verständnis der Thematik in der Bevölkerung führen.

Parteiübergreifende Debatte: Im Blick auf anti-europäische politische Parteiprogramme, die gegenwärtig an Zuspruch gewinnen, ist eine transparente politische Debatte wünschenswert: Wie lässt sich „Digitale Souveränität“, von denen EU-Papiere sprechen, in Einklang mit zunehmend nationalen Bestrebungen innerhalb Europas bringen oder gerade nicht? Wie kann technologische Unabhängigkeit erreicht werden ohne in nationaler Isolierung zu münden?