Toxische Tech-Abhängigkeit

Der steinige Weg zur digitalen Souveränität

Deutsche Behörden, Polizei und Bundeswehr sind von Technologien aus den USA abhängig – angesichts der offenen Drohungen der Trump-Administration gegenüber der EU ist das eine massive Sicherheitslücke. Expert:innen fordern schon lange mehr Anstrengungen, um digitale Souveränität zu erlangen. Doch von einer solchen sind die meisten hiesigen Behörden bisher weit entfernt.

Von SONJA PETERANDERL

Schleswig-Holstein verabschiedet sich gerade von der Software des US-amerikanischen Tech-Riesen Microsoft. Mehr als 40000 Postfächer mit Millionen von Kalendereinträgen und E-Mails wurden in den vergangenen Monaten von Microsoft Exchange auf Open-Xchange umgezogen, rund 80 Prozent der Arbeitsplätze in der Verwaltung sind bereits auf die Open-Source-Software LibreOffice umgestellt. Der Umzug hat einen politischen Hintergrund: Er soll die Abhängigkeit von US-amerikanischer Technologie reduzieren, das Bundesland digital souveräner machen – und spart gleichzeitig mehrere Millionen Euro an Microsoft-Lizenzgebühren.[1] Künftig will Schleswig-Holstein zudem von Windows auf das freie, quelloffene Betriebssystem Linux wechseln. Auch Thüringen setzt zunehmend auf freie Software, europäische Alternativen und eine neue Thüringer Verwaltungscloud. Im Gegensatz zu kommerzieller Software ist der Quellcode von Open-Source-Software frei zugänglich und kann von jedem eingesehen, genutzt, verändert und weitergegeben werden, solange die jeweiligen Lizenzbedingungen eingehalten werden. Offene Standards ermöglichen es, Produkte und Dienste zu entwickeln, die mit anderen Systemen kompatibel sind, wodurch Anbieterwechsel möglich werden und die Abhängigkeit von einem einzigen Hersteller (»Vendor Lock-in«) entfällt.

SONJA PETERANDERL
arbeitet als Investigativjournalistin u. a. für ARD Team Recherche und ist Gründerin des BuzzingCities Lab.

Selbst die Bundeswehr kündigte vor kurzem an, auf die Office- und Kollaborationssuite openDesk umzustellen, die das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) im Auftrag des Bundesinnenministeriums entwickelt hat. ZenDiS, eine Firma im Besitz des Bundes, beobachtet derzeit eine starke Nachfrage aus der öffentlichen Verwaltung sowie der Privatwirtschaft nach Alternativen zu marktdominierenden, meist US-amerikanischen Office-Lösungen.[2]

Die Befürchtung, die diese Suche nach Alternativen aktuell antreibt, lautet: Die Technologie aus den USA könnte von politischen Gegnern künftig als politische Waffe

1 Digitale Souveränität ist möglich und wirtschaftlich, schleswig-holstein.de, 4.12.2025.
2 ZenDiS schafft zusätzliche Bezugsmöglichkeiten für openDesk, zendis.de, 30.9.2025.

missbraucht werden. In den vergangenen Jahrzehnten haben große Techkonzerne aus den USA eine gigantische Marktmacht aufgebaut, auch KI-Entwicklungen werden maßgeblich von wenigen US-Firmen wie Apple, Google, Meta, OpenAI, Microsoft oder Amazon dominiert. Gleichzeitig ist die Nähe der Tech-CEOs zur Trump-Administration heute so eng wie nie zuvor – und deren rechtsextremer, ultranationalistischer Kurs unberechenbar. In ihrer neuen Sicherheitsstrategie behauptet die US-Regierung, die liberalen Demokratien in der EU seien auf dem Weg zur »zivilisatorischen Auslöschung«, stellt Europa als einen Kontinent im Niedergang dar und kündigt an, die europäische Politik beeinflussen zu wollen, etwa durch die Unterstützung gleichgesinnter »patriotischer« Parteien.[3] Wie sehr die Interessen von Politik und Techkonzernen in den USA verschränkt sind, zeigt auch das Ende 2025 wegen angeblicher Zensur verhängte Einreiseverbot gegen die beiden Digitalexpert:innen und HateAid-Geschäftsführerinnen Josephine Ballon und Anna-Lena von Hodenberg.[4] Die deutsche NGO HateAid unterstützt seit Jahren von digitaler Gewalt Betroffene und setzt sich für eine strengere Regulierung von US-Plattformen etwa durch den europäischen Digital Services Act ein.

In diesem fragilen politischen Szenario bringt die Abhängigkeit von großen US-Techkonzernen europäische Staaten, Unternehmen und andere Organisationen in eine brenzlige Lage: US-Software wird unter den neuen geopolitischen Bedingungen zu einem massiven Sicherheitsrisiko, schließlich könnten die USA Technologie und ihre Infrastruktur künftig gezielt als politisches Druckmittel missbrauchen. In Konfliktfällen mit Europa oder Deutschland könnten US-Firmen oder Behörden den Zugang zu wichtiger Software oder Cloud-Diensten unterbrechen oder Updates und Support einstellen. »Wenn die US-amerikanischen Cloud-Dienste in relativ kurzer Zeit ausfallen oder in Teilen nicht mehr verfügbar sind, sind wir hier in der Europäischen Union innerhalb weniger Tage nicht mehr arbeitsfähig«, warnte Dennis-Kenji Kipker, wissenschaftlicher Direktor beim Cyberintelligence Institute, kürzlich gegenüber der »Tagesschau«.[5] Der US-amerikanische CLOUD Act erlaubt US-Behörden zudem den Zugriff auf Daten, die von US-Unternehmen weltweit gespeichert werden – auch auf europäischen Servern. Zwar bieten US-Konzerne wie Amazon mit seiner »AWS European Sovereign Cloud« Clouddienste an, deren logistische und rechtliche Infrastruktur ganz auf Europa setzt. Doch Datenschützer wie Markus Beckedahl halten eine juristische Trennung zwischen US-Mutterfirma und europäischem Ableger nicht für möglich; die US-Regierung könnte zudem über Exportkontrollen künftige Updates verhindern und die Software zum Betrieb der Rechenzentren schnell außer Kraft setzen.[6]

Ein digital souveränes Deutschland?

Angesichts dessen haben CDU, CSU und SPD digitale Souveränität auch in ihrem Koalitionsvertrag 2025 explizit als Ziel verankert. »Digitalpolitik ist Machtpolitik«, heißt es dort. »Wir wollen ein digital souveränes Deutschland. Dazu werden wir digitale Abhängigkeiten abbauen, indem wir Schlüsseltechnologien entwickeln, Standards sichern, digitale Infrastrukturen schützen und ausbauen. Wir schaffen europäisch

3 National Security Strategy of the United States of America, whitehouse.gov, November 2025.
4 US-Einreiseverbot für HateAid-Leiterinnen - Warum gerade sie?, wdr.de, 24.12.2025.
5 Jens Eberl, Fest in amerikanischer Hand, tagesschau.de, 18.11.2025.
6 Neue Amazon-Cloud in Brandenburg: Wie sicher sind die Daten vor einem US-Zugriff?, tagesschau.de, 15.1.2026.

integrierte und resiliente Wertschöpfungsketten für Schlüsselindustrien, von Rohstoffen über Chips bis zu Hard- und Software.«

In der Theorie klingt das gut, doch von tatsächlicher digitaler Souveränität ist dem IT-Sicherheitsberater Manuel Atug zufolge bisher nicht viel zu spüren. Einen echten Bewusstseinswandel und Umbruch in Richtung digitaler Souveränität und Alternativen zu US-Produkten wie Open-Source-Software und andere Produkte, die auf offenen und freien Standards basieren, oder europäische Software-Lösungen sieht Atug »leider oft nur auf dem Papier«.[7] Bayern etwa habe ohne Ausschreibung einen Deal mit Microsoft geschlossen und will die Zusammenarbeit mit der US-Firma noch intensivieren. Für die Nutzung von Microsoft 365 für alle dortigen staatlichen Behörden sollen über einen Zeitraum von fünf Jahren knapp eine Mrd. Euro an den US-Giganten fließen.[8] Auch einer Studie der IT-Sicherheitsberatungsfirma Myra zufolge klafft eine gravierende Lücke zwischen der deutschen Vision von digitaler Souveränität und der Wirklichkeit bei Unternehmen und Behörden. »Der Markt wird in Schlüsselbereichen noch immer klar von US-Anbietern dominiert«, heißt es in dem Bericht »State of Digital Sovereignty 2025«.[9] Einer Umfrage unter rund 1500 IT-Entscheider:innen zufolge sprechen sich zwar fast 85 Prozent der Befragten dafür aus, dass Staat und kritische Infrastrukturen vorrangig europäische Digitalprodukte nutzen sollten. In ihren eigenen Unternehmen dominieren jedoch weiterhin US-Produkte. Lediglich rund ein Drittel der Unternehmen plant, in den kommenden 24 Monaten europäische Software einzuführen.

> »Von digitaler Souveränität ist bisher nicht viel zu spüren.«

Technologieabhängigkeit: Die schlummernde Gefahr

Dabei bergen solche toxischen Tech-Beziehungen insbesondere für kritische Infrastrukturen wie staatliche Behörden, Polizeien oder das Militär enormen Sprengstoff: »Bei ihrem Ausfall oder einer Einschränkung liegt eine besondere Gefährdung der öffentlichen Sicherheit und der Versorgungssicherheit der Bevölkerung vor«, warnt Manuel Atug, der sich als Teil der Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS) für die Verbesserung der IT-Sicherheit und Resilienz von kritischen Infrastrukturen in Deutschland einsetzt. »Wenn die Kernfunktionen von Staat und Verwaltung und damit der Demokratie von externen Mächten und der Willkür von bekennenden Faschisten abhängig sind, haben wir als Rechtsstaat ein erhebliches Problem«, so Atug – so wie im Fall des Einsatzes der Software des umstrittenen US-Überwachungskonzerns Palantir in deutschen Sicherheitsbehörden. »Der Investor Peter Thiel ist bekennender Faschist, und der CEO Alex Karp äußert sich zur Migrationspolitik Deutschlands mit Methoden der ›Entsorgung‹ von Migranten, die der AfD in nichts nachstehen«, so Atug.

Palantir ist seit 2003 durch enge Verbindungen zu US-Geheimdiensten, Militär und US-Regierung zu einem zentralen Akteur digitaler Überwachung avanciert und bietet Geheimdiensten, Polizeien, Militär, aber auch Unternehmen weltweit zum Teil KI-basierte Analyse- und Prognose-Tools, die riesige Datenmengen nach Verbin-

7 Interview vom 16.12.2025.
8 Bayern plant Milliarden-Deal mit Microsoft, it-business.de, 20.11.2025.
9 State of Digital Sovereignty 2025. Digitale Souveränität: zwischen Anspruch und Realität, myrasecurity.com.

dungen und Netzwerken durchforsten, teils auch Zukunftsprognosen erstellen oder Ziele für militärische Attacken vorschlagen, wie etwa in Gaza.[10] Das Überwachungsinstrumentarium von Palantir bildet ein zentrales Rückgrat der Trump-Administration. Massenabschiebungen sollen etwa durch das Palantir-System »ImmigrationOS« weiter beschleunigt werden, das Migrant:innen identifiziert und ihre Bewegungen verfolgt. Palantir-Investor und Mitgründer Peter Thiel unterstützte Trump bereits 2016 im Wahlkampf, trieb den intellektuellen Rechtsruck in den USA voran und förderte radikale republikanische Politiker:innen wie den heutigen Vizepräsidenten JD Vance. Die Software eines US-Konzerns, der eine eigene politische Agenda verfolgt, verwandelt sich derzeit weltweit zum zentralen Steuerungsinstrument für sicherheitsrelevante Institutionen, Entscheidungen und Einsätze. In Deutschland nutzen bereits drei Bundesländer Polizeisoftware, die auf der Palantir-Software »Gotham« aufbaut: Hessen, Nordrhein-Westfalen und Bayern. Bayern hat mit Palantir 2022 zudem einen Rahmenvertrag geschlossen, der es auch anderen Bundesländern und dem Bund ermöglicht, die Software ohne erneutes, langwieriges Ausschreibungsprozedere einzusetzen. Bundesinnenminister Alexander Dobrindt (CSU) prüft derzeit die bundesweite Einführung von Big-Data-Software für Polizeien - er will sich zwar noch nicht auf einen Anbieter festlegen, verteidigt aber öffentlich Palantir-Produkte. »Ich habe kein Störgefühl gegenüber einer Software, nur weil sie vom Anbieter Palantir kommt«, sagte Dobrindt im August 2025 im »Stern«-Interview.[11]

»Palantir-Software verwandelt sich derzeit weltweit zum zentralen Steuerungsinstrument für sicherheitsrelevante Institutionen.«

Palantir als Übergangslösung? Die Suche nach Alternativen

Nachdem lange offenbar keine Alternativen zur Palantir-Software existierten, versuchen europäische Anbieter mittlerweile nachzuziehen, doch zumindest kurzfristig bleibt Palantirs Big-Data-Software weiter bei vielen Stellen die erste Wahl. Auch die Polizei Baden-Württembergs hält die Einführung des bereits in Bayern eingesetzten Palantir-Systems »Verfahrensübergreifende Recherche- und Analyseplattform« (VeRA) für eine möglichst schnelle und automatisierte Analyse polizeilicher Daten für »unentbehrlich«.[12] Voraussichtlich wird Palantir-Software dort im zweiten Quartal 2026 einsatzbereit sein; KI-Produkte von Palantir sollen dabei nicht verwendet werden. Dem Innenministerium zufolge soll deren Einsatz »lediglich eine Übergangslösung sein«, parallel läuft die Entwicklung einer europäischen Alternative, einer »Europa-VeRA«, die von Innenminister Thomas Strobl (CDU) im Rahmen einer Kooperation mit der Airbus Defence and Space GmbH sowie der Digitalsparte der Schwarz Gruppe, Schwarz Digits, und in engem Austausch mit Baden-Württembergs Sicherheitsbehörden entwickelt werden soll. Auch die französische KI-Firma Chaps-

10 Vgl. Sonja Peteranderl, Das Überwachungsimperium. Wie sich die deutsche Polizei von Peter Thiels Palantir-Software abhängig macht, in: »Blätter«, 8/2025, S. 91-96.

11 »Wir müssen die Überforderung unseres Landes beenden«, Bundesinnenminister Alexander Dobrindt im Interview mit dem »stern«, bmi.bund.de, 26.8.2025.

12 Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg, Pressestelle, E-Mail vom 23.12.2025.

Vision versucht sich in Europa als europäische Palantir-Alternative zu positionieren. Im Oktober 2025 gab die Firma eine Partnerschaft mit der deutschen IT-Firma Rola Security Solutions bekannt, die bereits Softwareprojekte für deutsche Polizeien betreut. Gemeinsam wollen sie die ChapsVision-Plattform ArgonOS für Big-Data-Analysen bei deutschen Polizeien und Geheimdiensten etablieren. Die KI-basierte Anwendung verknüpft verschiedene Datenquellen miteinander und ist bereits bei französischen Sicherheitsbehörden im Einsatz. Allerdings sind auch Frankreichs Sicherheitskräfte zumindest mittelfristig noch von Palantir abhängig. Der französische Inlandsgeheimdienst Direction Générale de la Sécurité Intérieure (DGSI) verlängerte den Vertrag mit dem US-Konzern gerade um drei weitere Jahre – »bis zur Einführung eines neuen souveränen Tools«[13].

Achillesferse Militär-Software

Auch für die Bundeswehr stellt die Digitalisierung eine »Achillesferse« dar: »Die heutigen Streitkräfte sind in hohem Maße von Software abhängig«, schreibt Alexandra Paulus von der Stiftung Wissenschaft und Politik (SWP) in einem Strategiepapier. »Softwareprodukte werden von komplexen Netzwerken aus Softwarekomponenten, Softwareanbietern, Dienstleistern und anderen Unternehmen entwickelt, die zusammen die Software-Lieferkette bilden.«[14] Alle Glieder seien ihr zufolge über Software miteinander verbunden und könnten jeweils als Einfallstor in militärische Systeme fungieren. »Insbesondere kleine und mittlere Unternehmen (KMU) und kleinere Open-Source-Software-Projekte (OSS) sind oft schlecht geschützt und daher ein leichtes Ziel für Angreifer«, warnt Paulus. »Darüber hinaus haben die Streitkräfte oft keinen Überblick über alle von ihnen verwendeten Softwareprodukte, geschweige denn über alle Akteure und Komponenten, die die Lieferketten dieser Produkte ausmachen.« Über weite Teile der Lieferkette habe die Bundeswehr wenig oder gar keine Kontrolle. »Da die Bundeswehr viele spezielle und auch schwere Geräte mit Software betreibt, etwa Panzer und Fregatten, steht sie immer vor der Herausforderung, aus welchem Land die darin befindlichen Softwarekomponenten kommen und wie diese abgesichert werden können«, beobachtet auch IT-Experte Atug, »kein einfaches Unterfangen, dem man sich aber recht gut stellt.« Atug hält auch die sogenannte *vulnerability disclosure policy* der Bundeswehr für eine sinnvolle Strategie, die Sicherheitsforscher:innen seit 2020 dazu einlädt, entdeckte Schwachstellen zu melden, sodass die Bundeswehr ihre Systeme besser sichern kann.[15]

Im Geschäftsbereich des Bundesministeriums der Verteidigung, einschließlich aller Teilstreitkräfte, wird Palantir-Software bisher nicht eingesetzt.[16] Die Nato gab im März 2025 bekannt, die KI-basierte militärische Plattform Palantir Maven Smart System Nato (MSS Nato) gekauft zu haben; KI solle künftig in zentralen militärischen Operationen eingesetzt werden und Informationsfusion, Zielerfassung, Lagebewusstsein, Einsatzplanungen im Kampfgebiet sowie die Entscheidungsfindung verbessern.[17]

13 US tech firm Palantir extends deal with French intelligence agency, lemonde.fr, 15.12.2025.

14 An Achilles Heel of Today's Armed Forces. Managing Software Supply Chain Risk in the Military Sector, swp-berlin.org, 17.11.2025.

15 Vulnerability Disclosure Policy der Bundeswehr, bundeswehr.de.

16 Sprecher des Kommandos Cyber- und Informationsraum Bundeswehr, E-Mail vom 17.1.2026.

17 NATO acquires AI-enabled Warfighting System, shape.nato.int, 14.4.2025.

In der Schweiz entschieden sich Bundesämter und Armee hingegen gegen Palantir-Software: Ein Militärgutachten rät hier stattdessen dazu, europäische Alternativen zu Palantir wie Software von SAP oder Accenture in Erwägung zu ziehen, Open-Source-Optionen zu prüfen oder eigene Datenanalyseplattformen zu entwickeln. Der Einsatz von Palantir-Lösungen biete zwar die Möglichkeit, schnellere datenbasierte Entscheidungen zu treffen und die Effizienz militärischer Operationen zu steigern, heißt es dort.[18] »Doch die Bedenken bezüglich Datenhoheit, nationaler Souveränität, Abhängigkeiten sowie ethischer und sicherheitspolitischer Aspekte sind nicht zu unterschätzen.« Es bestünde die Möglichkeit, dass sensible Daten durch US-Regierung und Geheimdienste eingesehen werden könnten. Auch eine potenzielle Abhängigkeit von externem hochqualifiziertem Personal der US-Firma halten die Gutachter:innen für riskant: »Eine solche Abhängigkeit kann die Handlungsfähigkeit der Armee in Krisensituationen einschränken«, warnen sie. »Sollten Palantir-Spezialisten abgezogen werden oder nicht zur Verfügung stehen, könnte dies die Einsatzfähigkeit der Systeme und damit die Effektivität der militärischen Operationen gefährden. Zugleich wird durch die dauerhafte Anwesenheit externer Spezialisten die Geheimhaltung militärischer Informationen herausgefordert, da sie Zugang zu kritischen Prozessen und Daten erhalten.«

»Beispiele wie die Open-Source-Strategie von Schleswig-Holstein zeigen, dass ein Abschied von US-Software möglich ist.«

Die Bundeswehr unterhält mit dem Bataillon Elektronische Kampfführung 912 immerhin auch ein eigenes KI-Labor, das zusammen mit zivilen IT-Expert:innen KI-Anwendungen für den militärischen Kontext erforscht und entwickelt. Sie verfolgt also verschiedene Tech-Ansätze parallel: Open Source-basierte Tools neben Eigenentwicklungen, Kooperationen mit europäischen Techfirmen sowie neue oder fortgesetzte Deals mit US-Konzernen, darunter auch eine neue Partnerschaft mit Google. Bis Ende 2027 soll die neue Cloud-Umgebung »Google Cloud Air-Gapped« in den Rechenzentren der Bundeswehr aufgebaut werden.[19] Noch sieht der IT-Experte Atug daher »erhebliche Defizite« bei der digitalen Souveränität der Bundeswehr. Tatsächlich lässt sich die Umstellung auf US-Alternativen in Bereichen wie der Kommunikation und Kollaboration deutlich leichter bewerkstelligen als bei sehr spezialisierter Software wie Datenanalysen für Polizei oder Militär. Beispiele wie die Open-Source-Strategie von Schleswig-Holstein zeigen Atug zufolge aber, dass ein Abschied von US-Software möglich ist. Die Lösungen seien auch in großem Maßstab denkbar, »insofern kann ganz Deutschland eine solche Vorgehensweise realisieren, wenn der Wille da ist«. Damit sich Open Source flächendeckend durchsetzt, bedürfe es aber eines Bewusstseinswandels: Noch sähen viele Entscheider:innen Open Source kritisch, weil es »umsonst« sei. Dabei mache die Umstellung auf Open-Source-Alternativen gerade wegen der offenen Standards unabhängiger und damit deutlich souveräner. Höchste Zeit also, dass das Vorbild Schleswig-Holstein auch im Rest der Republik Schule macht. ⬡

18 Schweizerische Eidgenossenschaft, Bericht: Palantir Technologies Inc., cdn.repub.ch, 4. 12.2024.
19 Google Cloud und BWI geben Partnerschaft bekannt, bwi.de, 26.5.2025.