

Macht ohne Mandat

Was passiert, wenn private Unternehmen Funktionen kontrollieren, die für Staaten strategisch unverzichtbar sind – etwa im Gesundheitswesen, dem Militär oder der staatlichen Verwaltung? Drei Beispiele.

Von Jana Ehrhardt-Joswig, Elke Schwarz und Daniel Castro

Bild nur in
Printausgabe
verfügbar

Schneller, höher, weiter: Tech-Unternehmen sind längst Teil des modernen Staates. Ihre Produkte und Dienstleistungen versprechen Innovation und Effizienz. Was ist der Preis?

Der Körper als Plattform

Von Hirnchips bis Smartwatches: Digitale Technologien versprechen bessere Medizin, schaffen aber auch neue Abhängigkeiten. Europa muss jetzt entscheiden, wem unsere Gesundheitsdaten gehören.

Von Jana Ehrhardt-Joswig

Science-Fiction ist Fiktion. Und doch steckt in ihr viel Wahrheit: Sie denkt die Gegenwart weiter. Nicht, indem sie orakelt, was kommen wird, sondern indem sie zeigt, wohin heutige Technologien führen könnten.

So wie die dystopische Netflix-Serie „Black Mirror“. In der Episode „Common People“ bricht die Lehrerin Amanda mitten im Unterricht zusammen. Die Ärzte finden einen inoperablen Hirntumor. Das Unternehmen Rivermind bietet ihr eine zweite Chance: Amandas Gehirn wird an eine digitale Infrastruktur angeschlossen. Sie lebt weiter.

Doch von nun an hängt ihr Leben an einem Abonnement. Der zunächst erschwingliche Dienst bekommt neue Bedingungen, zusätzliche Leistungen kosten extra. Amanda muss Werbung auftragen, ihr Bewegungsradius und ihr Alltag werden von der Plattform bestimmt. Je verzweifelter ihr Ehemann Mike versucht, ein erträgliches Leben zu finanzieren, desto stärker gerät auch sein eigenes Leben in den Sog des Unternehmens. Überflüssig zu schreiben, dass es kein gutes Ende nehmen kann, wenn Verzweiflung zum Geschäftsmodell wird.

Mensch und KI verschmelzen

Die Idee, das menschliche Gehirn an eine digitale Struktur anzuschließen, ist nicht weit hergeholt. Pionier auf diesem Gebiet ist der Tech-Milliardär Elon Musk. Sein Hirnchip Neuralink, eine sogenannte

Hirn-Computer-Schnittstelle, wurde 2024 erstmals einem querschnittgelähmten Patienten eingesetzt. Der Chip erkennt Aktivitätsmuster und übersetzt neuronale Signale in digitale Befehle. So können Menschen etwa einen Cursor oder andere Geräte steuern – kraft ihrer Gedanken. Anfang 2026 gelang es einem querschnittgelähmten Patienten sogar, einen Roboterarm anzusteuern, um sich selbst zu füttern, etwas zu trinken oder sich zu kratzen.

„Die Ingenieursleistung, die dahintersteckt, ist absolut bemerkenswert“, sagt Surjo Soekadar, der an der Berliner Charité an Neurotechnologien forscht, die das Gehirn stimulieren und Computer oder Roboter mittels Hirnsignalen steuern. Anders als Musk setzt er dabei vor allem auf nichtinvasive Methoden, also das Messen und Beeinflussen der Hirnaktivität von außen. „Wir möchten keine Technologien entwickeln, die in den Körper eindringen“, sagt er. Nicht, weil er invasive Technologien grundsätzlich ablehne, sondern weil er vermeiden wolle, dass Menschen langfristig von einzelnen Anbietern und deren Geschäftsmodellen abhängig werden. Er möchte Innovations- und Geschäftsmodelle entwickeln, die genau das Gegenteil bewirken: Autonomie und Wahlfreiheit erhalten.

Außerdem akzeptiere er die Grenzen der Biologie, so Soekadar. Musk habe die Gehirn-Computer-Schnittstelle von Anfang an als Chance beschrieben, die



Jana Ehrhardt-Joswig

ist Redakteurin im Team von Tagesspiegel Background Gesundheit & E-Health.

Menschheit mit Künstlicher Intelligenz zu verschmelzen. Diese „transhumanistische Perspektive“ sei jedoch „überhaupt nicht“ Soekadars Sicht auf die Welt und für ihn kein wünschenswertes Leitbild.

Gesundheitsdaten in der App

Technologische Abhängigkeit beginnt allerdings nicht erst bei der Verschmelzung mit einer KI. Es gibt sie bereits. „Wir leben längst in einer Welt, in der wir nicht mehr digital unabhängig von amerikanischen Plattformen agieren können“, sagt Henrik Matthies. Er ist Mitgründer und Co-CEO von Honic, einer Plattform, die Gesundheitsdaten für Forschung nutzbar macht. Von 2019 bis 2021 leitete er den Health Innovation Hub, eine Denkfabrik, die das Bundesgesundheitsministerium bei der Digitalisierung des Gesundheitswesens unterstützte.

Was er damit meint: Apple und Google verlangen Provisionen oder Servicegebühren für Apps in ihren Stores. Damit kontrollieren sie wichtige Zugänge zur digitalen Versorgung. Eine App kann aus einem Store verschwinden, ein Plattformdienst eingeschränkt werden. Mit dem Abschalten einer lebenswichtigen Behandlung ist das zwar nicht vergleichbar. Aber je mehr Versorgung auf solchen Diensten aufbaut, desto dringlicher wird die Frage: Wer entscheidet über ihre Verfügbarkeit und ihre Bedingungen?

Die Kontrolle betrifft nicht nur den Zugang zu Anwendungen, sondern auch die technischen Regeln des Datenaustauschs. Mit HealthKit und Health Connect betreiben Apple und Google zentrale Schnittstellen für Gesundheits- und Fitnessdaten. Mit Zustimmung der Nutzer können Apps etwa Bewegungs-, Schlaf- oder Herzfrequenzdaten auslesen und austauschen. Zugleich erzeugen die Geräte eigene Datenbestände. Apple Watches

erfassen unter anderem Herzfrequenz, Bewegung, Schlaf und teils EKG-Daten. Googles Pixel-Watch- und Fitbit-Angebote liefern ebenfalls Aktivitäts- und Schlafdaten.

Der weltweite Wearables-Markt wächst stetig. Nach Angaben des international tätigen Marktforschungsunternehmens IDC wurden im ersten Quartal dieses Jahres weltweit rund 146 Millionen vernetzte, am Körper getragene Geräte ausgeliefert – 4,3 Prozent mehr als im Vorjahreszeitraum. Hearables, also Kopf- und Ohrhörer mit und ohne Gesundheitsfunktionen, waren am gefragtesten. Smart-Brillen und smarte Ringe verzeichneten dagegen das stärkste Wachstum.

Obwohl nicht alle von IDC erfassten Wearables medizinische Messgeräte sind und Gesundheitsdaten messen, tun sehr viele Smartwatches, Fitnesstracker oder smarten Ringe genau das: Sie zeichnen permanent Körper- und Verhaltensdaten auf, erzeugen gewissermaßen eine kontinuierliche Datenspur ihrer Nutzer. Je mehr Menschen solche Geräte dauerhaft tragen, desto mehr Daten fallen an, und desto detaillierter lässt sich ihr Gesundheitszustand abbilden.

Für die Gesundheitsforschung kann das eine riesige Chance sein. In einem im Mai 2026 in *Nature Reviews Disease Primers* erschienenen Beitrag bezeichnen Forscherinnen Wearables als potenzielles Mittel gegen einen „blinden Fleck“ der Medizin: die Unterrepräsentation von Frauen. Die kontinuierlichen Messungen könnten physiologische Veränderungen über längere Zeiträume sichtbar machen, etwa im Zusammenhang mit Menstruationszyklus, Schwangerschaft oder Wechseljahren.

Matthies sieht in den umfassenden Datenbeständen aber auch eine Gefahr. Er sagt: „Die Machtverhältnisse verschieben

sich.“ Wer die gesundheitlichen Risiken oder Schwachpunkte eines Menschen und seiner Familie kennt, könnte dieses Wissen nutzen, um Druck auszuüben – „wir werden dadurch erpressbar“.

Messen im Namen der Verteidigung

Dieselben Daten, die der Medizin neue Einblicke in den menschlichen Körper ermöglichen, können auch dazu dienen, Menschen leistungsfähiger und einsatzbereiter zu machen. Das zeigt das Beispiel Oura. Der Hersteller des gleichnamigen smarten Rings kooperiert seit 2019 mit dem US-Verteidigungsministerium. Nach eigenen Angaben hat das Unternehmen inzwischen Zehntausende Ringe im US-Verteidigungssektor eingesetzt. Sie erfassen unter anderem Schlaf, Stress, Ermüdung und andere biometrische Daten der Soldatinnen und Soldaten. Dies dient nicht nur der Überwachung ihrer Gesundheit, heißt es bei Oura. Es gehe dabei auch darum, ihre Leistungsfähigkeit und Einsatzbereitschaft zu optimieren.

Oura, Hersteller eines smarten Rings, kooperiert seit 2019 mit dem US-Verteidigungsministerium

Dass dabei Palantir mitmischt, das „geheimnisvollste Unternehmen der Welt“, wie es oft genannt wird, gibt dem Ganzen einen bitteren Beigeschmack. Hinter Palantir steht der Tech-Milliardär und Trump-Unterstützer Peter Thiel, der aus seiner Abneigung gegenüber Europa keinen Hehl macht. Auch wenn Oura betont, Palantir habe keinen Zugriff auf die Gesundheitsdaten ziviler Nutzer, ändert das nichts an der grundsätzlichen Frage, wie weit die Vermessung des mensch-

lichen Körpers gehen sollte – und wer über diese Daten verfügen darf.

KI in Krankenhäusern

Dabei sollte man nicht nur die bekannten Silicon-Valley-Konzerne in den Blick nehmen, betont Aldo Faisal. Der Informatiker und Neurowissenschaftler lehrt Digital Health und Data Science an der Universität Bayreuth sowie KI und Neurowissenschaften am Imperial College London. Seit 2024 ist er außerdem Mitglied des Deutschen Ethikrats.

Man müsse zwischen Ländern, Unternehmen und den unterschiedlichen Ebenen der digitalen Versorgung unterscheiden. Während Apple vor allem auf persönliche Gesundheit und Consumer-Produkte setze, seien Amazon und Microsoft auf der Cloud- und Infrastrukturebene aktiv. Im Krankenhaus wiederum gehe es um spezialisierte Anbieter wie Epic, InterSystems und Oracle Health.

Dahinter stünden jeweils unterschiedliche Plattformmodelle. Im Krankenhaus könnten sogenannte Krankenhausinformationssysteme (KIS), die Behandlungsabläufe und medizinische Dokumentation unterstützen, künftig zur Plattform für zahlreiche spezialisierte Anwendungen werden – ähnlich wie ein Smartphone für seine Apps. Eine KI könnte beispielsweise Röntgenbilder auswerten, eine andere Veränderungen in Labor- und Vitaldaten erkennen und das Behandlungsteam auf mögliche Komplikationen hinweisen. Neue Anwendungen müssten dann nicht jeweils eine eigene technische Infrastruktur mitbringen, sondern könnten gemeinsame Dienste und freigegebene Daten nutzen.

Eine Plattform könne aber auch öffentlich organisiert sein, sagt Faisal und verweist dafür auf die App des britischen Gesundheitsdiensts NHS. Patientinnen

und Patienten können darüber unter anderem Rezepte nachbestellen und Untersuchungsergebnisse einsehen.

Eine funktionierende Versorgung ist seiner Ansicht nach ein wichtiger Pfeiler der Demokratie: „Wo sie zusammenbricht, erodiert auch das Vertrauen in den Staat.“ Die Alternative heiße deshalb nicht weniger Digitalisierung. Diese müsse jedoch so gestaltet werden, dass sie die öffentliche Handlungsfähigkeit stärkt, statt sie durch neue Abhängigkeiten zu begrenzen.

Europas Chance auf Souveränität

Dafür stünden Europas Chancen nicht schlecht, sagt Matthies: „Paradoxerweise ist der digitale Rückstand unseres Gesundheitswesens ein glücklicher Umstand.“ Weil das Gesundheitswesen so lange unterdigitalisiert war, sei die Kontrolle über seine Daten noch nicht in gleichem Maße an große Plattformen verloren gegangen. Europa könne nun aus den Fehlern anderer lernen und seine Infrastruktur souverän gestalten. Das sei

auch deshalb wichtig, so Matthies, weil sich die US-Regierung mit dem US Cloud Act Zugriff auf Daten sichert, die ein amerikanisches Unternehmen in der Cloud speichert oder kontrolliert, selbst wenn die Server in Europa stehen.

Auch Soekadar sagt: „Technologien, denen eine europäische Gesellschaft vertrauen will, müssen auch hier entwickelt werden.“ Das Potenzial sei vorhanden. Allerdings müsse sich in Deutschland und Europa einiges ändern: „Wir brauchen mehr Mut zum Risiko, mehr Kapital für Deep Tech, weniger Zögern – sonst verpassen wir den Anschluss.“

Im Europäischen Gesundheitsdatenraum (EHDS) sieht Matthies die Chance, eine europäische Dateninfrastruktur digital souverän zu gestalten. Der EHDS soll den Austausch elektronischer Gesundheitsdaten über Ländergrenzen hinweg erleichtern und ihre Nutzung für Forschung und neue Therapien ermöglichen – unter gemeinsamen Regeln. Ab 2029 soll es losgehen. Damit „Common People“ Fiktion bleibt.



Dr. Elke Schwarz

ist British Academy Fellow for Global Innovation am Zentrum für Sicherheit und Verteidigung der DGAP. Sie lehrt und forscht als Professorin an der Queen Mary University of London.

Das Geschäft mit dem Krieg

Technologie-Start-ups wie Helsing, STARK Defence und Anduril haben in der Verteidigungsbranche Fuß gefasst. Finanziert werden sie von Risikokapitalgebern – eine riskante Entwicklung für Demokratien.

Von Elke Schwarz

Der Einzug des Silicon Valley in die Verteidigungsindustrie vollzieht sich seit gut einem Jahrzehnt, nicht nur in den USA, sondern verstärkt auch in Europa. Künstliche Intelligenz (KI) und Autonomie dominieren viele

moderne Militärstrategien. Digitalisierte Zielplanungssysteme, KI-gesteuerte Drohnen und autonome Systeme aller Art stehen ganz oben auf der Wunschliste der NATO-Staaten und ihrer Streitkräfte. Oft wird dabei eine Zukunft des Krieges

prophezeit, in der man ohne KI und autonome Waffen nicht gewinnen oder gar überleben kann. Ein wachsender Anteil der rapide steigenden Verteidigungsbudgets fließt inzwischen in solche Systeme. Für Technologiefirmen und Investoren eröffnet das finanzielle Chancen.

Der globale Markt für militärische KI ist lukrativ. Sein Volumen wird derzeit auf rund 16,8 Milliarden US-Dollar geschätzt, bei einem erwarteten jährlichen Wachstum von ungefähr 13 Prozent über die kommenden zehn Jahre. Ähnlich verhält es sich bei autonomen Waffensystemen: Dieses Segment hat weltweit einen Wert von etwa 14,3 Milliarden Dollar und wächst um rund 10 Prozent jährlich. Auch sogenannte Kamikaze-Drohnen sind ein Wachstumsgeschäft, mit einer jährlichen Rate von rund 12 Prozent. Zum Vergleich: Traditionelle Systeme wie Kampffjets oder Panzer wachsen um 3 bis 5 Prozent.

Immer häufiger setzt man auf Technologie-Start-ups, um KI-fähige, autonom aufgestellte Streitkräfte zu schaffen und frischen Wind in den als verstaubt geltenden Verteidigungssektor zu bringen. Wo es Start-ups gibt, sind private Geldgeber meist nicht weit. Vor allem Risikokapital (Venture Capital, VC) setzt seit Kurzem auf die Verteidigungsbranche als Milliardenchance. Mit dem Einzug des Silicon Valley haben also nicht nur Technologien aus Kalifornien Fuß gefasst, sondern auch die finanzielle Logik der US-Technologiebranche und damit das Konzept des „patriotischen Kapitals“. Risikokapital ist auf Disruption spezialisiert, und Disruption zerstört Bestehendes. Der Silicon-Valley-Mythos der kreativen Zerstörung rückt in den Mittelpunkt.

Risikokapital trifft Rüstung

Venture Capital ist kein Neuling in der Verteidigungsbranche. Schon zur Geburts-

stunde des Silicon Valley in den 1950er Jahren waren Militär, Technologie und Risikokapital eng miteinander verbunden. Das änderte sich allerdings rasch, als Informationstechnologien in den 1980er und 1990er Jahren außergewöhnlich große Gewinnchancen versprachen. Außerdem unterlagen Militärbeschaffungen strengen Bestimmungen, und der Markt wurde von den fünf führenden Unternehmen, den sogenannten Primes, dominiert. Sie hatten die Beschaffung und die Auftragsvergabe für militärische Zwecke fest im Griff. Hinzu kam für viele Investoren ein Tabu: Vom Krieg zu profitieren, war verpönt und galt als etwas vulgär. Für viele institutionelle Investoren war das nicht mit ihren ESG-Standards vereinbar, also mit Standards zu Umwelt, Sozialem und Unternehmensführung.

Seit 2014 hat sich das deutlich verändert. Die Idee, dass Krieg vor allem ein Softwareproblem sei, das sich mit Ansätzen aus dem Silicon Valley lösen lasse, hat sich immer mehr durchgesetzt. Amerikanische Initiativen wie die Defense Innovation Unit, die privates Kapital mit militärischen Innovationsprojekten zusammenbrachte, sorgten dafür, dass dem US-Verteidigungsministerium gezielt die DNA des Silicon Valley injiziert wurde.

Weltweit sind Risikokapitalanlagen im Verteidigungsbereich in den vergangenen Jahren deutlich angestiegen. Ohne diese Art von Kapital gäbe es die neuen Start-up-Lieblinge der Rüstung nicht, allen voran Helsing, STARK Defence und Quantum Systems, aber auch Anduril und Palantir. 2025 war ein Rekordjahr für Risikokapital in der Verteidigungstechnologie, global wie in Europa. Seit 2021 sind weltweit rund 150 Milliarden Dollar Risikokapital in die Rüstung geflossen, in Europa waren es 2025 rund fünf Milliarden. Zwar ist der Anteil von Rüstungs-Start-ups am

Risikokapitalmarkt nach wie vor gering. Dennoch lässt sich beobachten, dass die Logik des Risikokapitals und insbesondere die des Silicon Valley – „move fast and break things“ – einen immer stärkeren, unverhältnismäßigen Einfluss auf die Ausrichtung der militärischen Praxis und das Verteidigungsethos gewinnt. Disruption, Innovation, Risiko, Schnelligkeit und Masse sind zu vorrangigen Werten geworden. Das entspricht unmittelbar den Dynamiken und Bedürfnissen des Risikokapitalmarkts im Silicon Valley.

Wetten auf schnelles Wachstum

Die Ziele und Erwartungen von VC bringen Tempo und Masse („speed and scale“) in die Verteidigungsbranche. VC-finanzierte Start-ups müssen ihren Wert schnell und im Idealfall in großem Umfang steigern, um die außergewöhnlichen Renditen zu erzielen, an die sich das Risikokapital gewöhnt hat. Wie der Name schon sagt, ist das investierte Kapital mit Risiken verbunden: In der Regel scheitern zwischen 75 und 90 Prozent der Start-ups.

Die Krux dabei ist, dass das Produkt der Risikokapitalfirmen Wachstum ist. Im Vordergrund steht also die Bewertung der Firmen, die oft in kurzer Zeit astronomische Höhen erreicht. Anduril etwa gibt es erst seit 2017; derzeit wird das Unternehmen mit 61 Milliarden Dollar bewertet, ohne je Gewinn gemacht zu haben. Der Umsatz von Anduril belief sich 2024 auf lediglich eine Milliarde Dollar. Ähnlich ist es bei deutschen Militär-Start-ups wie Helsing, STARK Defence oder Quantum Systems. Oft werden enorme Summen eingesetzt, um ihr exponentielles Wachstum zu befeuern. Die neuen Rüstungs-Start-ups sind damit nicht nur Drohnen- oder KI-Unternehmen, sondern auch Kapitalanlagen, von denen erwartet wird, dass sie schnell an Wert gewinnen.

Der Großteil des Venture Capital und die erfolgreichsten Start-ups der Rüstungsbranche kommen aus den USA. Das amerikanische Geschäftsmodell dominiert damit auch in Europa. VC-Unternehmen mindern ihr Risiko und das ihrer Investoren, indem sie diversifizieren und die vielversprechendsten Start-ups eng begleiten. Der Fokus liegt auf Produkten, die sich am besten skalieren lassen, und das ist nicht immer das innovativste Produkt. Um Einfluss auf Entscheidungsträger zu nehmen, setzt man auf Lobbyisten, Anwälte und eine spezifische, breit gestreute Medienstrategie, die darauf abzielt, den Verteidigungssektor den kulturellen Grundwerten der amerikanischen VC-Branche anzupassen.

Kreative Zerstörung

Das eigentlich Revolutionäre liegt damit oft nicht in der technologischen Erfindung selbst, sondern im Umkrempeln alter Strukturen, die als antiquiert, obsolet oder gar gefährlich bezeichnet werden. Das führt zu einer Aufwertung einer spekulativen Zukunft, während die Gegenwart abgewertet wird. Dafür werden bestimmte Narrative wiederholt: Die Rüstungsbeschaffung sei viel zu langsam, das Problem sei nicht die Technik, sondern die Bürokratie; man dürfe das Rennen nicht verlieren, man müsse umdenken und mehr Risiko eingehen; eine Krise sei stets am Horizont. Außerdem wird immer häufiger die Notwendigkeit einer Reindustrialisierung betont. Begleitet wird all dies von der Losung, Frieden und Demokratie müssten mithilfe neuer Waffentechnologie gesichert werden – si vis pacem para bellum.

Eine Handvoll äußerst aktiver US-Risikokapitalgesellschaften investiert entweder selbst in Verteidigungs-Start-ups in Europa und anderswo oder ist mit Netz-

Bild nur in Printausgabe verfügbar

Risikokapital macht's möglich: Die unbemannte Kampfdrohne YFQ-44A Fury des Rüstungs-Start-ups Anduril gehört zu einer neuen Generation teilautonomer Waffensysteme, die im Auftrag des Pentagons gebaut werden.

werken verbunden, die finanziell vom Aufbau der europäischen und britischen Kriegsmaschinerie profitieren. Zu den lautstärksten Akteuren gehören einige politisch und finanziell sehr präsente Figuren, darunter Marc Andreessen, Peter Thiel und Alex Karp. Dieser „Vibe Shift“ umfasst die Aufwertung des Konflikts, eine größere Bereitschaft, Opfer als notwendig hinzunehmen, und die Normalisierung von Gewalt als Mittel, um Frieden und Freiheit zu stiften.

Es entsteht eine deutliche Spannung zwischen der Dynamik von Risikokapitalinvestitionen, den Anreizen für Start-ups im Verteidigungsbereich und dem moralisch komplexen Feld des Krieges. Risikokapital ist nicht einfach ein weiterer Akteur in der Verteidigungsindustrie, sondern einer, der darauf angewiesen ist, dass sich der Markt seiner eigenen Dynamik anpasst. Und Verteidigung ist nicht einfach ein weiteres Geschäftsfeld, sondern ein zutiefst menschlicher Bereich, in dem moralisch so viel auf dem Spiel steht wie in kaum einem anderen.

Regierungen fehlen die Ressourcen und der demokratische Spielraum, um wie Risikokapitalgeber auf spekulative Möglichkeiten zu setzen. Auch können sie Risiken nicht gleichermaßen auffangen, schon gar nicht in der Verteidigung. Die Umwälzungen, die Risikokapital auslöst, bringen ein gewisses Chaos mit sich und brechen mit etablierten Normen. Sie können dazu führen, dass überzogene Versprechen zu spekulativen technologischen Fähigkeiten normalisiert werden; dass Prototypen routinemäßig in realen Konflikten erprobt werden; dass krisenbedingte Dringlichkeit demokratische Grundwerte untergräbt und dass ethische Grenzen marginalisiert werden.

Krieg ist eine schreckliche Tragödie für diejenigen, die ihn am eigenen Leib erleben. Wenn die neuen Dynamiken aus dem Silicon Valley bedeuten, dass Krieg zur finanziellen Chance werden kann, dann ist der Interessenskonflikt offensichtlich. Es ist eine grundlegende Aufgabe der Politik, diesen Konflikt klar im Blick zu behalten.

Der digitale Staat

Regierungen setzen bei öffentlichen Dienstleistungen immer häufiger auf private Tech-Unternehmen. Das muss kein Problem sein: Kontrollierte Abhängigkeit kann den Staat sogar leistungsfähiger machen.

Von Daniel Castro

Wenn ein Bürger online eine Steuererklärung abgibt, Sozialleistungen beantragt, einen Pass erneuert oder sich mit einer digitalen Identität ausweist, scheint es, als fände der Austausch allein zwischen Bürger und Staat statt. Immer häufiger stehen jedoch private Technologieunternehmen dahinter. Sie stellen Cloud-Infrastruktur, Software, Daten und andere Technologien bereit, auf die öffentliche Dienstleistungen angewiesen sind.

Diese Konstellation wirft eine grundlegende Frage zur staatlichen Macht auf: Was geschieht, wenn private Unternehmen die Fähigkeiten kontrollieren, die Bürger im Umgang mit dem Staat benötigen? Eine Regierung kann Fähigkeiten hinzugewinnen, indem sie sich auf einen spezialisierten privaten Anbieter stützt. Sie kann aber auch Handlungsfreiheit einbüßen, wenn sie an einen Anbieter gebunden ist, zu dem es keine glaubwürdige Alternative gibt.

Diese Unterscheidung ist wichtig, weil die europäische Politik Abhängigkeit an sich verstärkt als Souveränitätsproblem betrachtet, vor allem wenn ein Anbieter seinen Sitz außerhalb der EU hat. Dabei ist die Abhängigkeit vom Privatsektor kaum neu, und ausländischer Besitz bedeutet nicht automatisch ausländische Kontrolle.

Was Zensus und Cloud verbindet

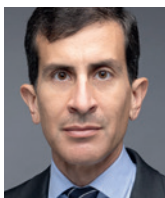
Regierungen stützen sich seit Langem auf private Unternehmen, wenn es um Infra-

struktur, Technologie und Fachwissen geht, deren interne Entwicklung kostspielig oder unpraktisch wäre.

Das US Census Bureau (Volkszählungsbehörde) liefert ein frühes Beispiel dafür, wie Regierungen mit der Abhängigkeit von spezialisierter privater Technologie umgehen können. Nachdem die Volkszählung von 1880 die bestehenden Methoden der Datenverarbeitung überfordert hatte, schrieb die Behörde 1888 einen Wettbewerb für ein mechanisches System aus, das die Auswertung automatisieren sollte. Das System von Herman Hollerith setzte sich durch, und die Behörde mietete seine Maschinen für die Volkszählung von 1890. Die Technologie beschleunigte die Auszählung erheblich: Sie war Monate vor dem geplanten Termin und zu deutlich geringeren Kosten als erwartet abgeschlossen. Als Hollerith später seine Preise erhöhte, entwickelte das Census Bureau ein eigenes, konkurrierendes Auswertungssystem.

Die Lehre daraus: Privates Fachwissen kann staatliche Kapazitäten stärken, vorausgesetzt, die Regierung behält die Möglichkeit umzusteuern, falls die Beziehung zu kostspielig wird.

Cloud-Computing überträgt diese Dynamik in die Gegenwart. Hyperscaler können enorme Fixkosten auf Millionen von Kunden verteilen, globale Netzwerke betreiben, kontinuierlich in Cybersicherheit investieren und Spezialisten beschäftigen, die Regierungen nur schwer



Daniel Castro ist Präsident der Information Technology and Innovation Foundation (ITIF), einem gemeinnützigen Thinktank für Wissenschafts- und Technologiepolitik.

anwerben und halten könnten. Der Einkauf dieser Dienstleistungen kann Regierungen daher Fähigkeiten verschaffen, die sie selbst nicht effizient nachbilden könnten. Problematisch wird es jedoch, wenn Anbieter zu tief in die Systeme eingebettet sind, auf die sich der Staat stützt und die sich kaum noch ersetzen lassen.

Wer von wem abhängig ist

Vier Dimensionen bestimmen Art und Gewicht der Abhängigkeit einer Regierung von einem Technologieanbieter.

Technische Spezialisierung liegt vor, wenn ein Anbieter über Fähigkeiten verfügt, die ein Staat nur schwer oder mit hohen Kosten selbst aufbauen könnte. Marktkonzentration spielt eine Rolle, wenn nur wenige Anbieter diese Fähigkeiten bereitstellen können. Netzwerkintegration entsteht, wenn Regierungssysteme tief in das Ökosystem miteinander verbundener Technologien und Dienstleistungen eines Anbieters eingebettet sind, sodass Änderungen an einem System von anderen abhängen. Und rechtliche Risiken entstehen, wenn eine Regierung auf ein Unternehmen angewiesen ist, das den Gesetzen oder geopolitischen Zwängen eines anderen Staates unterliegt.

Diese Dimensionen können sich gegenseitig verstärken: Technische Vorteile können zu Marktkonzentration führen, Konzentration kann die Wechselkosten erhöhen, und eine tiefe Netzwerkintegration kann diese Kosten weiter in die Höhe treiben. Unterliegt der Anbieter ausländischem Recht, kommt ein zusätzliches Risiko hinzu. So mag eine Regierung rechtlich frei sein, den Anbieter zu wechseln, und dennoch vor erheblichen praktischen Hindernissen stehen.

Nichts davon setzt voraus, dass sich ein Anbieter schlecht verhält. Abhängigkeit kann aus rationalen Entscheidungen

*Problematisch wird es,
wenn private Tech-Anbieter zu tief in staatliche Systeme eingebettet sind*

von Behörden entstehen, die bessere Technologie, mehr Sicherheit, niedrigere Kosten oder Fähigkeiten anstreben, deren Eigenentwicklung unpraktikabel wäre. Die politische Herausforderung besteht darin, sicherzustellen, dass die Abhängigkeit den Staat nicht darin einschränkt, seine Technologieanbieter auszuwählen, zu beaufsichtigen oder zu wechseln.

Hier unterscheidet sich Abhängigkeit von Interdependenz. Abhängigkeit beschreibt eine asymmetrische Beziehung, in der eine Partei die andere benötigt und nur wenige Alternativen hat. Interdependenz meint hingegen ein Verhältnis, in dem beide Parteien großen Nutzen aus der Zusammenarbeit ziehen und beiden erhebliche Kosten entstünden, sollte diese zusammenbrechen.

So sind europäische Regierungen bei bestimmten digitalen Fähigkeiten von amerikanischen Technologieunternehmen abhängig, während diese Unternehmen ihrerseits auf europäische Kunden, Arbeitskräfte, Lieferanten, Kapital und Märkte angewiesen sind. Diese Interdependenz beseitigt zwar nicht das Machtungleichgewicht, stellt aber die Annahme infrage, dass ausländischer Besitz automatisch ausländische Kontrolle bedeutet. Entscheidend ist, wie viel Handlungsfreiheit Regierungen behalten, wenn sich die Beziehung verändert.

Resilienz ist nicht alles

Regierungen haben gute Gründe, Wert auf Resilienz zu legen. Ein kritischer

öffentlicher Dienst sollte weiter funktionieren, wenn ein Anbieter Opfer eines Cyberangriffs wird, länger ausfällt, geopolitischen Beschränkungen unterliegt oder aus anderen Gründen nicht mehr verfügbar ist.

Doch Resilienz ist nur eines von mehreren Zielen der öffentlichen Beschaffung. Regierungen müssen auch Kosten, Leistung, Cybersicherheit, Zuverlässigkeit, Innovation, technische Fähigkeiten, Skalierbarkeit und die Qualität ihrer Dienstleistungen berücksichtigen. Ein ausschließlicher Fokus auf geopolitische Resilienz birgt eigene Risiken: Eine Regierung könnte sich für ein weniger innovatives, weniger sicheres, weniger leistungsfähiges oder teureres System entscheiden, nur weil es die Abhängigkeit vom Ausland verringert. Darunter würde auch die Zufriedenheit der Bürger mit ihrer öffentlichen Verwaltung leiden.

Das politische Ziel sollte daher eine Art kontrollierte Abhängigkeit sein. Regierungen müssen ihre wirklich kritischen Systeme identifizieren, genug eigenes Fachwissen vorhalten, um Anbieter zu überwachen, Datenportabilität und Interoperabilität gewährleisten, Migrations- und Notfallpläne testen und unnötige Konzentrationen vermeiden.

Europas Cloud-Dilemma

Brüssel betrachtet diese Fragen vermehrt unter dem Gesichtspunkt der digitalen Souveränität. Die Europäische Kommission definiert technologische Souveränität unter anderem als Entwicklung und Kontrolle von Schlüsseltechnologien, Daten und Infrastruktur bei gleichzeitiger Verringerung der Abhängigkeit von Anbietern außerhalb der EU. Ihr Cloud and AI Development Act sieht einen gemeinsamen EU-Rahmen zur Bewertung der Cloud-Souveränität sowie einen

Beschaffungsmechanismus für den öffentlichen Sektor vor, der Europas Position im Cloud-Computing stärken soll.

Der Abbau bestimmter Abhängigkeiten kann sinnvoll sein. Europäischer Besitz ist jedoch kein verlässlicher Indikator für Sicherheit oder Widerstandsfähigkeit.

Außerdem steht dieser Ansatz im Widerspruch zu den Grundprinzipien des öffentlichen Beschaffungswesens. Das WTO-Übereinkommen über das öffentliche Beschaffungswesen verpflichtet die Vertragsstaaten, Lieferanten aus anderen Vertragsstaaten Inländerbehandlung und Nichtdiskriminierung zu gewähren, vorbehaltlich ausgehandelter Geltungsbereiche und Ausnahmen. Das Übereinkommen hält ausdrücklich fest, dass Beschaffungsvorschriften nicht dem Schutz inländischer Lieferanten dienen sollten. Auch das EU-Vergaberecht verlangt Gleichbehandlung, Nichtdiskriminierung, Transparenz und Verhältnismäßigkeit.

Europäischer Besitz ist kein verlässlicher Indikator für Sicherheit oder Widerstandsfähigkeit

Diese Regeln existieren aus guten Gründen. Inländische Anbieter unabhängig von ihrer Leistung zu bevorzugen, kann den Wettbewerb einschränken, die Kosten erhöhen und Innovationsanreize schwächen. Sicherheitsausnahmen erlauben es Regierungen, technische und rechtliche Anforderungen zu stellen, wenn Systeme echte sicherheits- oder geopolitische Risiken bergen. Diese Anforderungen sollten direkt am Risiko ansetzen, statt davon auszugehen, dass ein

europäischer Anbieter per se sicherer oder widerstandsfähiger ist als ein außer-europäischer.

Europas eigene Politik ist Ausdruck dieser Spannung. Der Bericht über den Stand der digitalen Dekade 2025 stuft die Abhängigkeit von Nicht-EU-Anbietern bei Cloud-Diensten und anderer digitaler Infrastruktur als strategische Abhängigkeit ein. Zugleich nennt er unzureichende Investitionen, fragmentierte Märkte, regulatorische Komplexität und einen Mangel an fortgeschrittenen digitalen Kompetenzen als Hindernisse für Europas technologische Entwicklung. Ein geschützter heimischer Cloud-Markt würde diese Probleme nicht automatisch lösen und könnte genau den Wettbewerbsdruck verringern, der die Hyperscaler überhaupt erst attraktiv gemacht hat.

Hin zu praktischer Autonomie

Ein besserer Ansatz zielt auf die Mechanismen ab, die gewöhnliche in übermäßige Abhängigkeit verwandeln. Das EU-Datengesetz liefert ein Beispiel: Es verpflichtet Cloud-Anbieter, Anbieterwechsel sowie Daten- und Anwendungsportabilität zu erleichtern; Wechsel- und Datenausgangsgebühren sollen ab Januar 2027 wegfallen.

Regierungen sollten bei der Beschaffung den gesamten Lebenszyklus im Blick behalten: Ein niedriger Anfangspreis kann hohe Migrationskosten verbergen; eine technisch hervorragende Plattform kann problematisch werden, wenn dem Staat das erforderliche Fachwissen verloren geht, um sie zu beaufsichtigen oder zu ersetzen; und ein einzelner Anbieter kann zur systemischen Schwachstelle werden. Regierungen müssen lernen, Anbieterabhängigkeit, Datenrechte, Lebenszyklusrisiken, Konzentration und Kontinuität gezielt zu steuern.

Ziel sollte sein, sich Optionen offenzuhalten. Das kann bedeuten, einen ausländischen oder inländischen Anbieter zu wählen, mehrere Anbieter zu nutzen oder kritische Infrastruktur selbst zu betreiben. Entscheidend ist, ob die gewählte Lösung der Regierung die benötigten Fähigkeiten, Sicherheit, Leistung und Widerstandsfähigkeit zu vertretbaren Kosten bietet.

Private Unternehmen werden ein fester Bestandteil des modernen Staates bleiben, zumal wesentliche technologische Fortschritte nach wie vor aus dem Privatsektor kommen. Das entspricht der üblichen technologischen Spezialisierung und Wirtschaftsorganisation. Die Frage für demokratische Regierungen lautet, ob diese Abhängigkeit ihre Handlungsfähigkeit stärkt oder einschränkt. Souveränität hängt letztlich von praktischer Handlungsfreiheit ab – nicht nur davon, Regeln festzulegen, kritische Systeme zu überwachen und den Kurs zu ändern, sondern auch von der Fähigkeit, Probleme tatsächlich zu lösen und für die Bürger Ergebnisse zu liefern. Ein Staat, der sich im Namen geopolitischer Unabhängigkeit selbst die Hände bindet, verspielt diese praktische Autonomie.

Europa sollte digitale Infrastruktur daher eher an der operativen Handlungsfreiheit messen, die sie bietet, als an der Unternehmensidentität ihrer Anbieter. Strenge Sicherheitsanforderungen, interoperable Standards, eigenes Fachwissen und leistungsorientierte Beschaffung erlauben es Regierungen, staatliche Kapazitäten mit privater Innovation zu verbinden. So können sie das Potenzial des Privatsektors voll ausschöpfen, ohne die Kontrolle über ihre eigenen Entscheidungen aus der Hand zu geben.

Übertragen aus dem Englischen von T. Hofmann **IP**