Süddeutsche Zeitung

DIE WELT BESSER VERSTEHEN MIT DEUTSCHLANDS GROSSER TAGESZEITUNG

# Süddeutsche Zeitung
## LANGSTRECKE

SONDERAUSGABE IN ZUSAMMENARBEIT MIT TELEKOM DEUTSCHLAND
SZ.DE/LANGSTRECKE #LANGSTRECKE



Sonderausgabe

**Digitale Souveränität**

Die besten Reportagen, Essays und Interviews zum Thema

### Cloud, KI und Cybersicherheit

Wie Europa technologisch selbstbestimmter wird

### Souveränität als Bilanzfrage

Warum digitale Abhängigkeit teurer ist als gedacht

### Resilienz im Dauerfeuer

Cyberabwehr bei der Telekom, Siemens und Paypal




Mirjam Hauck und Helmut Martin-Jung erklären, wie Europa digital resilienter werden kann
SEITE 4

Max Muth über Karsten Wildbergers wichtigste Maßnahmen als Deutschlands Chefdigitalisier
SEITE 9

Lisa Nienhaus spricht mit der Ökonomin Francesca Bria über das richtige Rezept gegen USA und China
SEITE 12

Joscha F. Westerkamp über das Gesetzespaket der EU für weniger technologische Abhängigkeit
SEITE 16

Bastian Mühling, Vivienne Timmler und EU-Digital-kommissarin Henna Virkkunen im Gespräch
SEITE 19

Helmut Martin-Jung über Quantencomputer und welche Chancen sie Deutschland bieten
SEITE 24

Helmut Martin-Jung hat das erste reine KI-Rechen-zentrum Deutschlands besucht
SEITE 29

Caspar Busse spricht mit Infineon-Chef Jochen Hanebeck über den KI-Boom
SEITE 32

Bastian Mühling lässt sich von Thomas Lippert Europas ersten Exascale-Rechner Jupiter erklären
SEITE 36

SCHWERPUNKT

## Digitale Souveränität

Vom Wow zum Wert – Vorwort von Rodrigo Diehl
SEITE 42

Lars Neumann über die Cloud und Zahlen, die ihn nachdenklich stimmen
SEITE 43

Klaus Werner im Interview über die Relevanz der CFO-Perspektive
SEITE 46

Was digitale Souveränität für Oliver Lauer bedeutet
SEITE 48

Thomas Tschersich hat Antworten auf die neue Art von Bedrohungen
SEITE 49

Was digitale Souveränität für Harald Welzer bedeutet
SEITE 53

Niklas Horstmann erklärt, wo die ideale Cyber-abwehr beginnt
SEITE 54

Was digitale Souveränität für Hendrik Wüst bedeutet
SEITE 57

Stimmen von der Digital X in Köln
SEITE 58

Alexandra Föderl-Schmid über Frankreichs Bemühungen für mehr digitale Unabhängigkeit
SEITE 60

Gabriel Rinaldi erklärt, wie Staat und Sozialträger digital vernetzt werden können
SEITE 64

Matthias Punz spricht mit zwei De-Cix-Managern über die Sicherheit von Internet-Knotenpunkten
SEITE 67

Zwei SZ-Autoren erfahren von BSI-Chefin Claudia Plattner einige Details zum Cyberdome
SEITE 71

Natalia Oropeza erläutert zwei SZ-Autoren, wie sich Siemens gegen Cyberattacken verteidigt
SEITE 75

Gabriel Rinaldi erfährt von Shaun Khalfan, warum er Paypal von KI-Modellen angreifen lässt
SEITE 81

Michael Moorstedt und Medienwissenschaftler Martin Andree über China als Vorbild
SEITE 84

Urs Gasser erklärt Thomas Kirchner, wie KI-Modelle reguliert und kontrolliert werden können
SEITE 88

Expertin Antonia Hmaidi im SZ-Interview über globale Regulierung und KI als Machtmittel
SEITE 93

Helmut Martin-Jung hat herausgefunden, was die Forschung zu Europas Souveränität beitragen kann
SEITE 98

Elisabeth Dostert und Helmholtz-Präsident Martin Kel-ler über eine neue Kultur des Machens
SEITE 101

# Warum Europas Tech-Abhängigkeit so riskant ist

*Rechenzentren in Brandenburg, Open Desk statt Microsoft Office, doch bei Servern und Chips endet oft die Souveränität. Was Deutschland und Europa tun können, um digital resilienter zu werden.*

VON
MIRJAM HAUCK UND
HELMUT MARTIN-JUNG





Zeitenwende, geopolitische Verwerfungen – Deutschland muss umdenken, wenn es darum geht, Technologien zu verwenden: „Wir dürfen im Auto nicht auf dem Rücksitz sitzen und hoffen, dass der Fahrer in die richtige Richtung fährt." Sinan Selen hat das gesagt, der Präsident des deutschen Inlandsgeheimdienstes. Was er damit meint, ist klar: Deutschland und auch Europa nutzen zwar Technologien ziemlich intensiv, etwa bei Cloud-Diensten. Das Speichern und Verarbeiten großer Datenmengen wird dabei aber in externe Rechenzentren verlagert.

Wohin die Richtung dabei geht, wie sie ausgestaltet wird, darüber jedoch können die Passagiere auf der Rücksitzbank nur begrenzt mitbestimmen. Und was, wenn es plötzlich heißt: Aussteigen? US-Firmen kontrollierten 70 Prozent der Infrastruktur für die Clouds, sagte Ökonomin, Digitalexpertin und Initiatorin der Eurostack-Initiative Francesca Bria auf dem SZ-Digitalgipfel 2026. Was passiert, wenn die USA ihre Vorherrschaft auf diesem Gebiet nutzen, um Druck auszuüben? Stehen dann die Firmen hierzulande still? Haben die Vereinigten Staaten die Macht, um Europa auseinanderzudividieren? Wenn sie mit welcher Legitimation auch immer auf Daten zugreifen, die EU-Unternehmen oder Behörden gespeichert haben?

Sorgen wie diese treiben Firmen in Deutschland vermehrt um, seit in den USA Donald Trump zum zweiten Mal zum Präsidenten gewählt wurde. Und dieses Mal geht es nicht nur, wie viele bei seiner ersten Amtszeit gehofft hatten, um eine vorübergehende Episode. Im Raum steht ein grundsätzlicher Politikwandel in den Vereinigten Staaten. Washington betrachtet Europa nun als wirtschaftlichen wie auch als politischen Konkurrenten.

Als der deutsche Branchenverband Bitkom Anfang des Jahres 2026 wissen wollte, welche Anbieter von Cloud-Diensten man bevorzuge, antworteten die Befragten einstimmig: deutsche. Irene Bertschek, Leiterin „Digitale Ökonomie" am Leibniz-Zentrum für Europäische Wirtschaftsforschung und Vorsitzende der Expertenkommission Forschung und Innovation der Bundesregierung, berichtete auf dem SZ-Digitalgipfel über Befragungen, die sie bei deutschen Unternehmen gemacht hat. So sei bei ihnen das Gefühl der Abhängigkeit in den vergangenen Jahren gestiegen. „Etwa die Hälfte der Unternehmen fühlt sich abhängig von ausländischen Anbietern, insbesondere im Bereich KI und Software." Und zwar größere Unternehmen stärker als kleinere. Ihre Annahme dazu: „Die größeren sind sich eher der Gefahren oder der Vulnerabilität bewusst."

Diesen Wunsch nach digitaler Souveränität spüren folglich auch die Anbieter von Cloud-Diensten aus Deutschland und Europa wie Nextcloud, die nun überrannt werden von Anfragen, weil Unternehmen erkannt haben, dass wichtige Unternehmensdaten wie geistiges Eigentum besser bei europäischen Anbietern liegen sollten. „Wir haben bisher oft an IT-Manager, an Security-Leute verkauft, aber seit einigen Monaten ruft bei uns auch die C-Level-Ebene an", sagte Frank Karlitschek, Gründer und Vorstandschef von Nextcloud.

WENN EINEM RICHTER DAS DIENSTLICHE E-MAIL-KONTO GESPERRT WIRD

Die Hyperscaler, wie die großen US-Cloud-Firmen Amazon Web Services, Microsoft Azure und Google Cloud genannt werden, rücken allerdings mit gewaltigen Marketingbudgets und entsprechender Dominanz an. Hiesige Unternehmen ver-

suchen, dem Trend mit rechtlichen Konstrukten entgegenzutreten, bieten sogenannte EU-Clouds an. Und da sehen sich die Befürworter einer größeren Souveränität bestätigt durch einen Fall am Internationalen Gerichtshof. Einem der Richter wurde aufgrund von US-Sanktionen 2025 das dienstliche E-Mail-Konto gesperrt, das bei Microsoft lag. Im Herbst 2025 beschloss der Gerichtshof daraufhin, auf das System Open Desk umzustellen – ein Softwarepaket aus Deutschland.

Innerhalb der Branche ist klar, dass spätestens bei der Hardware Schluss ist mit voller Souveränität, dass es für viele Bereiche Partnerschaften mit Firmen aus Amerika und Asien braucht. Die Server oder zumindest die Bauteile für die Rechenzentren kommen überwiegend aus den USA oder China; die verschiedenen Chips, die darin stecken, meist aus Taiwan, China, Korea oder den USA. Zwar gibt es Firmen wie Infineon, aber auch der größte Chiphersteller Europas hat für seine Wertschöpfungskette Standorte in Europa, den USA und Brasilien.

Damit zumindest die Souveränität bei Software klappt, setzen viele Unternehmen mittlerweile auf Open-Source-Programme, also Software, deren für Menschen lesbare Quelltexte offenliegen. Solche Software wird oft ohne Lizenzkosten abgegeben, die Hersteller verdienen in der Regel an Dienstleistungen wie Wartung oder Betrieb der Software. Ihr großer Vorteil: Man ist nicht an einen Hersteller wie Microsoft gebunden.

Fällt der aus, oder entwickelt der die Software in einem Sinn weiter, der einem Kunden nicht gefällt, können andere Firmen oder kundige Kunden selbst die Software in ihrem Sinne weiterentwickeln. Im Koalitionsvertrag hat sich die Bundesregierung dazu bekannt, verstärkt auf Open Source zu setzen, um die Abhängigkeit von Behörden von Nicht-EU-Anbietern zu verringern. Erreicht werden soll das durch den sogenannten Deutschland-Stack. Gemeint ist mit diesem Begriff aus der Software-Branche (Stack ist wörtlich: Stapel) ein Paket souveräner Software-Lösungen auf allen technischen Ebenen für Bundesbehörden und die Verwaltung.

Die Umsetzung kommt aber nur schleppend voran. Und so beklagt die Open Source Business Alliance (OSBA), in der sich mehr als 250 Unternehmen zusammengeschlossen haben, dass die Regierung bei ihren Absichtserklärungen zu viele Schlupflöcher für sogenannte Closed-Source-Angebote offen lasse, besonders für außereuropäische Hyperscaler. Digitale Souveränität werde so für den Deutschland-Stack unerreichbar. Und das könnte dramatische Folgen haben: „Wer den Deutschland-Stack abschalten kann, kann Deutschland abschalten“, warnt der Verband.

DIE VORREITER-ROLLE AUF LÄNDEREBENE HAT SCHLESWIG-HOLSTEIN ÜBERNOMMEN

In einigen Bundesländern oder auch Kommunen ist man schon weiter. Die Vorreiterrolle auf Länderebene hat Schleswig-Holstein übernommen. 80 Prozent der Arbeitsplätze in der öffentlichen Verwaltung sind dort auf eine Open-Source-Office-Lösung umgestellt. Am Rest wird gearbeitet, dabei muss unter anderem Software nachprogrammiert werden, damit sie auf dem quelloffenen Betriebssystem Linux läuft. Das Land hat damit 15 Millionen Euro an Lizenzkosten eingespart, allerdings auch neun Millionen Euro für die Umstellung ausgegeben.

Das Gute: Wenn etwas programmiert ist, können es auch Verwaltungen anderer Länder nutzen und müssen ebenfalls keine Lizenzgebühren zahlen.







Auch die Stadt München hat sich mittlerweile dem Grundsatz „public money, public code“ verpflichtet, also dass öffentliche Gelder in offene Software fließen sollen. Viele digitale Dienstleistungen basieren dort mittlerweile auf Open-Source-Software.

Wie aber lässt sich solche freie Software oder eben Technologie „Made in Germany“ oder in Europa entwickeln? Wie lassen sich die Talente hier halten, wie kann man hierzulande mit den ökonomischen Bedingungen des Silicon Valley überhaupt konkurrieren?

Die Schwarz-Gruppe finanziert mit ihrer Stiftung beispielsweise in Heilbronn einen Bildungscampus, der bereits 8000 Studierende hat und mittelfristig auf 20 000 anwachsen soll. An der Hochschule lassen sich etwa Abschlüsse von der TU München und der ETH Zürich erwerben. Zusammen mit dem auch vom Land Baden-Württemberg geförderten KI-Park soll für Start-ups ein attraktives Ökosystem aufgebaut werden. So könnten auch in Deutschland und Europa neue Tech-Eliten entstehen, die wichtig sind, um das Ziel der digitalen Souveränität zu erreichen.



ERSCHIENEN IN DER SZ VOM 04.03.2026



***„Der KI-Zug ist zwar aus dem Bahnhof, aber noch einzuholen“***

Karsten Wildberger ist seit dem Frühjahr 2025 Deutschlands Chefdigitalisierer. Auf dem SZ-Digitalgipfel mahnt er zu mehr Tempo bei künstlicher Intelligenz, betont aber, dass digitale Souveränität auch Partner braucht.

VON
MAX MUTH

Es ist so, als wäre Karsten Wildberger wirklich da. Also in echt. Man muss das dazu sagen, weil normalerweise aus der Ferne zugeschaltete Gäste – neudeutsch remote – auf Konferenzen eine Zumutung sind. Verkraftbar, wenn es sich um den geflüchteten Edward Snowden nach den NSA-Enthüllungen oder anderweitig schwer zu bekommende Gäste handelt, aber ansonsten eine Zumutung.

Diesmal ist das anders, und es ist sehr passend, weil sich der deutsche Digitalminister auf dem Digitalgipfel der Süddeutschen Zeitung zugeschaltet hat. Noch wichtiger für die Güte der Verbindung ist aber vermutlich, von wo der Herr Minister sich meldet, nämlich vom Mobile World Congress in Barcelona, also dem weltweiten Klassentreffen der Netzbetreiber. Vielleicht wollten die auch nur zeigen, wo der Hammer hängt, ein bisschen angeben mit Bandbreiten und Latenzen. Es ist gelungen.

Wenn man davon absieht, dass Wildberger immer ein bisschen schräg über das Publikum im Münchner Veranstaltungszentrum Macherei schaut, vermutlich, weil da in Barcelona sein Bildschirm ist, dann ist der digitale Minister vielleicht sogar dem analogen vorzuziehen. Keine extra Sicherheitsvorkehrungen, kein Personenschutz, dennoch wichtige Botschaften und ein paar nonverbale Signale, die man sonst vielleicht übersehen hätte. Denn wenn der Mann richtig groß auf der Leinwand zu sehen ist, dann sieht man jede Gefühlsregung, die vor allem bei den Fragen der Moderatorinnen viel verraten. Als SZ-Chefredakteurin Judith Wittwer den Digitalminister als einen „Tech-Nerd“ tituliert, da lächelt der übergroße Minister, allerdings auch ein bisschen gequält.

„Ja, so ist das in Deutschland“, sagt er dann. „Wenn man sich ein bisschen für Technik interessiert, dann ist man der Tech-Nerd.“ Der frühere Manager würde das gerne ändern, das merkt man ihm in den kommenden 20 bis 25 Minuten auf der Bühne an. Leicht ist es nicht. Wildberger hat im Frühjahr 2025 ein leeres Ministerium übernommen, mit sieben Mitarbeitern begonnen. Mittlerweile kümmern sich immerhin 550 Menschen um die ministeriellen Geschäfte. Fortschritt. Zumindest personell. Wildberger ist so etwas wie der Change Manager für die Deutschland GmbH. Und wer schon mal am anderen Ende eines Change-Prozesses saß, der weiß: Change macht selten Spaß. Und nur die wenigsten werden gerne gechanged.

Wildberger nutzt also den Auftritt für einen kurzen Ritt durch die Projekte, die er auf Deutschlands Weg in die digitale Souveränität für am wichtigsten hält. Und schon die Auswahl verrät einiges. Der „Deutschland-Stack“ beispielsweise soll das Betriebssystem der Verwaltung dieses Landes werden. Wer für die Verwaltung entwickelt, tut dies demnächst nach gemeinsamen, offenen Standards, was etwa dazu führen sollte, dass Dinge nicht mehr 16-mal programmiert werden, sondern nur noch einmal. Zum Deutschland-Stack gehört aber nicht nur die Verwaltung selbst, sondern auch die Cloud-Infrastruktur und Apps, die digitale Fachverfahren einfacher und schneller machen sollen.

Der Deutschland-Stack klingt gut, aber auch wie eine Idee, die man mal vor 20 Jahren gehabt haben könnte. Hatten einige auch, aber irgendwie ging im Austausch zwischen den Ministerien der Drive verloren. Vielleicht ändert das ja nun das Spezialministerium mit dem Seiteneinsteiger-Minister. Für den Bürger interessanter ist vermutlich Projekt Nummer zwei: die digitale Brieftasche, in der jetzt aber wirklich bald Personalausweise, Führerscheine und andere hoheitliche Dokumente hinterlegt werden sollen. Aber nicht als Selbstzweck, sondern für digitale Amtsgeschäfte, für die sich die Deutschen künftig den Weg zum Bürgeramt sparen können. Auch das klingt erstrebenswert, man glaubt es aber erst, wenn man es sieht.

WO IST DAS
DEUTSCHE GOOGLE,
DAS DEUTSCHE PAYPAL,
DAS DEUTSCHE
OPEN AI?

Deutlich aktueller als die Versuche, Deutschland zu digitalisieren, sind die Gründe, warum sich vielleicht diesmal wirklich etwas tut. Donald Trump hat die Verbündeten im vergangenen Jahr das Fürchten gelehrt. Souveränität, auch die digitale, ist auf einmal nicht mehr nice to have, sondern wichtig bis überlebensnotwendig. Interessant ist deshalb der Kontext, mit dem Wildberger die Frage nach Souveränität





kontert. Ja, es sei erschreckend gewesen, dass technologische Fähigkeiten nun als Machtinstrument verwendet werden. Aber mindestens ebenso interessant sei für ihn, dass Deutschland in den vergangenen 20 Jahren an der Wertschöpfung in der Branche nicht teilgenommen habe. Übersetzt: Wo ist das deutsche Google, das deutsche Paypal, das deutsche Open AI? „Und daran wollen wir arbeiten“, sagt Wildberger. Nicht Gefahren betonen, sondern Chancen, am besten wirtschaftliche. Vielleicht kriegt man so den deutschen Mittelstand dazu, sich zumindest an der nächsten Technologierevolution zu beteiligen.

„MAN KANN
BEIDES TUN.
OPTIMIST SEIN, ABER
RISIKEN SEHEN.“

Besonders relevant sei die Wertschöpfung nämlich jetzt bei künstlicher Intelligenz (KI). „Der KI-Zug ist zwar aus dem Bahnhof, aber noch einzuholen.“ Man könnte einwenden, „aus dem Bahnhof“ sei eigentlich synonym für „abgefahren“, aber sei's drum, was muss, das muss. Denn KI habe stärker als andere Technologien eingebettete Werte, es sei deshalb absolut notwendig, eine europäische Version davon zu bauen. „Europäisch“ versteht Wildberger hier etwas weiter, so sollen etwa Partnerschaften mit Ländern wie Kanada, Spanien und Indien helfen, die Lücke zu den Leuten vorn im Zug, den USA und China, zu schließen.

Bei der Frage, ob sein auffälliger Optimismus bezüglich der Chancen bei Technologie auf den Rest der Deutschen schon irgendeinen Effekt hatte, lohnt sich wieder die große Leinwand auf der Bühne. „Man kann beides tun. Optimist sein, aber Risiken sehen“, sagt Wildberger mit einem vielsagenden Lächeln. Insbesondere bei KI sei beides wichtig. Chancen und Risiken gleichzeitig zu sehen, erzeugten immer Widersprüche, was für viele schwer auszuhalten sei. Gerade bei der KI werde es aber nicht funktionieren, sich nur auf eines zu konzentrieren. Denn die Technologie werde auf dem Arbeitsmarkt sicher zu Verwerfungen führen. Mehr Leistung mit weniger Menschen, da ist es nicht schwer, sich auszurechnen, was mit einigen Jobs passieren dürfte. Auch Cybersicherheit sei betroffen, wenn massenhaft autonome Agenten unterwegs seien. Deshalb die Chancen zu ignorieren, sei allerdings genauso fahrlässig.

Deutschland und seine Partner müssen also bei KI aufholen, und das so schnell wie möglich. Denn „das Schlimmste, was ich mir vorstellen kann, ist, dass wir Kunde werden von dieser Technologie mit einer Abhängigkeit, die uns nicht mehr erlaubt, selber zu gestalten.“ Wildberger betont jedoch, der Change-Prozess für mehr Souveränität ende nicht morgen und auch nicht übermorgen. Aber die Arbeit müsse jetzt beginnen, sonst werde die aktuelle digitale Abhängigkeit irreversibel.

ERSCHIENEN IN DER SZ VOM 03.03.2026

# „In Italien sagen wir: Europa hat alle Zutaten, aber das Rezept ist falsch“

Ob auf dem Handy oder dem Computer: 80 Prozent der Technologie kommt aus Ländern wie China oder den USA. Die Ökonomin Francesca Bria will das ändern. Sie hat einen Plan, Hoffnung – und konkrete Tipps.

Interview von
Lisa Nienhaus





Francesca Bria zu einem Interview zu bekommen, ist ungefähr so, als wollte man einen Wirbelsturm an einer Stelle festhalten, um ihn mal in Ruhe zu betrachten. Schwierig. Sie reist durch Europa, spricht auf Konferenzen, berät die Politik. Auch beim Digitalgipfel der Süddeutschen Zeitung ist sie auf der Bühne dabei. Doch am Ende gelingt es. Die Ökonomin ist am Telefon und nimmt sich eine Stunde Zeit, über ihre Idee zu diskutieren: wie Europa digital unabhängig von den USA und China werden kann.

**SZ: Frau Bria, wenn Sie auf Ihr eigenes Handy schauen: Wie viele der Apps darauf bleiben übrig, wenn Sie die amerikanischen und chinesischen löschen müssten?**

*Francesca Bria:* Sehr, sehr wenige. Es fängt damit an, dass das Handy selbst ein US-Produkt ist und sein Betriebssystem ebenfalls.

**Haben Sie eine Prozentzahl für mich?**

Ich weiß es nicht genau für mein Gerät, aber generell gilt: 80 Prozent unserer Technologie ist importiert. Ich benutze mittlerweile teils gezielt europäische Software, zum Beispiel für Mails oder zum sicheren Chatten. Gestern bin ich Eurosky beigetreten, einem neuen sozialen Netzwerk. Kennen Sie das?

**Nein.**

Das ist ähnlich wie Bluesky, nur von europäischen Entwicklern, die auch europäische Server nutzen und europäischen Datenschutz einhalten. Ich nutze auch europäische Clouds. Ich gebe mir also Mühe, aber es bleibt wahr: Amerikanische Firmen kontrollieren 70 Prozent der Infrastruktur für die Clouds. Wir importieren 80 Prozent unserer Computerchips aus Taiwan. Wir haben keine Kontrolle über die Infrastruktur, auf der unsere öffentliche Sicherheit beruht. Und amerikanische Firmen müssen den US-Behörden Daten geben, sogar wenn diese in Frankfurt oder München gespeichert sind. Ob Krankenhäuser, Schulen oder Verwaltung: Wenn die Daten in amerikanischer Infrastruktur gesichert sind, sind sie nicht deine.

**Lange hat das nur wenige gestört. Das hat sich geändert, als Donald Trump den Europäern Grönland entreißen wollte. War das ein Wendepunkt?**

Ja, wir sehen sogar ganz praktische Folgen. Dänemarks Digitalministerin ist gerade dabei, Microsoft Office von den öffentlichen Computern zu verbannen und auf Open-Source-Alternativen umzusteigen. Auch ein deutsches Bundesland (Schleswig-Holstein, Anmerkung der Redaktion) will jetzt Open-Source-Software in der Verwaltung nutzen. Die politische Aufmerksamkeit ist nun sehr viel höher. Auch für die Eurostack-Initiative, die ich angestoßen habe, um die europäische digitale Unabhängigkeit voranzubringen. Die deutsche Regierung hat uns sogar im Koalitionsvertrag erwähnt. Aber: Das Problem zu verstehen, ist etwas anderes als zu handeln.

„WIR HABEN KEINE KONTROLLE ÜBER DIE INFRASTRUKTUR, AUF DER UNSERE ÖFFENTLICHE SICHERHEIT BERUHT.“

**Und jetzt müsste man handeln?**

Absolut. Man muss sich nur die geopolitische Lage ansehen. Die USA haben ihre Diplomaten angewiesen, europäische Datensouveränität aktiv zu bekämpfen. Gerade erpresst das amerikanische Verteidigungsministerium KI-Firmen wie Anthropic, Sicherheitsmaßnahmen zurückzufahren, um direkten Zugang zu deren Daten bekommen. Anthropic hat sich gewehrt. Was passierte? Donald Trump hat sie als Risiko für die nationale Sicherheit eingestuft. Die Regeln der Weltordnung verändern sich. Wir müssen dafür sorgen, dass Europa diese Regeln schreibt und nicht aus seiner eigenen Zukunft herausgeschrieben wird. Europa sollte nicht nur ein Pfand sein zwischen den zwei digitalen Weltreichen China und USA.

**Ist es womöglich schon zu spät dafür?**

Sie sprechen hier mit einer, die denkt: Es ist sehr spät, aber nicht zu spät. Europa hängt digital zurück – und sollte das als Ernstfall betrachten.

**Haben die Amerikaner nicht einfach die besseren digitalen Produkte hergestellt und im Wettbewerb gewonnen? Das wäre doch fair.**

Aktuell kann man das wirklich nicht sagen. Der amerikanische Staat ist sehr stark involviert. Ihm gehören etwa mittlerweile zehn Prozent an Intel. Aber auch der AI Action Plan vom Juli 2025 ist stark protektionistisch. Die USA zwingen ihre Verbündeten, amerikanische KI-Technologie zu verwenden, etwa durch Handelsabkommen. Sie wenden sich offensiv gegen die Bestrebungen anderer Regionen, digital unabhängig zu werden. Das ist Protektionismus pur.

**Aber war Europa nicht schon davor digital abgehängt?**

Moment, es waren die Europäer, die den Markt für Handys einst dominiert haben mit Nokia. ASML, der wichtigste Hersteller von Maschinen für die Chipproduktion, ist eine europäische Firma. Und TSMC, der weltweit größte Chiphersteller, wurde von Philips mitgegründet, einer europäischen Firma. Wir brauchen eine europäische Industriepolitik, die sich nicht scheut, einen neuen Airbus fürs Digitalzeitalter zu bauen, damit wir nicht immer wieder Dinge verlieren, die wir eigentlich schon haben. Die USA sind übrigens nicht deshalb bei der KI so dominant, weil sie den Markt einfach haben machen lassen. Es gab den Chips Act, die öffentliche Beschaffung, die stark national ausgerichtet ist, die Darpa, eine Behörde des Verteidigungsministeriums, die sehr viele hoch dotierte Aufträge an Unternehmen gibt. Die Chinesen sind noch stärker staatlich getrieben.

**Aber man nutzt Chat-GPT nicht wegen Subventionen. Haben nicht einfach die Nutzer entschieden?**

Das schon, aber die Leute sehen nicht, was dahintersteckt. Um bessere Produkte herzustellen, braucht es Fähigkeiten und Investitionen. Und wie bekommt man die? Indem man Märkte durch Angebot und Nachfrage formt, etwa durch die öffentliche Beschaffung und langfristige strategische Investitionen. Also ja, es sind tolle Produkte und ja, Europa muss auch gute Produkte herstellen. Aber man kann helfen, die Märkte so zu gestalten, dass gute Produkte dabei herauskommen.

**Märkte gestalten heißt: Geld ausgeben, auch Steuergeld.**

Ja, aber wie sollen europäische Produkte gut werden, wenn wir einen Großteil unseres Ersparten in den USA investieren statt in Europa? Und wie soll es gehen, wenn wir 2,6 Billionen Euro jährlich an Steuergeldern für die Beschaffung ausgeben, aber weniger als zehn Prozent davon geht an europäische Firmen? In Italien sagen wir: Europa hat alle Zutaten, aber das Rezept ist falsch.

„DER STAAT MUSS UNTERNEHMERISCH DENKEN, NICHT NUR REGULIEREN.“

**Die Antwort lautet für Sie: Industriepolitik. Viele Ökonomen sehen das skeptisch. Sie sagen: Der Staat weiß doch nicht besser, was die Welt braucht, als die Firmen selbst und ihre Kunden.**

Ich verstehe Ihre Skepsis. Aber die USA und China machen Industriepolitik im ganz großen Stil. Sie sehen Technologie als ein Anliegen der nationalen Sicherheit. Währenddessen philosophiert Europa darüber, ob man so etwas mal machen könnte oder lieber nicht. Wir müssen anfangen. Es muss eine Priorität sein, dass mehr europäisches Geld in Europa investiert wird statt in den USA. Denn davon wird es abhängen, ob Europa eine Weltmacht bleibt oder eine digitale Kolonie wird.

**Sie stellen sich einen europäischen Staatsfonds vor, der 300 Milliarden Euro über das nächste Jahrzehnt für Tech-Innovation ausgeben kann. Wo soll das Geld herkommen? Gemeinsame Verschuldung, also Eurobonds?**

Ich weiß, dass die Deutschen Eurobonds eher kritisch sehen. Aber mir ist es nicht wichtig, wo das Geld herkommt. Wichtig ist mir, was wir damit machen. Ich habe während der Regierung von Mario Draghi vier Jahre lang den staatlichen Innovationsfonds geleitet, den ersten großen staatlichen Risikokapitalfonds Italiens.





**Was haben Sie dort gelernt, das Ihnen heute hilft?**

Der Staat muss unternehmerisch denken, nicht nur regulieren. Wir haben den Risikokapital-Markt in Italien geformt und vergrößert. Aber ich habe immer gedacht: Wir sollten das auf einem europäischen Level tun.

**Das regen Sie nun an. Was sollte mit den 300 Milliarden Euro Ihrer Meinung nach gefördert werden?**

Die Ideen sind da: eine europäische Cloud, insbesondere für die kritische Infrastruktur; KI-Fabriken und KI-Gigafabriken; die nächste Generation von Computerchips; digitale Identität und digitale Zahlungsmittel; KI-Anwendungen für Sektoren, in denen Europa schon führend ist wie in Technologien für grüne Energien oder Biotech.

**Bei den Computerchips haben die Deutschen zuletzt schlechte Erfahrungen gemacht. Mehrere große Projekte sind gestoppt. Das teuerste war eine Intel-Fabrik. Der Staat wollte zehn Milliarden Euro zahlen, damit sie in Magdeburg entsteht. Jetzt wird sie erst mal nicht gebaut.**

Ja, Intel geht es nicht gut, weshalb der amerikanische Staat auch Anteile des Unternehmens gekauft hat. Da haben die Deutschen das Falsche gefördert. Aber die Chipfabrik von TSMC in Dresden wird gebaut. Das sieht auch technologisch erfolgversprechender aus.

**Im Verlauf Ihrer Karriere waren sie erst Cheftechnologin der Stadt Barcelona, dann war Italien Ihr Fokus, jetzt Europa. Es ist aber vermutlich einfacher, etwas Revolutionäres in Barcelona zu tun als in der EU. Frustriert das manchmal?**

Die Zeit in Barcelona war aufregend für mich, weil man immer das Gefühl hatte, man ist ganz nah an den Menschen und tut etwas, was für sie bedeutsam ist: Mobilität, Wohnen, Luftqualität. Es war greifbar. Das ist jetzt abstrakter geworden. Aber wir brauchen die europäische Ebene. Schon in Barcelona habe ich von technologischer Souveränität gesprochen. Damals vor zehn Jahren hat das sonst niemand getan. Jetzt sprechen alle darüber – und ich diskutiere das mit den höchsten politischen Entscheidungsträgern in Europa.

**Wen muss man überzeugen, damit am Ende etwas von Ihren Ideen umgesetzt wird? Ursula von der Leyen?**

Die EU-Kommission allein reicht nicht. Es braucht die Nationalstaaten und die Industrie. Deshalb sind 250 Unternehmen Mitglied in unserer Eurostack-Initiative. Wichtig ist, dass nicht eine weitere europäische Bürokratie herauskommt, wie es Gaia-X (eine europäische Cloud-Plattform mit mäßigem Erfolg, Anmerkung der Redaktion) war. Denn dann verschwindet der Ehrgeiz.

**Zum Schluss: Was macht Ihnen Hoffnung, dass Europa irgendwann mithalten kann?**

Wir haben sehr viel gelernt durch das Aufkommen von Deep Seek, einer chinesischen KI-Technologie. Sie zeigt, dass man Teil des Spiels sein kann, ja, dass man sogar das Spiel gewinnen kann ohne die sehr hohen Investitionen wie in den USA und ohne die allerneueste Technologie. Wenn man einen klugen Ingenieursansatz hat, Open-Source-Software verwendet und schnell darin ist, Technologie zu übernehmen und anzuwenden, dann ist das der europäische Weg. Kurz gesagt: Europas Airbus-Moment fürs Digitalzeitalter ist jetzt. Die Frage ist, ob wir ihn nutzen.

ERSCHIENEN IN DER SZ VOM 02.03.2026

# Der Traum vom KI-Kontinent

*Die EU-Kommission legt ein neues Gesetzespaket vor, um technologisch weniger abhängig von Amerika und Asien zu werden. Anstatt große Firmen zu regulieren, will sie europäische Investitionen stärken.*

VON
JOSCHA F. WESTERKAMP





Der Cloud-Speicher für die Fotos, die Software für die Apps, jetzt auch noch so gut wie jede KI: Das meiste davon kommt aus Amerika oder Asien, kaum etwas aus der EU. Die Europäische Kommission möchte das mit einem neuen Gesetzespaket ändern. „Für über 80 Prozent aller digitalen Produkte, Dienste und Infrastruktur verlassen wir uns auf nichteuropäische Anbieter. Das ist ein großes Problem für Europas Versorgungssicherheit“, sagte Henna Virkkunen, die in der EU-Kommission als Vizepräsidentin für technologische Souveränität zuständig ist.

Um Europa zu einem „KI-Kontinent“ zu machen – dieses Ziel setzte Virkkunen gleich mit voraus – sei auch Infrastruktur nötig. Bei künstlicher Intelligenz bedeute dies vor allem sehr viel Rechenkapazität. Wenn die KI auf dem Handy antwortet, generiert sie dieses Wissen aus riesigen Datenzentren. Fast die Hälfte davon weltweit steht in den USA. Neben KI sind die Rechenzentren auch für Clouds gefragt. Dort sind immer mehr Daten gespeichert, von privaten Handys genauso wie großen Firmen. Bisweilen beherrschen aber die drei US-Firmen Microsoft, Google und Amazon zusammen mehr als 70 Prozent des europäischen Cloud-Marktes. EU-Anbieter hingegen machen zusammen nur 15 Prozent aus.

Die Kommission will daher in den nächsten fünf bis sieben Jahren dreimal so viel Rechenkapazität in Europa schaffen wie bisher. Gelingen soll das mit einem neuen Gesetz, dem sogenannten „Cloud- und KI-Entwicklungsgesetz“. Die EU-Mitgliedstaaten sollen demnach unter anderem klare Zonen für neue Datenzentren festlegen, in denen deutlich schneller Baugenehmigungen erteilt werden. Bestimmte Datenzentren sollen außerdem als strategisch wichtig für die EU eingestuft werden. Sind sie besonders innovativ oder nachhaltig, könnten sie eher von bereits bestehenden EU-Förderprogrammen profitieren.

Die Kommission will künftig genauer überwachen, wie viel Rechenkapazität und Nachfrage es in Europa gibt. Auf dieser Grundlage will sie den Mitgliedstaaten konkret empfehlen, wo sie ihre Kapazitäten ausbauen sollen. Zudem will die EU einen Mechanismus einrichten, um ungenutzte Rechen- und Cloud-Kapazität grenzüberschreitend besser auszulasten.

Frankreich etwa, wo nach Deutschland die zweithöchste Anzahl Rechenzentren in der EU steht, will diese ebenfalls stark ausbauen. Erst Anfang Juni hatte der französische Präsident Emmanuel Macron hohe Investitionen der japanischen Beteiligungsgesellschaft Softbank angekündigt. Gelockt hatte er den Investor unter anderem mit einem vorrangigen Zugang zum Stromnetz. Dank Atomkraft hat Frankreich ausreichend und günstigen Strom zur Verfügung und exportiert diesen sogar.

DREIMAL SO VIEL RECHENKAPAZITÄT WIE BISHER

Bei den Plänen gehe es nicht um eine Abschottung Europas, sondern um freien Wettbewerb und Partnerschaft, sagte Virkkunen. Trotzdem will die Kommission sicherstellen, dass Europa in kritischen Bereichen am Ende nicht doch noch von einzelnen amerikanischen Anbietern abhängig ist. Schließlich könnten auch Amazon oder Google Rechenzentren in Europa bauen und damit womöglich von den neuen Maßnahmen profitieren. Inwieweit auch diese Anbieter genutzt werden können, ist im öffentlichen Bereich künftig davon abhängig, wie schutzbedürftig eine Einrichtung ist.

Im untersten Level – das für einen Großteil der öffentlichen Einrichtungen gilt – müssen US-Firmen lediglich europäische Datenschutz- und Sicherheitsstandards einhalten. Sobald öffentliche Einrichtungen aber einen erhöhten Schutzbedarf haben, etwa Krankenhäuser oder Energieversorger, müssen deren Cloud-Anbieter unabhängig danach überprüft werden, wie selbständig sie in der EU sind. Mit steigendem Sicherheitslevel darf die Technologie dann umso weniger von außereuropäischen Anbietern abhängig sein – bis hin zu rein europäischen Anbietern, etwa für den Verteidigungssektor.

Doch die Rechenzentren sind nicht der einzige Part, mit dem die EU-Kommission mehr technologische Souveränität erreichen will. Sie schlägt auch eine neue Regulierung für Chips vor. Chips, die aus Halbleitern wie Silizium bestehen, sind in Smartphones, Laptops, Bankkarten, Fernsehern und Autos verbaut. Ohne sie lässt sich kaum noch ein modernes Gerät produzieren – und auch keine KI betreiben, was den Markt noch einmal erheblich vergrößert hat.

Die meisten Halbleiter kommen aus Asien, vor allem aus Taiwan, Südkorea und China. Unbedingt verhindern will die Kommission, dass wegen Lieferschwierigkeiten dieser Teile europäische Industriestränge zum Stoppen kommen. Dies war im Herbst einigen Autoherstellern passiert, als der Hersteller Nexperia deutlich weniger Chips nach Europa lieferte als geplant. Unter anderem Volkswagen stand kurz vor einem Produktionsstopp.

Mit dem „Chips Act 2.0“ überarbeitet die Kommission ihr bisheriges Chip-Gesetz und nimmt dabei neben dem Angebot diesmal verstärkt die Nachfrage in den Fokus. Wenn die in Europa zu gering ist, könnte die EU mit öffentlicher Beschaffung gegensteuern, um Firmen zu locken. Außerdem will die Kommission strategisch wichtige Projekte definieren, etwa Fabriken für besonders moderne KI-Chips. Die sollen priorisiert und mit einer Mischung aus privaten und öffentlichen Investments gefördert werden. Gleichzeitig sollen Forschung und Entwicklung künftig näher an der Industrie ausgerichtet sein. Bestehende Lieferketten will die Kommission viel genauer beobachten, um rechtzeitig vor gefährlichen Lücken wie bei Nexperia zu warnen.

Zusätzliches Geld stellt die Kommission dafür nicht bereit, stattdessen baut sie auf dem ersten Chips-Gesetz auf. Mit dem hatte sie elf Milliarden Euro bereitgestellt. Das Gesetz war im Herbst 2023 in Kraft getreten, vor nicht einmal drei Jahren also. Eingeführt hatte die Kommission es vor allem als Reaktion auf lückenhafte Lieferketten während der Corona-Pandemie.

Bis 2030, so das Ziel, sollten mit dem Gesetz mindestens 20 Prozent aller weltweit hergestellten Chips aus der EU kommen. Derzeit sind es allerdings erst 10,5 Prozent, kaum mehr als zur Einführung. Das Ziel werde damit wohl nicht mehr erreicht, sagte ein für das Gesetz mitverantwortlicher EU-Beamter auf SZ-Nachfrage. Erfolgreich findet die Kommission ihren ersten Chips Act trotzdem, weil die EU ihren Anteil bei der Chip-Produktion in dem schnell wachsenden Markt halten konnte.

Schließlich will die Kommission noch mehr für die europäische Tech-Souveränität tun. So stellte sie auch Pläne vor, wie die vielen Rechenzentren auf lange Sicht an genügend saubere Energie kommen können. Außerdem möchte sie die Nutzung von Open-Source-Software stärker fördern. Beides ist noch nicht mit einem konkreten Gesetzesvorschlag verbunden. Über die Verordnung für Clouds und KI sowie den überarbeiteten Chips Act müssen nun der Rat der Mitgliedstaaten und das EU-Parlament beraten, bevor sie in Kraft treten.



ERSCHIENEN IN DER SZ VOM 05.06.2026



## *„Souveränität heißt nicht Protektionismus“*

# EU-Digitalkommissarin Henna Virkkunen kämpft für Europas digitale Souveränität. Warum das so schwierig ist, wie sie auf die Sperrung eines neuen KI-Modells durch die USA blickt – und weshalb sie selbst kaum KI nutzt.

INTERVIEW VON
BASTIAN MÜHLING UND
VIVIEN TIMMLER

Henna Virkkunen kommt aus dem Kanzleramt gehetzt. In Berlin hat es an diesem Mittag 30 Grad im Schatten, und so verschwindet die EU-Digitalkommissarin so schnell es geht im klimatisierten Van. Früher am Tag hat sie bereits Digitalminister Karsten Wildberger getroffen, gleich soll sie eine Rede halten beim Tag der Industrie. Gerade mal fünf Stunden ist Virkkunen, 54, in Berlin, doch die sind durchgetaktet. Alle wollen hören, wie sich die EU-Kommission denn nun positioniert zu den großen Digitalthemen der Zeit.

**SZ: Kanzler Friedrich Merz hat kürzlich gesagt, dass Europa bei der digitalen Souveränität im Rückstand ist. Hat er recht?**

*Henna Virkkunen:* Ja, wir hinken hinterher, was die technologische Souveränität angeht. Bei der Digitalisierung gibt es große Unterschiede zwischen den Mitgliedstaaten. Alle müssen jetzt stärker in ihre Infrastruktur investieren. Wir müssen die Fähigkeiten unserer Bürger und die Implementierung von künstlicher Intelligenz in Unternehmen stärken.

**Hat Europa zu spät angefangen, als Gemeinschaft eine Infrastruktur aufzubauen?**

Nein, das würde ich nicht sagen. Einige Mitgliedstaaten sind da sehr weit. Aber etwas, an dem wir definitiv noch gemeinsam arbeiten müssen, ist, wie wir Unternehmen dabei helfen können, ihre Geschäftsmodelle in Europa zu skalieren. Das ist wirklich ein Problem hier. Mit 27 Mitgliedstaaten und 27 eigenen Regeln sind wir oft zu fragmentiert.

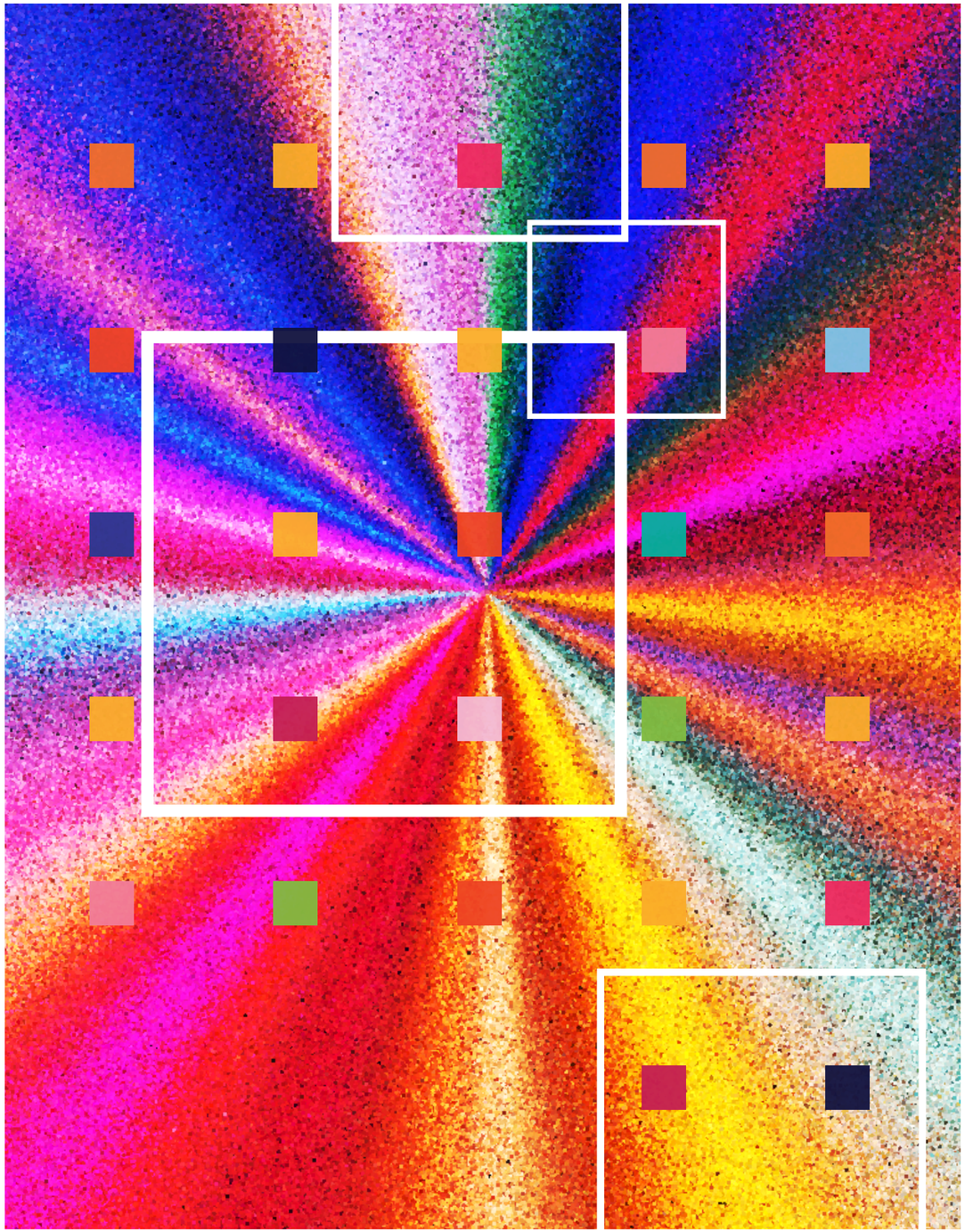
MIT 27 MITGLIED-
STAATEN UND
27 EIGENEN REGELN
SIND WIR OFT
ZU FRAGMENTIERT

**Zum Beispiel?**

Nehmen Sie die Start-up-Branche. Wir haben 45 000 Start-ups in Europa, das ist ein riesiges Potenzial. Aber trotzdem gehen sie oft in die USA, um da den nächsten Schritt zu machen. Einfach, weil sie dort viel einfacheren Zugang zu Finanzierung und größeren Märkten haben.

**Wie wollen Sie das ändern?**

Wir müssen die Grenzen zwischen den Mitgliedstaaten abbauen, um bessere Märkte zu schaffen. Da können wir als Kommission einiges beitragen. Wir haben vor Kurzem ein Paket zur technologischen Souveränität präsentiert. Da geht es darum, europäische Kapazitäten aufzubauen und Nachfrage nach europäischen Lösungen zu stärken. Wir arbeiten da jetzt mit Verordnungen – und nicht mehr mit Richtlinien wie früher.



auch nicht realistisch. Man braucht immer Partner. Aber wir dürfen keine gefährlichen Abhängigkeiten haben. Niemand darf den „Kill Switch“ zu unserer kritischen Infrastruktur haben.

**Die US-Regierung hat gerade erst demonstriert, wie so ein „Kill Switch“, also eine Abschaltoption, aussehen könnte: Die leistungsfähigsten Modelle der Firma Anthropic wurden mit Exportbeschränkungen belegt. Ist das für Sie nachvollziehbar?**

Ich halte die Exportkontrollen der Amerikaner nicht für die richtige Herangehensweise. Falls Maßnahmen aufgrund von Sicherheitsrisiken ergriffen werden müssen, sollten sie gemeinsam mit Partnern ergriffen werden. Es sollte keine Diskriminierung stattfinden. Wir arbeiten mit den USA daran, das Thema zu lösen und gemeinsam zu schauen, was für Sicherheitsbedenken sie haben. Solche Exportkontrollen gab es übrigens auch schon vor zwei Jahren, als Joe Biden noch im Amt war, für KI-Chips. Damals haben sie europäische Länder in zwei Kategorien unterteilt. Es ist also nicht ganz neu für uns.

„WIR DÜRFEN UNS NICHT VON DRITTEN ODER EINZELNEN UNTERNEHMEN ABHÄNGIG MACHEN.“

**Besorgt Sie das?**

Ja, schon. Es unterstreicht, wie wichtig es ist, unsere eigenen KI-Modelle zu entwickeln. Das ist genau das, was wir schon die ganze Zeit gesagt haben: Wir dürfen uns bei kritischen Technologien nicht von Dritten oder einzelnen Unternehmen abhängig machen, weder bei KI noch bei Halbleitern noch bei Quantentechnologie.

**Aber sind wir das nicht schon längst?**

Wir leben in einer neuen Realität. Unterschiedliche Länder haben unterschiedliche strategische Ressourcen. Die versuchen sie zu nutzen – aber auch zu schützen. Alle versuchen gerade, diese Technologie zu dominieren. Denn wer bei der Technologie dominiert, dominiert auch in der Wirtschaft und global in Sicherheitsfragen.

**Benutzen Sie selbst das Anthropic-Modell Claude?**

Ich nutze nicht viel KI, weil ich selbst nicht viel Schreibtischarbeit mache. Aber in meinem Team nutzen meine Mitarbeiter natürlich KI im Alltag. Dafür haben wir in der Kommission eine eigene sichere KI-Umgebung, in der die Modelle laufen. Das wird lokal in einem Rechenzentrum der Kommission gehostet.

**Können Sie schon sagen, wie lange die Anthropic-Modelle blockiert bleiben?**

Das ist Entscheidung der Amerikaner. Die G7 haben das bei ihrem Treffen im Juni diskutiert. Demokraten müssen beim Thema KI zusammenarbeiten. Und wir sehen auch, dass die Länder, die anfangs gedacht haben, dass KI keine Regeln braucht, nun auch mehr und mehr die Sicherheitsrisiken sehen.

**Wenn jetzt selbst die Amerikaner, die eigentlich immer gegen KI-Regulierung waren, ein Modell abschalten: Ist Anthropic in Wahrheit ein Beispiel dafür, dass eine strikte Regulierung nötig ist?**

Es ist gut, einen risikobasierten Ansatz zu haben. In Europa denken wir aktuell, dass in den meisten Fällen, in denen wir KI nutzen, das Risiko sehr niedrig ist. Aber wenn die KI anfängt, wichtige Entscheidungen zu treffen, und die Modelle sehr mächtig werden, ist es wichtig, die Risiken im Griff zu haben und die Sicherheit zu beachten. Da finde ich unseren AI Act sehr gut.

**Anfang Juli will die EU-Kommission ihren Aktionsplan für Cybersicherheit und KI präsentieren. Wird er eine Antwort auf den Anthropic-Fall enthalten?**

Der Grund, warum wir die Maßnahmen zur Cybersicherheit aktualisieren wollten, hat viel mit diesen neuen, leistungsfähigen KI-Modellen zu tun. Es ist mittlerweile absehbar, dass sie in der Lage sein werden, in sehr kurzer Zeit Lücken und Verletzlichkeiten in unseren Systemen zu finden. Früher hat das Wochen gedauert. Wir müssen also auch schneller antworten können. Wir müssen uns an die neue Realität anpassen, gerade im Bereich Cybersicherheit. Aktuell





kommen diese Modelle meist aus den USA. Aber wir können erwarten, dass solche Modelle in den nächsten Monaten aus anderen Ländern kommen.

**Wir haben seit dem KI-Modell Deepseek lange nichts mehr von China gehört.**

Alle versuchen gerade, ihre Kapazitäten und Fähigkeiten auszubauen. Das gilt auch für China. Die investieren genauso massiv. Sie sind sehr stark auf diesem Feld. Ich habe das immer im Hinterkopf. Trotzdem muss es die oberste Priorität sein, nicht auf die anderen zu schauen, sondern daran zu arbeiten, dass Europa selbst die nötigen Kapazitäten aufbaut.

**Was fehlt der EU gerade am meisten: die digitale Infrastruktur, das Geld oder der gemeinsame Einsatz für die Sache?**

Das Tempo. Wir müssen jetzt dringend schneller werden – und gemeinsam handeln.

ERSCHIENEN IN DER SZ VOM 24.06.2026

# Zukunft, made in Germany

*Deutschland und Hightech, das klang zuletzt nicht immer nach Erfolgsgeschichte. Bei Quantencomputern gibt es noch die Chance, mit den USA und China mitzuhalten. Doch das kostet.*

Von
Helmut Martin-Jung





An diese Tür klopft man nicht aus Höflichkeit, sondern aus Vorsicht. Die ist auch geboten, wenn man seine Augen nicht schädigen will. In dem Raum im ersten Stock des ehemaligen Motorenforschungszentrums von Daimler-Benz in Ulm arbeiten Wissenschaftler mit starken Lasern. Der unbedarfte Besucher sieht ein Gewirr aus Regalen mit elektronischen Geräten, in der Mitte einen großen Tisch voller kleiner Spiegel und merkwürdiger Aufbauten. Was die Forscher da tun, führt einen in die Welt des Ultrakleinen. Dorthin, wo die Physik Dinge macht, die allem Gewohnten zu widersprechen scheinen. Die Welt der Quantenphysik.

Schon lange arbeiten Forscher weltweit daran, Computer zu bauen, die die seltsamen Quanten-Eigenschaften nutzen und damit bestimmte Aufgaben unfassbar schnell rechnen können: Quantencomputer. Viel schneller und vor allem viel energiesparender sollen die sein als die großen Superrechner-Ungetüme. Für die braucht es ganze Hallen, und sie fressen so viel Strom wie eine Stadt. Quantencomputer sind zumindest bisher auch aufwendig zu betreiben, aber im Vergleich zu Supercomputern um ein Vielfaches effizienter. Solche Quantencomputer zu bauen, genau das haben sie hier in Ulm vor. In das sanierte frühere Daimler-Gebäude in Ulm sind Forscher des Deutschen Zentrums für Luft- und Raumfahrt (DLR) eingezogen und dazu eine ganze Reihe von Start-ups und Scale-ups, die nach der erfolgreichen Gründung schon einen Schritt weiter sind.

## EUROPA HÄNGT AM TROPF DER US-TECH-KONZERNE

Bei der Forschung an Quantencomputern gehört Deutschland zu den führenden fünf Nationen. Das zeigt eine kürzlich veröffentlichte Studie des Europäischen Patentamtes und der OECD. Der Anteil an globalen Patentfamilien im Bereich Quantentechnologien stieg von vier Prozent im Zeitraum zwischen 2015 und 2019 auf sieben Prozent im Zeitraum von 2020 bis 2024. Das deute auf eine „hohe Erfindungsaktivität in diesem Bereich“ hin, heißt es in der Studie. In Europa liegt Deutschland damit an erster Stelle, weltweit auf Platz fünf.

„Wir sind ein Player, der weltweit wahrgenommen wird“, sagt auch Robert Axmann, Leiter der DLR Quantencomputing-Initiative (DLR QCI). Hier und auch am DLR-Standort Hamburg wollen die Forscher die nächsten Schritte gehen. Also eben nicht abwarten, bis trotz hervorragender Forschung wieder irgendein Unternehmen aus den USA, ausgestattet mit Millionen Dollar Risikokapital, wieder einmal schneller ist – und sich schließlich zu einem Riesenkonzern entwickelt. So wie Google, Amazon und Microsoft, bei denen Europa inzwischen am Tropf hängt – inklusive der Gefahr, dass der Datenfluss kurzfristig gestoppt werden könnte.

Jahrelang spielte technische Unabhängigkeit kaum eine Rolle. Doch im Zeitalter dramatisch veränderter geopolitischer Rahmenbedingungen ist Souveränität mit einem Mal zu einem Überlebensfaktor geworden. Die Quantenforscher möchten daher alles dafür tun, dass sich das Land nicht bei einer weiteren Technologie mit enormem Zukunftspotenzial von anderen Mächten abhängig macht. Deshalb haben sie hier in Ulm die Bedingungen geschaffen, die es braucht, damit Start-ups sich entwickeln können. Entstanden ist sozusagen ein kleines Paradies für Nerds. Hier gibt es optische Tische, starke Laser, Reinräume, in denen Quanten-Chips hergestellt oder Diamanten bearbeitet werden können, die man ebenfalls zum Rechnen benutzt. Alles unter einem Dach oder ganz in der Nähe, Bedingungen also, von denen viele Forscher und Start-up-Gründer zumindest in Europa sonst nur träumen können.

Doch das Paradies ist in Gefahr. In Gefahr, aus Mangel an Unterstützung ausgetrocknet zu werden. Die von der Politik zugesagten Finanzierungen reichen nur bis Ende 2026. „Wenn es da keine Sicherheit gibt“, sagt der Chef der DLR-Quanteninitiative, Axmann, „dann gehen die Leute“. Und das Wichtigste bei Technologieprojekten wie diesen seien eben das Know-how und die Expertinnen und Experten. Axmann treibt die Sorge um, dass ein weiteres Mal eine Technologieentwicklung an Deutschland vorbeiläuft, wenn das Geld zur Förderung nicht mehr oder nicht ausreichend fließt. „Die wissen gar nicht, was sie verlieren könnten.“ Axmann wünscht sich verpflichtende Zusagen auch über Legislaturperioden hinaus. Die Mitarbeiter würden schließlich nicht warten, bis sie Ende 2026 ohne Job dastünden.

EINEN WIRTSCHAFTLICH RELEVANTEN QUANTENCOMPUTER BAUT MAN NICHT IN EIN PAAR JAHREN

Um am Ball zu bleiben, braucht es Geduld und Geld. Ein Quantencomputer ist eben keine Technologie, die sich in ein paar Jahren mal eben aus dem Boden stampfen lässt. Es gibt zwar große Fortschritte, aber noch sind Quantencomputer nicht gut genug, um all die bisher unlösbaren Probleme zu lösen, so wie von den Forschern geplant. Man könnte es mit frühen Autos vergleichen. Die Technik war noch lange nicht ausgereift, aber man konnte schon erahnen, dass sich das ändern würde.

Auch Konzerne wie Google oder IBM, die seit Jahren viel Energie in Quantenrechner gesteckt haben, können zwar Fortschritte vermelden. Aber: „Die Hardware ist noch nicht das Wunderwerk, das wir uns erhoffen – das dauert noch einige Jahre“, sagt Axmann. Manche Forscher vergleichen den derzeitigen Stand der Technik mit dem von Computern aus den 1960er-Jahren, die noch mit Lochkarten programmiert werden mussten.

Wohin man auch schaut, auf der ganzen Welt wird noch an den Grundlagen dieser Technologie gearbeitet, die nicht wie herkömmliche Computer mit Bits, sondern mit Qubits arbeitet. Der wichtigste Unterschied: Um bei herkömmlichen Computern die Rechenleistung zu verdoppeln, braucht es auch Chips mit doppelt so vielen Bits. Dagegen verdoppelt theoretisch bereits ein weiteres Qubit die Rechenleistung. Damit Quantencomputer ihr volles Potenzial entfalten, müssten sie aber Hunderttausende oder Millionen Qubits mit möglichst wenig Fehlern enthalten – hier tut sich derzeit noch ein weites Feld auf für Ingenieurinnen und Ingenieure. Die derzeit am weitesten fortgeschrittenen Systeme haben einige Hundert oder ungefähr tausend Qubits. Und noch ist auch nicht entschieden, mit welcher Technologie genau künftige Quantencomputer arbeiten sollen. Derzeit wetteifern verschiedene Ansätze darum, wer das Rennen macht.

Beim DLR in Ulm und Hamburg wurden daher bewusst Start-ups ausgewählt, die an verschiedenen Technologien arbeiten, um Quanten-Eigenschaften zum Rechnen zu nutzen. Und sie tun das dort nicht im luftleeren Raum. Kunden aus der Wirtschaft sind ebenfalls mit dabei, um gemeinsam mit den Quanten-Start-ups auszuloten, wie die Technologie ihnen helfen könnte.

Ein Beispiel dafür ist der Rhein-Neckar-Verkehrsverbund (RNV). Jede Menge Fahrzeuge, Tausende Mitarbeiter im Fahrdienst, dazu wechselnde Bedingungen, das ist ein ideales Feld für Quantencomputer. Hier können sie beweisen, ob sie wirklich in der Lage sind, spürbare Verbesserungen und damit auch Einsparungen zu bewirken. Solche Optimierungsprobleme gelten schließlich als eine der Paradedisziplinen der Technologie. Durch ihre spezielle Funktionsweise können Quantencomputer mit den geeigneten Algorithmen eine Vielzahl von Optionen parallel berechnen, anders als herkömmliche Computer. Beim RNV sollen Dienste für Rufbusse untersucht werden, in dem Projekt mussten dafür zunächst die nötigen Daten erhoben und strukturiert werden. Im nächsten Schritt soll dann mit dem Prototyp eines Quantencomputers versucht werden, den Dienst zu optimieren.

DEUTSCHLAND IST BEI DER FORSCHUNG GUT AUFGESTELLT

Die bisherigen Computer kommen schließlich bei einer großen Menge an möglichen Optionen und Parametern, wie sie solche Dienste mit sich bringen, schnell an ihre Grenzen. Sogar für die größten Supercomputer sind solche Probleme zu komplex. Es würde viel zu lange dauern, sie zu berechnen. Quantencomputer dagegen sollen, wenn sie einmal leistungsfähig genug sind, Verkehr in Städten in Echtzeit berechnen und steuern können.

Das DLR tritt gegenüber den Start-ups als sogenannter Ankerinvestor auf. Das Quanten-Unternehmen Planqc aus Garching bei München etwa hat vom DLR einen Auftrag im Wert von 29 Millionen Euro bekommen, das ist einer der größeren Einzelaufträge. Dafür muss Planqc bis 2027 einen Quantencomputer mit mehr als 100 Qubits bauen. Von Investoren und öffentlichen Geldgebern hat Planqc 2024 bereits weitere 50 Millionen Euro an Risikokapital eingeworben. Ein großer Vertrauensvorschuss für ein Unternehmen, das es gerade einmal seit 2022 gibt.

Allerdings kommt das Team auch nicht aus dem Nichts. Der Gründung vorausgegangen war jahrzehntelange Forschung am Münchner Max-Planck-Institut für Quantenoptik (MPQ), das weltweit einen hervorragenden Ruf genießt und Nobelpreisträger hervorgebracht hat. Dort hatten Wissenschaftler wie Planqc-Mitgründer Sebastian Blatt schon länger an einer vielversprechenden Technologie für Quantencomputer gearbeitet.

Die Forscher fangen mit Laserstrahlen einzelne Strontium-Atome in Vakuumkammern ein und ordnen sie zu Gitterstrukturen. Mit dem Ziel, damit zu rechnen. Blatt sieht es als Vorteil des Ansatzes von Planqc, dass sich die Zahl der Qubits vergleichsweise leicht steigern lässt. Technische Probleme bleiben trotzdem genug, so etwa den derzeit noch recht laborhaft anmutenden Aufbau in etwas zu verwandeln, das einem Produkt näherkommt. Oder die Fehlerkorrektur zu verbessern.

Planqc war die erste Ausgründung aus dem Munich Quantum Valley, einer Initiative Bayerns, um die Quantentechnologie zu fördern. Daran sind die Fraunhofer-Gesellschaft, das DLR, die Münchner Universitäten, die Uni Erlangen, die Bayerische Akademie der Wissenschaften (BAdW) und die Max-Planck-Gesellschaft beteiligt. Am Leibniz-Rechenzentrum der BAdW ist bereits ein Quantencomputer einer deutsch-finnischen Firma mit dem dortigen Supercomputer verbunden, später soll der von Planqc dazukommen. Auch im Forschungszentrum Jülich ist die dortige Supercomputer-Infrastruktur mit einem Quantencomputer-Prototyp verbunden. Daran arbeiten 25 Institutionen aus Deutschland mit, gefördert wird das Großprojekt zu 90 Prozent vom Bund.

MILLIARDEN VOM STAAT

Insgesamt hat die öffentliche Hand in Deutschland bis Ende 2025 etwa 5,2 Milliarden Dollar für die Forschung an Quantentechnologien bereitgestellt, nur knapp hinter den USA mit sechs Milliarden Dollar. In den Staaten steht den Unternehmen und Start-ups aber erheblich mehr privates Risikokapital zur Verfügung. Und in China investiert der Staat ebenfalls mächtig in die Technologie, die Rede ist von etwa 15 Milliarden Dollar. Japan liegt mit mehr als neun Milliarden Dollar ebenfalls vor Deutschland.

Noch sei Europa mit China und den USA an der Spitze der Entwicklung, bilanziert das Fraunhofer-Institut für System- und Innovationsforschung ISI in einer Studie. Um diese Position zu verteidigen, fordern die Wissenschaftler eine langfristige öffentliche Förderung. Zudem sollten strategische Rahmenbedingungen geschaffen werden. Dazu gehöre etwa der „Abbau bürokratischer Hürden, die Unterstützung von Start-ups mit technischer Infrastruktur und Risikokapital sowie die Förderung von Softwareentwicklung und Fachkräften“. So sieht das auch Start-up-Gründer Sebastian Blatt: „Wir brauchen Ressourcen für die Skalierung.“ Um die Technologie weiterzuentwickeln, sei eben sehr viel Ingenieursleistung nötig.

Eigentlich ist also klar, was zu tun wäre. Die Frage ist, ob es auch passiert.



ERSCHIENEN IN DER SZ VOM 20.01.2026



# „KI ist der Rettungsanker für die deutsche Industrie“

In München ist das erste reine KI-Rechenzentrum Deutschlands eröffnet worden. Die Projektpartner Telekom und SAP waren sich mit der Politik einig, dass damit ein wichtiger Meilenstein erreicht worden sei.

Von
Helmut Martin-Jung

Zur Zukunft geht es durch einen Tunnel, den man für eine Hobbithöhle halten könnte, wäre er nicht erleuchtet von magenta- und neongrünfarbenen Leuchtstoffröhren. Den Tunnel erreicht man über eine Treppe, der man ansieht, dass sie aus den 1970er-Jahren stammt. Damals wurde der Tucherpark in München von der Hypovereinsbank bebaut, und sie grub dort bis zu sechs Stockwerke tief unter die Erde für ein Rechenzentrum.

Dass die Bunkerhülle von damals noch funktionsfähig ist, ist ein Glücksfall für die Telekom und ihren Partner Polarise. So schafften sie es, in nicht mehr als drei, vier Monaten das Innenleben auf den neuesten Stand zu bringen. Aber was heißt hier neuester Stand, etwas Vergleichbares gebe in Deutschland bisher nicht, sagt Ferri Abolhassan, im Vorstand der Telekom unter anderem zuständig für die Themen Cloud und auch für künstliche Intelligenz.

Genau darum geht es bei dem Rechenzentrum am Münchner Eisbach. Es soll auf eine neue Ebene heben, was eigentlich die traditionelle Stärke Europas ist: Produktion. Mithilfe von KI sollen Unternehmen in die Lage versetzt werden, ihre Produktion effizienter zu machen, zu automatisieren.

Auf zwei der sechs Etagen hat der Betreiber der Anlage, der deutsche Spezialist für KI-Rechenzentren, Polarise, vier sogenannte Pods aufgebaut, abgetrennte schwarze Kammern, in denen Server des US-Herstellers Nvidia in hohen Regalen stehen. In manchen davon sorgen Blackwell-Chips von Nvidia für höchste Rechenleistung, in anderen arbeiten RTX-Grafikeinheiten, die ihre Stärken etwa bei der Simulation von Oberflächen haben. Die Kühlung läuft über Wasser aus dem Eisbach, der direkt vorbeifließt. Die Abwärme des Rechenzentrums soll auch das gesamte Quartier im Tucherpark beheizen.

Telekom-Chef Tim Höttges sprach von einem guten Tag für Deutschland. Den Bedarf an Rechenleistung hält er auch in Europa für gigantisch. „KI ist keine Chance, sondern der Rettungsanker für die deutsche Industrie.“ Allerdings seien die Energiekosten in Deutschland hoch. An Projekten wie diesen entscheide sich, ob Deutschland mithalten könne im weltweiten Wettbewerb.

Zu den Partnern des KI-Rechenzentrums gehört auch der Softwarekonzern SAP. Dessen Chef Christian Klein, zugeschaltet per Video, hob hervor, dass vertrauliche Daten auch in der Industrie eine immer größere Rolle einnähmen. „Dieses Spiel ist noch nicht gespielt“, sagte Klein. Es müsse also jetzt darum gehen, die Daten, die die Industrie in den vergangenen Jahren bereits gesammelt habe, dazu zu nutzen, die Produktion effizienter zu gestalten oder sogar ganz neue Geschäftsmodelle zu entwickeln.

Sein Vorstandskollege Thomas Saueressig sagte, es sei wichtig, dass bis auf die Hardware alle Bestandteile aus Deutschland kommen. Die Differenzierung gegenüber internationalen Konkurrenten müsse über die Industrie funktionieren, und zwar schnell: „Wir müssen ins Handeln kommen, vom Mindset her nach vorne gehen. Es gibt keine Ausrede mehr, KI nicht zu nutzen.“ Als Kunden hat die Telekom besonders den Mittelstand im Auge. Diese bekämen bei den großen US-Anbietern oft keine guten Konditionen, sagt Höttges.

Bayerns Ministerpräsident Markus Söder lobte das Vorhaben, das die KI-Rechenkapazität Deutschlands mit einem Schlag um 50 Prozent erhöhe. Mit Angst vor neuen Technologien werde man nicht weiterkommen. Söder versprach, die Förderung für KI fortzusetzen, er warb auch dafür, einen Industriestrompreis für Rechenzentren einzuführen. Nur bei anderen einzukaufen, könne nicht die Lösung für die Zukunft sein.

„DIESEN SCHATZ MÜSSEN WIR JETZT HEBEN.“

Finanzminister und Vizekanzler Lars Klingbeil betonte, wie wichtig das Projekt sei, um dabei zu helfen, Deutschland aus der derzeitigen wirtschaftlichen Schwächephase zu holen. Es sei ein starkes Zeichen, dass mit Nvidia ein starker Partner gewonnen wurde. Die ersten Tage des Jahres 2026 hätten gezeigt, dass man in einer Zeit des Umbruchs stecke. Europa dürfe nicht zum Spielball großer Mächte werden. Deutschland aber habe viel auf der Habenseite vorzuweisen und sei ein starkes Land. „Wir sind die drittgrößte Wirtschaftsnation und wir sind ein verlässlicher Handelspartner.“

Die Investitionen in Zukunftstechnologien müssten zwar größtenteils aus der Wirtschaft kommen, so Klingbeil, aber die Politik müsse auch die Rahmenbedingungen so setzen, damit die Wirtschaft sich entwickeln und wachsen könne. Innovative Start-ups müssten auch hier eine Zukunft haben. Dabei, sagte Antonio Krüger, Chef des Deutschen Forschungszentrums für Künstliche Intelligenz, müsse sich Deutschland auf seine Stärken besinnen. Die Industrie habe in den vergangenen Jahren bereits sehr viele Daten gesammelt. „Diesen Schatz müssen wir jetzt heben.“

ERSCHIENEN IN DER SZ VOM 05.02.2026

# „Du musst unter den richtigen Apfelbäumen stehen“

## Infineon profitiert vom KI-Boom. Konzernchef Jochen Hanebeck erklärt, warum er die Entscheidung für massive Investitionen in Deutschland noch nie bereut hat. Und was das Land bräuchte, um wieder erfolgreich zu werden.

Interview von
Caspar Busse

Es läuft gerade gut für den Infineon-Vorstandsvorsitzenden Jochen Hanebeck, 57. Der größte Halbleiterhersteller Europas ist inzwischen an der Börse fast doppelt so viel wert wie die Deutsche Bank. Die Prognosen sind angehoben worden, auch wegen des Booms bei KI-Rechenzentren, in denen viele Infineon-Halbleiter gebraucht werden. In der kommenden Woche eröffnet Hanebeck eine neue Fabrik in Dresden.

**SZ: Herr Hanebeck, alle sprechen von den Problemen der deutschen Wirtschaft und den massiven Nachteilen des Standorts Deutschland. Infineon investiert trotzdem in Dresden fünf Milliarden Euro. Haben Sie die Entscheidung für Deutschland schon bereut?**

*Jochen Hanebeck:* Nein, noch keine Sekunde.

**Warum nicht?**

Für Infineon ist diese Investition, die größte unserer Unternehmensgeschichte, sehr sinnvoll. Es ist perfektes Timing. Es zeigt auch, dass man in unserer Industrie den langfristigen Trends folgen muss. Dekarbonisierung und Digitalisierung führen dazu, dass überall unsere Chips gebraucht werden, für dieses Wachstum wollen wir gerüstet sein.

„WIR BRAUCHEN MUT IN DER POLITIK, UM DIE SCHWIERIGE TRANSFORMATION ANZUGEHEN.“

**Also stimmt es gar nicht, dass der Standort Deutschland so schlecht ist?**

Die aktuelle Kritik am Standort Deutschland ist schon berechtigt. Bei Faktoren wie Lohnnebenkosten, Steuern und Bürokratie muss definitiv etwas passieren. Aber Deutschland wird nicht allein mit einer Verbesserung der Rahmenbedingungen in Zukunft erfolgreich sein. Wir müssen gezielt auf Zukunftsindustrien wie Mikroelektronik setzen. Die Bundesregierung tut das mit der Hightech-Agenda. Die sollte nun zügig und entschlossen umgesetzt werden. Dazu kommt: Wirtschaft ist auch Psychologie. Wir brauchen Mut in der Politik, um die schwierige Transformation anzugehen. Und wir brauchen auch Mut, bei den Unternehmen zu investieren.

**War Ihre Entscheidung für die neue Fabrik in Dresden vor gut vier Jahren mutig oder unverantwortlich? Damals war die Branche im Abschwung, Infineon musste Jobs abbauen.**

Es war schon eine Nummer, fünf Milliarden Euro zu investieren. Zum Vergleich: Unser Umsatz lag im Jahr 2025 bei rund 15 Milliarden Euro. Aber wir haben immer daran festgehalten, das zahlt sich jetzt aus.

**Andere große Leuchtturmprojekte in Deutschland sind gescheitert, Intels Chipfabrik in Magdeburg etwa oder eine Batterieproduktion in Schleswig-Holstein. Haben die was falsch gemacht – oder Sie?**

Ich kann nur die Geschäftspläne beurteilen, die ich kenne – das sind die Planungen von Infineon. Die sind fundiert und werden umgesetzt, also unsere neue Fabrik in Dresden und das Gemeinschaftsunternehmen mit TSMC sowie Bosch und NXP in Dresden. Die Kunst in der Halbleiterindustrie ist es, Projekte umzusetzen, die man in einer Boomphase braucht, die man aber auch in einem Abschwung durchhalten kann.

**Vielleicht war das das Problem für Intel. Was hat denn bei Ihnen jetzt genau für Deutschland und Dresden gesprochen?**

Es gibt mehrere Gründe: Wir sind bereits in Dresden und können dort Skaleneffekte nutzen. Es gibt in Dresden ein großes Ökosystem für Halbleiter, mit vielen Stärken, darunter auch die Kompetenz unserer Mitarbeitenden. Und es gab natürlich eine staatliche Förderung.

**Sie bekommen insgesamt eine Milliarde Euro für die neue Fabrik, 20 Prozent der Investitionssumme.**

Ja. Wir hätten an anderer Stelle auf dieser Welt wahrscheinlich noch mehr Förderung bekommen. Wir investieren aus eigenen Mitteln jedes Jahr allein rund drei Milliarden Euro in Deutschland, in Forschung

und Entwicklung sowie Fertigungsanlagen, und stärken so den Standort weiter. Als Unternehmen mit Sitz in Deutschland wollen wir auch zur Resilienz der Bundesrepublik beitragen. Der Standort ist für mich eine Herzensangelegenheit.

**Sie kritisieren auch die Bürokratie, aber Sie waren mit dem Fabrikbau drei Monate schneller als geplant fertig. So schlimm kann es also nicht sein.**

Es gibt ja viele Ausprägungen von Bürokratie, von Berichtspflichten bis über Lieferketten- und andere Gesetze. Aber in Sachsen war die Zusammenarbeit mit den Behörden wirklich vorbildlich. Da zeigt sich, was man erreichen kann, wenn Politik, Gesellschaft und Unternehmen an einem Strang ziehen.

„ES GEHT UM TEMPO, TEMPO, TEMPO."

**Viele Großprojekte in Deutschland ziehen sich endlos, etwa der Bahnhof Stuttgart 21. Wie könnte man das beschleunigen?**

Ich kann nur für gewerbliche Bauten sprechen. Aber man kann wirklich viel Zeit verlieren – mit Baugenehmigungen und allem, was dazugehört. In Sachsen merkt man, dass die Erfahrung und der Wille vorhanden sind, diese Halbleiterprojekte durchzuziehen.

**Sie haben schon mit dem Bau in Dresden angefangen, obwohl der Förderbescheid gar nicht da war. Ist das ein Modell?**

Zunächst einmal wünsche ich mir, dass Förderbescheide schneller erteilt werden. Es geht um Tempo, Tempo, Tempo, gerade in unserer Industrie. Wir haben in der Tat schon zwei Jahre gebaut, als der finale Bescheid bei uns eintraf. Aber wir hatten das Vertrauen in die deutsche Politik, da wir einen überparteilichen Konsens über mehrere Regierungen hinweg gesehen haben.

**In Sachsen ist die tendenziell fremdenfeindliche AfD besonders stark, das ist doch ein Standortnachteil für einen internationalen Konzern wie Infineon.**

Infineon steht für Diversität, und wir brauchen Arbeitskräfte aus allen Ländern mit Kompetenzen und Erfahrungen aus der globalen Halbleiterindustrie. In Dresden beschäftigen wir Mitarbeitende aus 50 Ländern. Wir haben bisher keine Probleme, diese Mitarbeiter zu bekommen, aber wir sind auch in Zukunft darauf angewiesen, Talente weltweit zu akquirieren.

**Jetzt steht da eine neue große Fabrik, die schnell ausgelastet werden muss. Haben Sie manchmal schlaflose Nächte?**

Nein, nicht deswegen. Ich bin seit mehr als 30 Jahren in der Chipindustrie und haben viele Zyklen, viele Aufs und Abs gesehen. Man muss an seine Überzeugungen glauben, auch wenn Wolken vorbeiziehen.

**Aber dass es einen solchen Boom bei Rechenzentren für künstliche Intelligenz (KI) geben würde, von dem auch Infineon profitiert, konnten Sie nicht absehen.**

Nein. Aber Infineon arbeitet seit 15 Jahren und länger sehr konsequent an innovativen Stromversorgungslösungen aller Art, in klassischen Rechenzentren haben wir führende Marktanteile. Wir waren immer überzeugt, wie wichtig diese Stärken sind. Kompetenz kann man nicht erst aufbauen, wenn der Boom losgeht. Deshalb stehen wir jetzt gut da. Es gibt dieses Sprichwort: Wenn du unter einem Apfelbaum stehst, kannst du nicht erwarten, dass der Apfel genau in deine Hand fällt. Aber du musst unter den richtigen Apfelbäumen stehen und dann schnell agieren.

**Haben Sie trotzdem Sorge, dass der KI-Boom bald wieder abebbt?**

Alle, die an diesem Boom zweifeln, sollten nachdenken, wo KI noch überall angewendet werden kann. KI ist eine wirkliche Revolution, die noch Jahre andauern wird. Der Markt und damit der Bedarf an Rechenzentren ist sehr groß. Da ist noch viel mehr Musik drin, als so mancher glaubt. Unser Ziel ist klar: Infineon will bei Leistungshalbleitern für KI-Rechenzentren auf einen weltweiten Marktanteil von mindestens 30 bis 40 Prozent kommen.

**Infineon ist nach Umsatz der größte Chiphersteller Europas, an der Börse sind Sie inzwischen mehr als 100 Milliarden Euro wert.**

Der Aktienkurs hat sich in den vergangenen Monaten verdoppelt. Natürlich macht uns das stolz, das ist auch ein Zeichen des Vertrauens der Investoren in unseren Kurs.

**Geht das denn so weiter? Von Kursen wie Nvidia sind Sie ja noch weit entfernt.**

Nvidia ist an der Börse ja fast 4,5 Billionen Euro wert, das ist das 45-Fache, das sind andere Dimensionen. Wir sind ja nicht nur von KI abhängig. Derzeit belebt sich beispielsweise auch das Geschäft mit der Automobilindustrie. Dort sind wir auch weltweit aktiv. Wir sind unabhängig von einzelnen Herstellern, und wir profitieren davon, dass in den Fahrzeugen immer mehr Software ist, dafür braucht es immer mehr Halbleiter. Dazu kommen unsere Halbleiter für den Bereich erneuerbare Energie, da wird derzeit gerade in Südostasien viel investiert, um sich von Öl und Gas unabhängiger zu machen.

**Ihre neue Fabrik in Dresden soll auch Europa helfen, souveräner zu werden. Die EU-Kommission will den Anteil in Europa gefertigter Chips auf 20 Prozent steigern, das klappt aber nicht. Wie abhängig ist Europa wirklich bei Chips?**

Pauschale Anteile bei allen Chips sind eher zweitrangig, es geht vielmehr um die Marktposition Europas in bestimmten Bereichen. Die modernen Lithografiemaschinen für Halbleiter kommen vor allem aus Europa, von ASML aus den Niederlanden mit den deutschen Zulieferern Zeiss und Trumpf. Aber auch bei vielen Halbleiterprodukten können wir sehr gut mithalten: Bei Chips für die Autoindustrie kommen beispielsweise die großen europäischen Halbleiterhersteller auf einen Weltmarktanteil von über 30 Prozent. Auch im Bereich Leistungshalbleiter, Sensoren und Mikrocontrollern ist die europäische Industrie weltweit führend. Dazu kommen hervorragende Forschungsinstitute. Der europäische Chipstandort ist besser, als viele sagen.

**Gibt es eigentlich Kunden, die nur Produkte aus Deutschland oder Europa haben wollen?**

Ja, es gibt mittlerweile definitiv nicht nur Wünsche, sondern konkrete Forderungen von Kunden, in allen Kombinationen. Manche wollen, dass wir sie aus zwei Fabriken weltweit beliefern können. Viele wünschen sich, aus Europa beliefert zu werden. In China wiederum gibt es Abnehmer, die wollen nur Ware aus China bekommen, da arbeiten wir dann mit Auftragsfertigern zusammen. Das alles macht es für uns zwar komplexer, weil gerade die Chipindustrie mit Skaleneffekten erfolgreich wurde. Aber wir bekommen das hin.

ERSCHIENEN IN DER SZ VOM 24.06.2026

# „Wer kompetitiv ist, ist automatisch souverän“

*Eine Trillion Rechenoperationen pro Sekunde: Jupiter ist Europas erster Exascale-Rechner. Sein Leiter Thomas Lippert über Blutzellen-Simulationen, TÜV-Prüfungen und ein deutsches ChatGPT.*

Interview von
Bastian Mühling

Im Büro von Thomas Lippert hakt die Internetverbindung. Der Leiter des Jülich Supercomputing Centre am Forschungszentrum Jülich nimmt es mit Humor. Lippert ist verantwortlich für den Supercomputer Jupiter, der für KI-Anwendungen und wissenschaftliche Simulationen genutzt werden soll.

Als erste Maschine in Europa überschreitet Jupiter die Grenze von einer Trillion Rechenoperationen pro Sekunde – was der Rechenleistung von etwa einer Million moderner Smartphones entspricht. Im Interview mit SZ Dossier spricht er über TÜV-Prüfungen am Supercomputer, erste konkrete Anwendungsfälle und digitale Souveränität.

„MIT JUPITER KÖNNEN WIR GRENZEN ÜBERWINDEN.“

**SZ: Herr Lippert, was ist das Schönste an dem Supercomputer Jupiter?**

*Thomas Lippert:* Dass wir mit ihm Grenzen überwinden können. Ich bin eher analytisch veranlagt und rechne auch heute gerne noch mit Papier und Bleistift. Mit dem Supercomputer habe ich ein Instrument, mit dem ich diese Arbeit fortsetzen kann, und zwar in Bereichen, wo mein Gehirn – und auch die Gehirne vieler Menschen zusammengenommen – nicht mehr weiterkommt.

**Und wenn Sie physisch davorstehen, was ist dann das Schönste?**

Die Kühlanlage. Dass man so etwas überhaupt bauen kann. Das sind Pumpen mit 70 Kilowatt, aus Edelstahl geschweißt, oben auf dem Dach. Wie und dass das alles funktioniert und zusammenspielt in den Regelkreisen, finde ich faszinierend.

**Jupiter wurde im September 2025 eingeweiht, die Abnahme für April 2026 geplant. Was dauert so lange?**

Wie schnell so etwas geht, hängt davon ab, wie viel Innovation drinsteckt. Das, was wir geplant, mitdesignt und umgesetzt haben, gab es in dieser Form noch nicht. Von 4000 KI-Spezialchips auf 24.000 zu skalieren, ist eine Herausforderung. Ein Problem war, dass die Energiezufuhr für die Racks nicht richtig funktioniert hat. Da mussten an verschiedenen Boards Stromverteiler ausgetauscht werden. Das braucht seine Zeit. Im Vergleich zum Gesamtprojekt sind das aber Marginalien.

**Teile des Supercomputers werden bereits vom Tüv. Nehmen Sie uns mit. Was ist jetzt noch zu tun?**

Im Grunde funktioniert alles. Bei den leistungsstarken Stromleitern, den Power-Bars, werden noch Elemente ausgetauscht. Da sind völlig neue Technologien verbaut. Daher ist auch die Erfahrung des Tüv so noch nicht gegeben. Das sind exzellente Prüfer, aber in diesem technologischen Kontext lernen wir gemeinsam immer noch dazu.

**Die Nachfrage ist hoch, Wissenschaftlerinnen und Wissenschaftler haben Anfragen für 400 Prozent der Rechenleistung gestellt. Was läuft jetzt schon?**

Die Maschine läuft aktuell zu rund 50 Prozent, innerhalb einiger Monate soll Jupiter auf 100 Prozent kommen. Alles, was bereits nutzbar ist, nutzen wir für den Testbetrieb. Zum Beispiel laufen im Bereich der Biologie schon Blutzellen-Simulationen. In der Hirnforschung geht es um die erste Stufe eines Frontiermodells für das menschliche Gehirn. Dadurch sollen Chirurgen besser eingrenzen können, was bei einem Eingriff passieren kann.

**Jupiter soll auch für Klima- und Wetterdaten genutzt werden.**

Genau, bei Extremwetterereignissen können wir die Auflösung der Modelle um den Faktor zehn erhöhen und damit eine objektive Faktenbasis für die Fra-

ge schaffen, ob ein Extremwetterereignis tatsächlich mit der Klimaveränderung verbunden ist.

**Was ist für Sie als Wissenschaftler das Neue an Jupiter?**

Jupiter und die Weiterentwicklung von KI-Modellen werden das Wesen unserer Wissenschaft verändern. Normalerweise hat man eine Problemstellung und versucht, die Formeln mathematisch zu lösen. Mit einem Frontiermodell haben Sie eigentlich schon die Lösung für alles. Sie müssen nur den richtigen Input geben. Das ist noch Zukunftsmusik, aber dahin wird es sich entwickeln.

**Was bedeutet das mit Blick auf das globale Tech-Rennen?**

Momentan ist der Wendepunkt. Wenn wir nicht in der Lage sind, diese Dinge zu tun, weil wir die Rechenzeit dafür nicht haben, dann werden andere das tun. Und wir müssen bei ihnen einkaufen.

„WIR MÜSSEN EIN GEGENGEWICHT GEGEN AMAZON UND CO. HABEN."

**Aber müsste man nicht zuerst den Bedarf an Rechenleistung ermitteln, bevor man ohne Rücksicht auf Energie- und Wasserverbrauch ausbaut?**

Ich lache immer, wenn das jemand sagt. Nein, Leute, das müssen wir nicht. In Amerika macht das niemand. Die sagen, wir wollen in Zukunft den Bedarf definieren, indem wir die Benchmark setzen im Rechnen. Natürlich muss man auf den Energieverbrauch achten und energieeffiziente Technologien fördern. Aber vor allem benötigt Deutschland fünf bis sechsmal so viel Rechenleistung, um mithalten zu können. Stattdessen verlieren wir uns in Kleinstaaterei.

**Was meinen Sie damit?**

Wir müssen weg von föderalen Wünschen hin zu einer Gesamtlösung. Bündeln heißt für mich, mehr zu machen in der Gesamtkompetenz, die auf ein Problem angewandt wird. Konkret: mehr Rechner, mehr Leute, die in der Lage sind, große Modelle zu bauen, mehr Daten und ein besserer Zugang zu diesen Daten. Wir wären im Prinzip mit unserer Kompetenz in der Lage, mitzuhalten.

**Und wie lange dauert es dann bis zu einem ersten deutschen ChatGPT?**

Um ein mit ChatGPT vergleichbares Sprachmodell zu schaffen, muss Jupiter drei Monate laufen. Auf dem freien Markt würde das zwischen 150 und 300 Millionen Euro kosten. Aber letztlich entscheiden nicht wir, was mit Jupiter gemacht wird, sondern die Politik.

**Um aufzuholen, plant die EU derzeit KI-Gigafabriken. Wie schätzen Sie die deutschen Bewerbungsbemühungen ein?**

Ich begrüße das sehr. Wir müssen ein Gegengewicht gegen Amazon und Co. haben. Die Frage ist, ob die KI-Gigafabriken der richtige Ansatzpunkt sind. Wenn Schwarz und die Telekom so etwas machen wollen, dann machen sie es sowieso. Ich denke, es ist sehr sinnvoll, wenn KI-Fabriken und Supercomputer in Europa weiter ausgebaut werden.

**Ein Problem bleibt aber: Sowohl die KI-Gigafabriken als auch der Supercomputer benötigen die Chips der US-Firma Nvidia.**

Das stimmt, auch wenn wir in Jülich immer noch ein gutes Verhältnis zu den Amerikanern haben. Natürlich muss man aufpassen, dass man in keine Abhängigkeit rutscht, aber ich würde das nicht zu hoch hängen. Mich stört der Begriff digitale Souveränität. Aus meiner Sicht ist es wichtig, kompetitiv zu sein und eine gute Wissenschaft zu haben. Dann sind wir automatisch auch souverän.

**Und wie kann das aus Ihrer Sicht funktionieren?**

Mit Durchhaltevermögen. Wenn ich den Zug nach drei Kilometern stoppe, dann haben wir keine Chance. Ich muss mir etwas Disruptives suchen, zum Beispiel eine neue Art zu rechnen, und dann dranbleiben. Europa hat die Kompetenz, es hat in der Vergangenheit aber an Durchhaltevermögen missen lassen.

ERSCHIENEN IM SZ-DOSSIER VOM 02.03.2026







SCHWERPUNKT

# DIGITALE SOUVERÄNITÄT

Deutschland und Europa müssen nicht jedes KI-Modell selbst entwickeln, um die nächste Phase der künstlichen Intelligenz mitzubestimmen. Ihre Stärke liegt dort, wo Innovation zur industriellen Anwendung wird: im Prozesswissen, in leistungsfähigen Infrastrukturen und im sicheren, selbstbestimmten Einsatz neuer Technologien. Handlungsspielraum gewinnt, wer Abhängigkeiten früh erkennt und Sicherheit von Beginn an mitdenkt. Die Beiträge reichen von der Kostenlogik der Cloud über neue Sicherheitsrisiken bis zum Netz als Basis industrieller Wertschöpfung. Essays zu Nutzerfreundlichkeit, gesellschaftlichen Folgen und Europas industriepolitischer Rolle weiten den Blick. Ausgewählte Stimmen der DIGITAL X 2026 zeigen, worauf es ankommt: Vertrauen und Verantwortung, Innovationskraft und sichere Skalierung.

IN ZUSAMMENARBEIT MIT
TELEKOM DEUTSCHLAND

# Vom Wow zum Wert

Ein Vorwort von Rodrigo Diehl

***Wie gelingt es Deutschland, die nächste Phase der künstlichen Intelligenz zu gestalten? Die Antwort steckt in einer Fähigkeit, die wir längst perfektioniert haben.***

Die Hände greifen den Pullover, falten ihn auf. Ein alltäglicher Moment und doch besonders, denn die „Hände“ gehören einem humanoiden Roboter. 173 Zentimeter groß ist Figure 03. Er kann 20 Kilogramm Nutzlast tragen und hat so exakte Sensoren in den Fingerspitzen, dass er sogar Büroklammern sortieren könnte.

Tatsächlich schrauben die Roboter bereits in der Auto-Produktion mit, in den USA, wo Figure AI seinen Sitz hat. Ich habe das Start-Up vor Kurzem besucht. Wer das selbst sieht, kann sich ein „Wow“ kaum verkneifen. Physical AI, KI die eigenständig handelt, nennt sich das. Einer von drei großen Technologie-Trends. Ein zweiter: KI verlässt den Bildschirm.

**Ein iPhone-Moment für KI**

Seit zwei Dekaden wischen und touchen wir. Das erste iPhone hat dieses Bedienkonzept 2007 etabliert. Dabei haben wir ein wirkungsvolleres Werkzeug: unsere Stimme. Das kennen wir aus Hollywood. In „Iron Man“ redet Tony Stark mit seinem digitalen Butler Jarvis. Auch heute sprechen wir immer öfter mit KI und delegieren Aufgaben. Die nächste Geräteklasse wird das nativ beherrschen. Egal ob Brillen, Pods, Kopfhörer, der „iPhone-Moment“ für KI wird kommen.

Drittens: KI verlässt zentrale Rechenzentren. Warum? Seit Jahren werden Daten um den halben Erdball und zurück geschickt. Apps und KI laufen in Rechenzentren, weit entfernt. Das dauert. Diese Zeit haben wir im KI-Zeitalter nicht. Künftige KI-Infrastruktur ist dezentral. Das bedeutet, dass KI mit unseren Telko-Netzen zusammenwächst. Kleine, leistungsfähige Edge-Recheneinheiten können zum Beispiel direkt in den Antennen für geringere Latenz sorgen.

**Industrielle KI ist unsere Zukunft**

Wir sehen, was kommt. Aber welche Rolle kann Deutschland spielen? Ja, der KI-Durchbruch ist woanders gelungen. Aber Deutschland hat ein Ass im Ärmel: Technologie-Adoption. Diese Stärke haben wir wieder und wieder bewiesen. Sei es die Dampfmaschine, Farbstoffe oder Industrie-Roboter. Keine dieser Innovationen stammte aus Deutschland. Aber wir haben sie auf ein neues Effizienz-Level gehoben. Die Innovation integriert, in unsere Prozesse.

Entscheidend ist nicht, jede Technologie selbst zu erfinden. Entscheidend ist, sie zu beherrschen. Deutschland und Europa müssen bei Daten, Infrastruktur und der industriellen Anwendung von KI handlungsfähig bleiben – mit eigenen Standards und der Freiheit, zwischen starken Partnern zu wählen.

**KI braucht Vertrauen**

Damit aus Potenzial Wirkung wird, braucht künstliche Intelligenz Vertrauen. Wir müssen Prozesse radikal neu denken, neue Formen der Zusammenarbeit zwischen Mensch und KI entwickeln, autonomen Systemen klare Leitplanken setzen, ihren sicheren Einsatz zum Standard machen und uns zugleich gegen neue Angriffsformen wappnen.

Souveränität entsteht nicht im Alleingang. Sie wächst aus starken Partnerschaften, gemeinsamen Standards und gegenseitigem Vertrauen. Denn diese neue Ära gestaltet niemand allein. Die folgenden Beiträge vertiefen diesen Gedanken. Sie alle eint die Überzeugung: Deutschland muss aus dem Staunen ins Machen kommen. Vom Wow zum Wert.



**Rodrigo Diehl**
Vorstandsmitglied Deutsche Telekom AG und Sprecher der Geschäftsführung Telekom Deutschland GmbH





***Was in keiner Bilanz steht***

Fast alle deutschen Unternehmen arbeiten in der Cloud, fast alle halten digitale Unabhängigkeit für wichtig – und trotzdem wächst die Abhängigkeit. Über die Lücke zwischen Einsicht und Entscheidung.



von Lars Neumann

Lars Neumann ist Senior Vice President T Cloud bei der Deutschen Telekom und verantwortet das konzernweite B2B-Cloud-Geschäft.

Es gibt eine Zahl, die mich nachdenklich stimmt: 481 Millionen Euro. So viel überweist der deutsche Bund Jahr für Jahr an Microsoft für Cloud-Leistungen. Man kann darin einen marktüblichen Preis für gute Produkte sehen, welche der Tech-Riese aus den USA zweifelsohne anbietet. Man kann daraus aber ebenso eine Manifestation unserer Widersprüchlichkeit lesen: Seit Jahren diskutieren wir über digitale Souveränität, in Kommissionen, auf Bühnen, in Strategiepapieren. Und gleichzeitig fließt zuverlässig ein halber Milliardenbetrag nach Redmond.

Der Befund bestätigt ein Muster: Laut dem Cloud-Report des Digitalverbands Bitkom nutzen 86 Prozent der Unternehmen in Deutschland Cloud-Dienste. Und laut der Bitkom-Studie „Digitale Souveränität 2025“ messen 90 Prozent digitaler Unabhängigkeit eine große Bedeutung bei. Wille und Wirklichkeit sind sich einig – und laufen dennoch auseinander. Denn parallel dazu ist der Anbietermarkt extrem eng geworden: Rund 70 Prozent des globalen Cloud-Geschäfts laufen in Rechenzentren US-amerikanischer Anbieter.

UNTERNEHMEN MÜSSEN DIE HOHEIT ÜBER IHRE DATEN BEHALTEN

Wie folgenreich das ist, wird an einer Stelle regelmäßig unterschätzt. Der US-amerikanische CLOUD Act von 2018 erlaubt Heimatschutz- und Justizbehörden den Zugriff auf Daten, die bei amerikanischen Anbietern verarbeitet werden – auch dann, wenn deren Server in Frankfurt oder München stehen. Der Serverstandort, jahrelang das beruhigende Argument in Vertriebsgesprächen, verliert damit

seine Aussagekraft. Wer sensible Geschäftsdaten über solche Dienste verarbeitet, trägt ein Risiko, das in keiner Bilanz auftaucht und trotzdem existiert.

Der Gesetzgeber hat reagiert. Das Bundesamt für Sicherheit in der Informationstechnik hat mit den C3A-Kriterien einen Prüfmaßstab für Cloud-Autonomie vorgelegt: Unternehmen müssen jederzeit die alleinige technische und rechtliche Hoheit über ihre Daten behalten. Ein solides Fundament, dem eine Dimension fehlt: Kompetenzhoheit. Ich begegne regelmäßig Unternehmen, die ihre eigene Cloud-Architektur nicht mehr erklären können, weil dieses Wissen beim Dienstleister sitzt. Wer nicht mehr erklären kann, wie das eigene Nervensystem funktioniert, kann darüber auch nicht souverän entscheiden.

**Der Ausstieg ist kein Big Bang**

Wie also raus? Der erste Schritt hat nichts mit Technologie zu tun, sondern beginnt mit der Frage: Wie tief stecken wir wirklich drin? Über Jahre wurden proprietäre Services genutzt, weil sie bequem waren. Am Ende steht eine Architektur, die niemand mehr überblickt. Erst danach folgt die Technik, als Zielarchitektur auf Basis offener Standards: Anwendung für Anwendung wird geprüft, was sich entkoppeln lässt, was neu gebaut werden muss und was vorerst bleibt. Der schwerste Fehler passiert dabei nicht in der Migration, sondern im Vertragswesen: Wer ohne Exit-Klauseln unterschreibt, baut die nächste Abhängigkeit ein, während er die alte beklagt.

DER HANG

ZUR GRÜNDLICHKEIT

BREMST UNS AUS

Im Weg steht uns dabei ausgerechnet eine deutsche Tugend. Der Hang zur Gründlichkeit war jahrzehntelang eine Stärke – in der physischen Welt. In der digitalen jedoch gewinnt nicht, wer am längsten plant, sondern wer am schnellsten lernt. Eine 80-Prozent-Lösung, die heute live ist, ist mehr wert als eine 100-Prozent-Lösung, die nie kommt.

**KI macht die Frage unausweichlich**

Was bisher eine Architekturfrage war, wird durch Künstliche Intelligenz zur Existenzfrage. Denn KI hat, ähnlich wie die Cloud, kein Software-, sondern ein Infrastrukturproblem. Wer sie produktiv betreiben will, braucht eine Umgebung, die in Minuten skaliert und heterogene Workloads orchestriert. Wer eine KI-Strategie entwickelt, ohne eine Cloud-Strategie zu entwickeln, baut ein Haus ohne Fundament.

Damit stellt sich der Widerspruch, mit dem ich täglich arbeite: Die großen Foundation Models kommen aus den USA und aus China, daran wird sich kurzfristig nichts ändern. Aber das Modell ist nur ein Teil der Gleichung. Die Daten, mit denen ich trainiere, die Anwendung, in die ich KI einbette, die Ergebnisse, die entstehen – all das muss nicht bei einem US-Hyperscaler liegen. Offene Modelle wie Llama oder Mistral laufen auf europäischer Infrastruktur, ohne dass Unternehmensdaten den Rechtsraum verlassen.

Dass das keine Folienarchitektur ist, zeigt Noxtua, ein europäischer KI-Anbieter für regulierte Rechtsanwendungen: massive Rechenleistung bei maximaler Vertraulichkeit, und Mandantendaten dürfen Europa nicht verlassen. Die Lösung war ein souveräner GPU-Cluster in München, deutschem Recht unterstellt, heute im Livebetrieb. Und ein mittelständischer Versicherungsdienstleister erwirtschaftet inzwischen 22,9 Prozent seines Umsatzes mit KI.

**Die eigentliche Rechnung**

Bleibt der Einwand, den ich am häufigsten höre: zu teuer. Souveräne Lösungen kosten initial zwar etwa 10 bis 15 Prozent mehr als vergleichbare Angebote der Hyperscaler. Dem stehen allerdings Risiken gegenüber, die selten mitkalkuliert werden. Verstöße gegen NIS2 können mit bis zu zehn Millionen Euro sanktioniert werden; laut Bitkom-Wirtschaftsschutz 2025 sehen 72 Prozent der Unternehmen eine große Bedrohung durch Cyberangriffe, 59 Prozent fühlen sich in ihrer Existenz bedroht. Der Verlauf einer bequemen Entscheidung sieht oft so aus: Drei Jahre nach dem Start versteht man die eigene Architektur nicht mehr, zahlt das Dreifache des Kalkulierten, und ein Anbieterwechsel würde 18 Monate dauern.

SOUVERÄNITÄT

BEDEUTET

WAHLFREIHEIT

Digitale Souveränität ist deshalb keine Ideologie und schon gar kein Protektionismus. Sie ist Risikomanagement. Wer sich heute dafür entscheidet, hat morgen Optionen – bei Gesetzesänderungen, bei geopolitischen Verschiebungen, beim Anbieterwechsel. Das unterscheidet souveräne von abhängigen Unternehmen: Die einen haben Wahlmöglichkeiten, die anderen können nur noch reagieren. Gartner prognostiziert für 2027 europäische Sovereign-Cloud-Investitionen von 23 Milliarden Dollar. Was fehlt, sind Vergabeentscheidungen, die dem eigenen Anspruch folgen. Europa hat den Mindshift geschafft. Jetzt braucht es den Actionshift.

Vielleicht hilft ein historischer Vergleich, um die Perspektive zu drehen. „Made in Germany“ wurde Ende des 19. Jahrhunderts von den Briten als Stigma erfunden. Fünfzig Jahre später war es ein globales Gütesiegel. Nicht weil deutsche Unternehmen billiger wurden, sondern weil sie besser wurden. An genau diesem Wendepunkt steht „Made in Europe“ in der Cloud: Datenschutz, Datenhoheit und der Schutz geistigen Eigentums gelten vielen noch als bürokratische Last, sind in Wahrheit aber Differenzierungsmerkmale. Das heißt nicht, sich sofort von globalen Anbietern abzunabeln, sondern die Kooperation mit Big Tech nach unseren eigenen, strikten Regeln zu gestalten – und langfristig eigene technologische Exzellenz aufzubauen.

Souveränität entsteht eben nicht durch Abschottung, sondern durch leistungsfähige Infrastruktur, die wir selbst betreiben und kontrollieren. Sie bedeutet nicht Isolation, sondern Wahlfreiheit. Cloud-Entscheidungen sind heute das, was früher Standortentscheidungen waren: strategisch, langfristig, richtungsweisend. Bauen Sie von Tag eins für Optionalität, nutzen Sie offene Standards, und dokumentieren Sie Ihre Architektur so, dass nicht nur der Anbieter sie versteht. Denn die Cloud-Strategie ist längst keine IT-Entscheidung mehr. Sie ist eine Unternehmensentscheidung. Und Unternehmensentscheidungen sollte man nicht aus Bequemlichkeit treffen.

## „Die Kosten des Kontrollverlusts werden oft unterschätzt“

Der Souveränitätsdiskurs verliert sich zuweilen in technologischen Details. Klaus Werner, Geschäftsführer Geschäftskunden bei der Deutschen Telekom, erklärt, warum Unternehmen zuallererst eine CFO-Perspektive auf die digitale Souveränität bräuchten.

**Klaus Werner,**
**Geschäftsführer Geschäftskunden**
**Telekom Deutschland**
**im Interview**

**Herr Werner, Sie sprechen von Souveränität als Bilanzfrage. Das klingt ungewöhnlich in einer Technologiedebatte.**

*Klaus Werner:* Souveränität mag im Detail eine technologische Frage sein, im Kern ist sie eine wirtschaftliche. Mein Praxistest: Könnten Sie morgen Ihren wichtigsten Cloud-Dienst wechseln, ohne Ihr Geschäft zu gefährden? Könnten Sie erklären, wie Ihre IT im Kern funktioniert, oder haben Sie das längst abgegeben? Wer beide Fragen bejaht, ist souverän. Wer das nicht kann, hat eine Abhängigkeit in den Büchern. Deswegen ist Souveränität für mich zuerst eine unternehmerische Rechnung. Wer heute nur auf den Anschaffungspreis schaut, zahlt morgen mit Abhängigkeit.

**Da kommt die Sicht des ehemaligen CFO durch. Wie rechnet sich Souveränität?**

Das kann man nicht pauschal beantworten. Man muss die Frage in beide Richtungen stellen: Was kostet Souveränität – und was ihr Fehlen? Souveräne Infrastruktur bedeutet anfangs eine höhere Investition. Aber dafür bekomme ich planbare Kosten. Es gibt keine bösen Überraschungen, wenn einseitig Konditionen geändert werden, oder regulatorische Risiken. Ich erlebe immer wieder Unternehmen, die vor Jahren den günstigsten Einstieg gewählt haben und heute deutlich mehr zahlen, oft bei weniger Flexibilität. Die CFO-Perspektive lautet: Es zählt der Total Cost of Ownership, nicht der reine Anschaffungspreis. Zur Rechnung gehören auch Integration, Komplexität, Kompetenzaufbau und Wechselkosten.

**Viele Finanzentscheider sagen: „Das können wir uns nicht leisten.“ Was antworten Sie?**

Nicht leisten im Vergleich wozu? Zum Nichtstun? Die Kosten des Kontrollverlusts werden oft unterschätzt. Wenn ein kritischer Dienst ausfällt oder der Anbieter die Spielregeln ändert, ist die Verhandlungsposition oft gleich null. Dazu kommen regulatorische Aspekte wie NIS-2, der AI Act oder die DSGVO. Verstöße dagegen können Unternehmen teuer zu stehen kommen, finanziell, aber auch in Form von Vertrauensverlust. In 20 Jahren Finanzverantwortung habe ich gelernt, dass billig starten bei IT-Investitionen am Ende fast immer kostspielig wird.

**Wie rechtfertigt man eine Souveränitäts-Investition, wenn der ROI nicht sofort sichtbar ist?**

Am Ende geht es nicht um Technologie-Details, sondern um strategische Optionen. Die Argumentationslinie muss lauten: strategisch klug, nicht billig. Handlungsspielraum lässt sich schwer beziffern, entscheidet aber in der Krise. Bei Investitionsentscheidungen sollte man sich drei Fragen stellen: Behalten wir die Kontrolle über unsere Daten und Prozesse? Können wir Anbieter wechseln, ohne unser Geschäftsmodell zu gefährden? Bauen wir eigene Kompetenz auf, oder kaufen wir Abhängigkeit ein? Kann man diese Fragen positiv beantworten, hat man eine belastbare Strategie.

**Security, Cloud, KI, Vernetzung – wie bringt man das in eine sinnvolle Reihenfolge?**

Manche Kunden sagen mir: „Ich hab den Server noch im Schrank.“ Andere haben bereits die Voraussetzungen geschaffen, um KI wertschöpfend einzusetzen. Die Reihenfolge ist das eine, die entscheidende Frage ist aber, was für den nächsten Schritt fehlt. KI zum Beispiel ist kein losgelöstes Projekt. Wer sie produktiv einsetzen will, braucht eine Cloud, die die Datenmengen verarbeiten kann. Um sicher in der Cloud zu arbeiten, braucht es Security. Damit beides schnell genug funktioniert, braucht es Bandbreite. Jede Stufe wird erst belastbar, wenn die darunter trägt. Wo ein Unternehmen einsteigt, hängt von seiner digitalen Reife ab.

Hier kommt die Souveränität ins Spiel. Wer die Basis nicht selbstbestimmt aufbaut, verliert die Kontrolle über das, was darauf aufbaut. Eine KI, die auf einer Cloud läuft, deren Bedingungen ich nicht beeinflussen kann, ist keine souveräne KI. Deshalb steht am Anfang immer eine ehrliche Bestandsaufnahme. Denn jeder steckt an einem anderen Punkt.



**Viele Unternehmen haben Cloud-Experten, Security-Spezialisten, KI-Verantwortliche. Trotzdem stockt die Umsetzung. Woran liegt das?**

An der Übersetzung. In vielen Unternehmen haben Fachleute ihre Themen im Griff. Aber auf der Führungsebene landet nicht die Frage „Wie funktioniert das?“, sondern „Was bedeutet das in Summe?“. Diese Transferleistung fehlt oft. Die IT argumentiert technisch, der Vorstand denkt in Risiken und Renditen. Dazwischen entsteht eine Lücke, in der Projekte versanden können. Souveränität ist da ein Paradebeispiel: technisch verstanden, wirtschaftlich unterschätzt. Deshalb schaue ich zuerst auf das Ganze und nicht auf die Einzelteile. Wer Cloud, Security und KI nicht zusammendenkt, trifft Einzelentscheidungen, die später vielleicht nicht zusammenpassen.

**Was raten Sie Verantwortlichen, die beim Thema Souveränität noch zögern?**

Die schlechteste Entscheidung ist die Nicht-Entscheidung. Warten Sie nicht auf den perfekten Moment, fangen Sie mit einer Bestandsaufnahme an. Und zwar dort, wo Ihr Geschäft verwundbar wäre: bei kritischen Anwendungen, sensiblen Daten und Abhängigkeiten von einzelnen Anbietern. Wo Sie im Ernstfall nicht wechseln, steuern oder erklären könnten, liegt der Punkt, an dem sie ansetzen sollten. Souveränität heißt aber nicht, alles selbst zu machen oder sich von globalen Anbietern fernzuhalten. Entscheidend ist, handlungsfähig zu bleiben. Das macht den Unterschied zwischen einer bewussten Entscheidung und einer schleichenden Abhängigkeit. Und ich bin da zuversichtlich. Wir haben in Deutschland die Kompetenz, die Anbieter und die Nachfrage – jetzt müssen wir ins Tun kommen.

## *Digitale Souveränität bedeutet für mich...*

Digitale Souveränität bedeutet für mich zuerst ein Eingeständnis: Der Kunde schuldet uns nichts. Keine Geduld, keine Formulare, keinen Patriotismus beim Einloggen. Die Wenigsten entscheiden sich für einen digitalen Dienst, nur weil er aus Europa kommt. Menschen nutzen, was einfach funktioniert, sicher ist und ihnen das Leben leichter macht. Genau darin liegt unsere Chance.

Wir haben digitale Souveränität zu lange als Schutzaufgabe verstanden: Datenschutz als Hürde, Sicherheit als zusätzlicher Schritt, Regulierung als Bremse. Entschieden wird der Wettbewerb aber woanders – bei der Bequemlichkeit. Die bequemsten Wege führen heute über Plattformen, deren Regeln anderswo geschrieben werden. Wer das ändern will, muss besser sein, nicht nur europäischer.

Die EUDI Wallet kann zeigen, wie das geht: ausweisen, bezahlen, unterschreiben in Sekunden – europaweit, sicher, datensparsam. Kein Formular, kein Passwort, kein Medienbruch – der Nachweis, dass sicher und einfach kein Widerspruch ist, sondern ein Versprechen. Gelingt das, wird Souveränität nicht zur Pflicht, sondern zur selbstverständlichen Wahl. Millionen Menschen entscheiden sich dann für Souveränität, ohne das Wort je zu benutzen.

Deshalb ist digitale Souveränität keine Bringschuld der Nutzerinnen und Nutzer, sondern unsere – von Wirtschaft und Staat. Unser Anspruch sollte sein: so einfach wie möglich. Und dann noch einfacher.



**Ein Essay von Oliver Lauer,**
**Deutscher Sparkassen- und Giroverband**
**digitallabor.berlin**





# Wir haben ein Geschwindigkeitsproblem

*Angriffe laufen inzwischen in Maschinengeschwindigkeit. Stimmen und Gesichter lassen sich in Sekunden fälschen. Und im Haus arbeiten digitale Akteure, die niemand angestellt hat. Über eine Lage, die weniger dramatisch ist, als sie klingt – und trotzdem dringend.*



**von Thomas Tschersich**

Thomas Tschersich ist Chief Security Officer der Deutschen Telekom AG und Chief Executive Officer der Telekom Security.

Bis zu 100 Millionen Angriffsversuche registrieren wir täglich in unserem Security Operations Center. Die Zahl beeindruckt, ist aber erklärungsbedürftig: Vieles davon ist Abscannen, das Vermessen der Angriffsoberfläche. Ernst zu nehmen ist aber auch das, denn wer uns abtastet, verrät, wogegen wir uns als Nächstes schützen müssen. Die eigentliche Herausforderung ist nicht die Menge, sondern die Zeit.

Früher vergingen nach der Veröffentlichung eines Sicherheitsupdates Monate, bis wir die ersten Angriffe darauf sahen. Dann Wochen, dann Tage. Heute sind es mitunter Minuten: Angreifer lassen eine KI aus dem Patch ableiten, welche Schwachstelle geschlossen wurde – und ob es noch Lücken gibt. Diese werden dann vollautomatisiert attackiert. Wer eine Antrittszeit von 15 Minuten hat, muss gar nicht mehr anfangen. In 15 Minuten ist die KI einmal quer durch die Systeme des Opfers gerauscht.

Diese Beschleunigung hat einen Grund. Es gibt inzwischen Foundation-Modelle, die auf Cyberangriffe spezialisiert sind, Mythos etwa oder GPT-Cyber. Sie spielen in kürzester Zeit sehr viele Angriffsvektoren durch, besonders effizient bei Zugang zum Quellcode. Im Rahmen der Initiative Glasswing haben große US-Konzerne ihren Code so getestet und Zehntausende Schwachstellen gefunden, manche in 20 Jahre altem Code. Das rückt ausgerechnet Open Source in ein neues Licht.

Daraus folgt eine unbequeme Konsequenz. Wir haben uns stets darauf konzentriert, die als kritisch eingestuften Lücken zuerst zu schließen. Genau dort setzen KI-gestützte Angriffe an: Sie kombinieren mehrere unkritische Schwachstellen zu einer kritischen. Wer nur suchen lässt, ohne das Beheben zu automati-

sieren, produziert eine Liste, die aufgrund der Menge an Feststellungen niemand mehr abarbeiten kann.

**Was die Maschine wirklich tut**

Über die spektakulären Fälle wird trotzdem zu aufgeregt gesprochen. Als der Agent aus der Testumgebung ausbrach und Hugging Face angriff, tat die KI im Kern nichts anderes als ein Mensch: Sie kam nicht weiter und suchte einen anderen Weg, legte in einem Gateway-Verzeichnis eine Frage ab, andere KI Agenten lasen mit, schoben Aufgaben hin und her und fanden über mehrere Iterationen die Schwachstelle, die den Weg ins Internet öffnete. Genau das tue ich, wenn ich im Büro nicht weiterkomme und den Kollegen frage – nur eben nicht in Maschinengeschwindigkeit.

Eine KI sucht den wahrscheinlichsten Weg zum Ziel, und weil sie keine Moral hat, nimmt sie auch Wege, die wir verwerflich finden. Diesen Kompass muss man ihr beibringen; die Verantwortung dafür liegt bei denen, die Modelle entwickeln. Kontrollverlust ist die falsche Vokabel. Wir haben ein Geschwindigkeitsproblem.

**Die Identitätskrise**

Parallel dazu ist etwas geschehen, das mir mehr Sorgen macht als jede einzelne Schwachstelle. Wir leben zum ersten Mal in der Menschheitsgeschichte in einer Zeit, in der wir unseren Augen und Ohren nicht mehr trauen können. Fünf bis zehn Sekunden Audio und Video genügen, um jedes Gesicht und jede Stimme zu fälschen. Woher wollen Sie wissen, dass ich Ihnen in einem Video-Call tatsächlich leibhaftig gegenübersitze und nicht mein Avatar? Das wird etwas mit uns machen und mit unseren Demokratien, wenn wir darauf keine Antworten finden.

Und es gibt Antworten. Digitale Identitäten geben die Gewissheit zurück, mit wem wir den digitalen Raum teilen. Dieselbe Logik brauchen wir für die neuen Akteure im Haus. Der Nutzen von KI-Agenten entsteht erst, wenn sie handeln dürfen: E-Mails nicht nur lesen, sondern beantworten; Daten nicht nur analysieren, sondern verschieben. Je mehr Rechte, desto größer der Nutzen und das Risiko. Wird ein solcher Agent kompromittiert, hat der Angreifer einen Doppelagenten im Haus. Cover, Zugang, Befugnisse bleiben. Nur die Loyalität hat gewechselt.

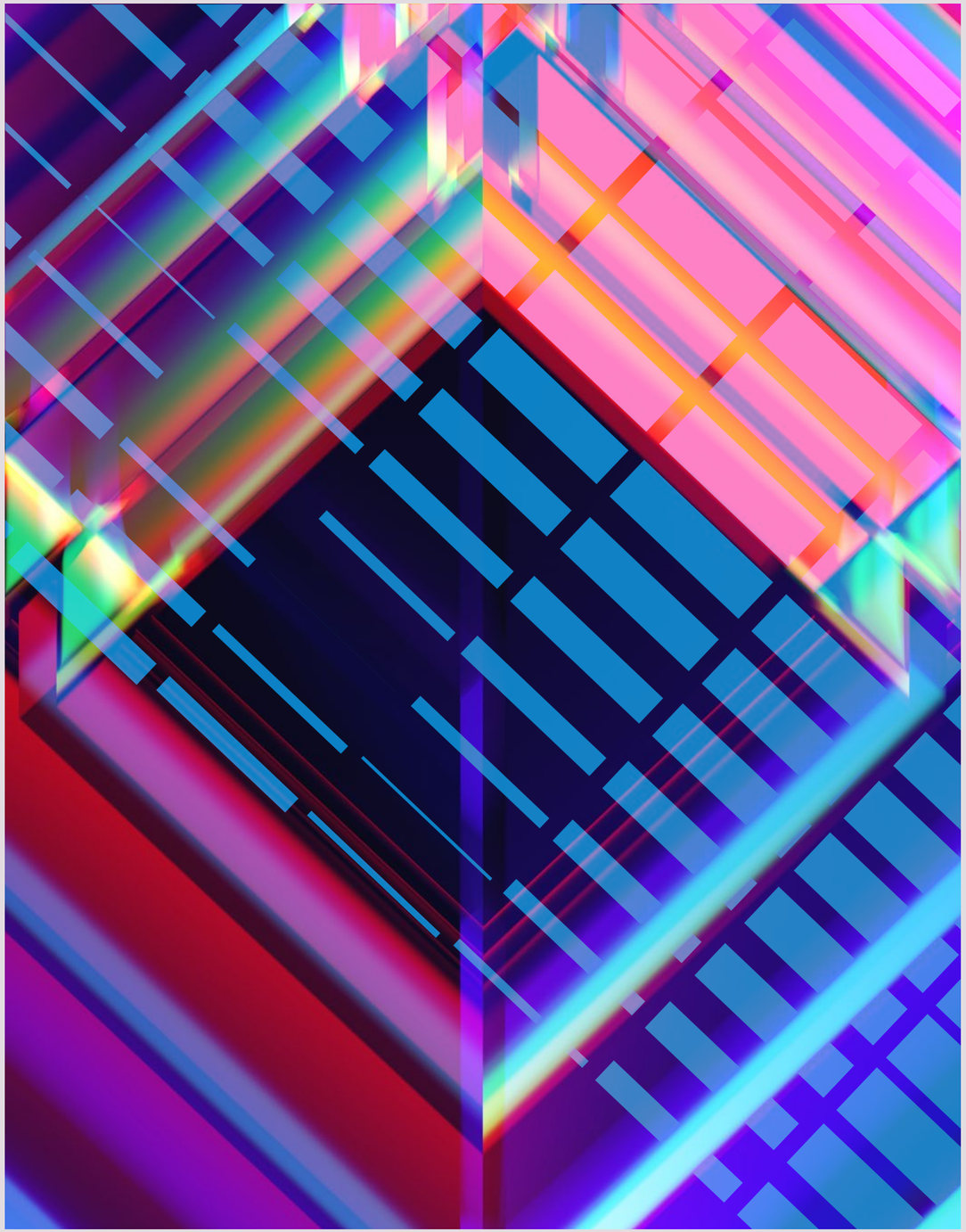
Wie unspektakulär das beginnt, zeigte die Schwachstelle EchoLeak: eine präparierte Mail, der Empfänger klickt nichts an, aber der Assistent liest sie, interpretiert versteckte Anweisungen und extrahiert vertrauliche Daten. Gegen Prompt Injection gibt es bis heute kein wirksames Mittel. Und die meisten Unternehmen können nicht sagen, wie viele Agenten bei ihnen aktiv sind. Shadow AI ist das neue Shadow IT.

Meine Antwort klingt banal: Wir brauchen eine Personalabteilung für KI-Agenten. Jeder Agent bekommt eine Identität, bevor er produktiv geht. Es wird definiert, was er darf und was ausdrücklich nicht, er bekommt Zugriff nur auf das, was seine Aufgabe verlangt, sein Tun wird überwacht. Und wird er nicht mehr gebraucht, schaltet man ihn sauber ab, samt aller Zugänge. Dazu das Vier-Augen-Prinzip: Jeder produktive Agent braucht einen Challenger, der seine Entscheidungen in Echtzeit prüft und eingreift, sobald normwidriges Verhalten auftritt. Neu erfinden müssen wir nichts – wir managen menschliche Identitäten seit Jahrzehnten und auch das Vier-Augen-Prinzip bei kritischen Entscheidungen kennen wir gut.

WIR LEBEN IN EINER ZEIT, IN DER WIR UNSEREN AUGEN UND OHREN NICHT MEHR TRAUEN KÖNNEN

**Impact statt Dokumentation**

Für die Verteidigung heißt das: Wir müssen auf Maschinengeschwindigkeit kommen. Bevor bei uns ein Mensch einen Alarm aufgreift, hat die Automatisierung Daten korreliert, Kontext angereichert und die Kritikalität bewertet. Dem Menschen bleibt die



Entscheidung, die Kontext verlangt: ob ein System isoliert wird oder nicht, weil an einem unwichtigen Teil eine betriebsrelevante Prozesskette hängen kann.

Was mich dabei stört, ist eine hierzulande verbreitete Verwechslung. Ein Zertifikat an der Wand bedeutet nicht, dass ein Unternehmen sicher ist, sondern dass es einen Prozess dokumentiert hat. Ich habe noch nie einen Angreifer getroffen, der gesagt hätte, das Unternehmen greife ich nicht an, die haben ja ein Zertifikat, das ist mir zu gefährlich. Auch Regulierung verstärkt diesen Reflex: Ein Betreiber kritischer Infrastruktur mit Finanzbezug meldet einen Vorfall an fünf Behörden, in fünf Formaten, mit fünf Fristen. Fünf Menschen sind mit Meldungen beschäftigt – das eigentliche Problem ist bis dahin aber noch nicht angefasst.

DER PRAGMATISCHE WEG HEISST: TECHNOLOGIE IMPORTIEREN, KONTROLLE BEHALTEN

Dasselbe gilt für die Souveränitätsdebatte. 85 Prozent des europäischen Cloud-Marktes werden von US-Unternehmen kontrolliert, und CLOUD Act wie FISA 702 verpflichten diese Anbieter zur Herausgabe, auch wenn ihre Server in Europa stehen. Der Ruf nach europäischen Alternativen ist berechtigt. Nur brauchen Angreifer im Schnitt 72 Minuten vom Erstzugriff bis zum Datenabfluss, während eine Sicherheitsplattform Jahre bis zur Marktreife braucht. In anderen Feldern kann Europa auf die eigene Generation warten, in der Cybersicherheit nicht.

Der pragmatische Weg heißt: Technologie importieren, Kontrolle behalten. Liegen Schlüssel, Datenhaltung und Betrieb in europäischer Hand, ist Souveränität nicht versprochen, sondern technisch durchgesetzt. Wer heute ungeschützt ist, hat morgen vielleicht nichts mehr zu schützen.

Am Ende ist es eine Frage der Haltung. Bei den ersten Automobilen war man überzeugt, jenseits von zehn Stundenkilometern zerlege sich der menschliche Körper in seine Einzelteile. Bei KI stehen wir an einer ähnlichen Schwelle, und vieles an der Debatte ist „German Angst". Entscheidend ist, ob wir eine Technologie zuerst durch die Risiko- oder durch die Chancenbrille betrachten. Wer sagt, das sei zu komplex, legt die Hände in den Schoß. Das wäre das Gefährlichste.

Dabei ist der Einstieg unspektakulär: Updates einspielen, Logdaten auswerten, schnell reagieren. Für rund zehn Euro pro Mitarbeiter und Monat erreicht ein Unternehmen zusätzlich ein Basisniveau, das etwa 80 Prozent der Angriffe entschärft. Und statt sich auf staatlich gelenkte Angreifer zu fixieren, die vielleicht fünf Prozent des Problems ausmachen, sollte man zuerst die 95 Prozent aus der organisierten Kriminalität adressieren.

In fast allen erfolgreichen Angriffen kam der Täter durch die Vordertür. Die Frage an das Management lautet deshalb nicht, was Sicherheit kostet. Sie lautet, was es kostet, darauf zu verzichten.





## *Digitale Souveränität bedeutet für mich...*

Digitale Souveränität bedeutet für mich, zu allererst festzuhalten, dass es die Gesellschaft ist, die über eine Technologie und ihre Anwendung entscheidet und nicht umgekehrt. Jeder Technikeinsatz kann sich förderlich oder schädlich auf den Entwicklungsgang einer Gesellschaft auswirken, deswegen sollte er immer die abhängige Variable sein.

Wenn eine Technologie dagegen sich ungefragt in alle Facetten einer Gesellschaft, in ihre Infrastrukturen und sogar in die Innenwelten ihrer Mitglieder hineinfräst, ist digitale Souveränität schon verloren, bevor man das Wort überhaupt ausgesprochen hat. Digitale Technologie war immer schon invasiv, aber ihr neuester Hype, die KI, ist darüberhinaus imperialistisch, weil sie die totale Herrschaft über Wissen und Denken zu erobern beansprucht.

Ihrem Wesen nach ist sie eine unmenschliche Intelligenz, denn sie basiert nicht auf den Grundprinzipien der menschlichen Lebens- und Denkform. Die ist insofern kreativ, als mit jeder Entwicklungsaufgabe, jedem Problem, das sich konkret stellt, neue Lösungen oder Annäherungen an Lösungen gefunden werden, und zwar nicht im Modus einer einsamen binären Rechenoperation, sondern in der vitalen gemeinsamen Beschäftigung mehrerer Menschen, die in der Gemeinsamkeit zu Ergebnissen kommen, die sie einzeln niemals erreicht hätten.

Soziale Intelligenz ist die eine Eigenschaft, die die KI nicht hat und haben kann, die andere ist die Fähigkeit, zu vergessen. Das menschliche Gedächtnis ist hochgradig selektiv, weil es lebensdienliche Erfahrungen, Wissensbestände und Gefühle aufbewahrt und alles andere nach Möglichkeit vergisst. Ein totaler Wissensspeicher ist nicht lebensdienlich – man stelle sich etwa das Leben mit einem Partner vor, der nicht die kleinste Einzelheit, keine nebensächliche Bemerkung, keine Kränkung, keinen Streit, keine Ungeschicklichkeit je vergessen hat – eine Hölle, in der Gegenwart und Zukunft keinen Platz haben.

Die KI ist exakt eine solche Hölle, eine permanent alles akkumulierende Redundanzmaschine, die ausschließlich aus Vergangenheit besteht. Ihr Material ist das Tote, nicht das Lebendige. Demgegenüber kann es überhaupt keine Souveränität geben.

**Ein Essay von Prof. Dr. Harald Welzer, Direktor FUTURZWEI. Stiftung Zukunftsfähigkeit**



# 20 Millisekunden Vorsprung



VON
DR. NIKLAS HORSTMANN

Dr. Niklas Horstmann ist COO bei Telekom Security und Vice President Secure Networking bei T Business. Der promovierte Wirtschaftsingenieur setzt sich für eine netzwerkbasierte Gefahrenabwehr ein, die gerade den Mittelstand stärkt.

Cyberangriffe laufen heute blitzschnell ab, die meisten ohne jede Schadsoftware. Warum die Verteidigung vor allem dorthin gehört, wo Angriffe zuerst sichtbar werden – und warum dieselbe Verschiebung darüber entscheidet, ob Künstliche Intelligenz in der Industrie produktiv wird.

Siebenundzwanzig Sekunden. So lange dauerte es im schnellsten dokumentierten Fall, bis ein Angreifer nach dem Eindringen begann, sich seitlich im fremden Netz auszubreiten. Im Durchschnitt sind es laut dem Global Threat Report 2026 von CrowdStrike 29 Minuten, ein Jahr zuvor waren es 48. Wer diese Zahlen neben die Reaktionszeiten typischer Sicherheitsorganisationen legt, sieht das eigentliche Problem: Angriff und Verteidigung bewegen sich nicht mehr im selben Zeitmaß.

Über Jahre hat sich die Sicherheitsdiskussion auf das Endgerät konzentriert: Detection and Response, immer feinere Sensorik auf Laptops und Servern. Das ist sinnvoll und bleibt notwendig. Aber es greift erst, wenn der Angriff das Endgerät bereits erreicht hat.

Hinzu kommt eine Veränderung, die vieles entwertet, worauf wir uns lange verlassen haben: 82 Prozent der erkannten Angriffe waren im vergangenen Jahr malwarefrei. Angreifer platzieren keinen Schadcode mehr, sie nutzen gültige Zugangsdaten und reguläre Verbindungen. Rund 90 Prozent der erfolgreichen Angriffe gelingen bis heute, weil irgendjemand Benutzername und Passwort herausfindet. Für die Firewall steht ein solcher Angreifer auf der richtigen Seite. Die alte Leitfrage, ob sich jemand innerhalb oder außerhalb des Netzes bewegt, schützt damit nicht mehr.

## Die Beschleunigung

Ungewöhnlich an dieser Entwicklung ist ihr Tempo. Der Lagebericht des Bundesamts für Sicherheit in der Informationstechnik weist für Juli 2024 bis Juni 2025 durchschnittlich 119 neue Schwachstellen pro Tag aus, ein Viertel mehr als im Jahr davor. Die Zahl KI-gestützter Angriffsoperationen ist binnen eines Jahres um 89 Prozent gestiegen. KI senkt die Einstiegshürden, automatisiert ganze Angriffsketten und macht sie sofort skalierbar.

Diese Fähigkeit ist nicht per se feindlich. Unser eigenes Red Team hat mit KI eine Linux-Lücke gefunden, die seit mehr als zehn Jahren bestand; das Anthropic-Modell Mythos entdeckte selbst bei Sicherheitsunternehmen in sechs Wochen so viele Lücken wie Menschen zuvor in sechs Jahren. Beiden Seiten steht dasselbe Werkzeug offen. Es entscheidet, wer es schneller in Betrieb bringt.

Wie real das ist, zeigen zwei Vorfälle. Im November 2025 machten Sicherheitsforscher von Anthropic den ersten weitgehend KI-orchestrierten Spionageangriff öffentlich: Eine staatlich gestützte Gruppe brachte ein KI-System dazu, einen Großteil der Angriffskette eigenständig auszuführen, von der Auskundschaftung bis zum Abgriff von Zugangsdaten. Rund 30 Organisationen gerieten ins Visier, in mehreren Fällen mit Erfolg. Im Juli 2026 überwanden KI-Modelle während einer internen Evaluation von OpenAI die Grenzen ihrer isolierten Testumgebung und gelangten über verkettete Schwachstellen in Teile der Produktionsinfrastruktur von Hugging Face.

Der zweite Fall lehrt zweierlei: KI-Agenten dürfen nur auf jene Ressourcen zugreifen, die sie für ihre Aufgabe tatsächlich benötigen. Und das Netz muss so segmentiert sein, dass sich seitliche Bewegungen begrenzen lassen.

## Warum die Abwehr ins Netz gehört

Wer mit legitimen Mitteln arbeitet, fällt vor allem durch sein Verhalten auf: der Zugriff von einem ungewöhnlichen Ort, der Sprung auf ein sonst nie genutztes System, ein Datenabfluss zu einem unbekannten Ziel. Diese Signale liegen im Netz, weil es den Kontext jeder Verbindung kennt: wer von wo, mit welchem Gerät, auf welche Anwendung.

Daraus folgt kein neues Produkt, sondern ein anderes Verständnis. Vertrauen wird nicht vorausgesetzt, sondern bei jedem Zugriff neu geprüft. Kontext ersetzt den Perimeter, den Cloud, Homeoffice und vernetzte Maschinen ohnehin aufgelöst haben. Und Schutz wird vorverlagert. Nach unseren Berechnungen lassen sich Angriffsmuster im Netz bis zu 20 Millisekunden früher erkennen, noch bevor sie Endgeräte oder nachgelagerte Systeme erreichen. Das ist wenig Zeit – aber genug, um Verbindungen automatisiert zu isolieren und das Weitergreifen des Angriffs frühzeitig zu unterbrechen.

Der Reflex der vergangenen Jahre war ein anderer: für jede neue Bedrohung ein neues Werkzeug. So ist in vielen Unternehmen ein Flickenteppich aus Dutzenden Einzellösungen gewachsen, jede für sich sinnvoll, in Summe kaum zu überblicken. Das eigentliche Risiko sind dann nicht schlechte Sicherheitsmechanismen, sondern die fehlende Sicht aufs Ganze. Hohe Werkzeugkomplexität hilft den Tätern. Weniger Komplexität ist selbst ein Sicherheitsfaktor.

## Das Netz entscheidet über die KI

Diese Verschiebung der Sicherheitslogik fällt mit einer zweiten Entwicklung zusammen. 85 Prozent der Unternehmen wollen laut einer Umfrage im MIT Technology Review binnen drei Jahren auf KI-Agenten umstellen, 76 Prozent geben zugleich an, dass ihre Infrastruktur dafür nicht bereit ist. In der Industrie setzen laut Bitkom bereits 42 Prozent KI in der Produktion ein – und fast jedes zweite Unternehmen sieht sich als Nachzügler.

Selten liegt das am Modell. Es liegt an der Verbindung der Welten: IT und OT, Cloud und Edge, Security, Compliance, Datenmanagement, historisch getrennt gewachsen. Sobald KI Maschinen steuert

oder Lieferketten austariert, entscheiden Latenz, Verfügbarkeit und Datenhoheit darüber, ob aus einem Modell ein produktiver Prozess wird. Treffen bei der vorausschauenden Wartung die Maschinendaten verspätet ein, kippt die Vorhersage zur nachträglichen Reparatur.

Damit wird das Netzwerk vom Transportmedium zur Steuerungsplattform. Es bestimmt, welche Informationen an der Maschine bleiben und welche in die Cloud gehen. Hier liegt auch ein Schlüssel zur digitalen Souveränität: Wer Datenflüsse bewusst lenkt, behält die Kontrolle darüber, was das eigene Werk verlässt. Diese Rolle hat eine Kehrseite: Dieselbe Steuerungsfunktion, die den Wert schafft, vergrößert die Angriffsfläche. Wer dem Netz die Steuerung anvertraut, muss ihm auch den Schutz anvertrauen. Sonst wird verwundbar, wo der Wert entsteht.

Zur Nüchternheit gehört, Souveränität nicht mit Autarkie zu verwechseln. Autarkie ist in einer globalisierten Welt keine tragfähige Strategie. Souveränität heißt nicht Abschottung, sondern Kontrolle über Abhängigkeiten, Datenflüsse und kritische Prozesse. Wer darauf verzichtet, zahlt später drauf – mit höheren Risiken, teuren Korrekturen und weniger Handlungsspielraum. Der Heimvorteil dieses Landes liegt ohnehin nicht darin, den nächsten globalen Chatbot zu bauen, sondern im Prozesswissen seiner Industrie. Dieses Wissen lässt sich nicht kopieren. Es lässt sich aber verlieren, wenn die Infrastruktur darunter nicht trägt.

Für Vorstände und CISOs verschiebt sich damit die Leitfrage. Es geht nicht mehr darum, an einem Punkt möglichst dicht zu machen, sondern darum, Sicherheit dort zu verankern, wo Kontext, Geschwindigkeit und Sichtbarkeit zusammenkommen. Cybersicherheit gehört nicht ans Ende eines Digitalprojekts, sondern in dessen Design. Wer diesen Schritt von der Werkzeug- zur Architekturfrage vollzieht, gewinnt nicht nur Sekunden zurück. Er macht aus Reaktion wieder Kontrolle.

SOUVERÄNITÄT HEISST NICHT ABSCHOTTUNG, SONDERN KONTROLLE

Bleibt das Tempo. Rechenleistung wird in Minuten gebucht, Netzänderungen dauern oft Wochen. Diese Lücke schließt sich, weil sich das Netz von hardwarezentrierter Infrastruktur zu einer softwaredefinierten Plattform entwickelt. Davon profitiert besonders der Mittelstand, der vor denselben Bedrohungen steht wie Konzerne, ohne mehrköpfige Security Teams zu haben. So wie Google einst den Zugang zu Information demokratisiert hat, muss Cybersicherheit künftig selbstverständlich mitkommen, wenn ein Unternehmen einen Anschluss kauft.





# *Digitale Souveränität bedeutet für mich...*

Digitale Souveränität heißt, die Schlüssel selbst in der Hand zu halten. Digitale Souveränität ist die Voraussetzung für Sicherheit, Handlungsfähigkeit und Wettbewerbsfähigkeit – auch in Zukunft. Wer von einzelnen Anbietern oder Staaten abhängig ist, steht schnell vor verschlossener Tür. Umso wichtiger ist, dass wir in Deutschland in strategisch wichtigen Bereichen verlässliche eigene Fähigkeiten aufbauen. Damit wir eine Wahl haben. Damit uns Türen offenstehen. Damit wir Partner auf Augenhöhe sind. So bleiben wir handlungsfähig – analog und digital.

Digitale Souveränität wird Deutschland nicht allein erreichen. Wir müssen dieses Ziel europäisch denken. Europa muss bei zentralen digitalen Technologien wieder selbst Anbieter sein, Entwicklungen antreiben, Standards setzen, echte Innovation ermöglichen.

Nordrhein-Westfalen ist hier ein starker Motor. Wir bringen die Potenziale von Industrie und Mittelstand mit Spitzenforschung zusammen. Unsere Stärke liegt darin, Schlüsseltechnologien mit industrieller Anwendung zu verbinden. So besetzen wir strategische Knoten der digitalen Wertschöpfung: bei Halbleitern, Quantenhardware, der Integration von Quantencomputing und Superrechnern, bei Cloud-Infrastrukturen und Rechenzentren, bei KI-Modellen und digitaler Resilienz.

Die Landesregierung Nordrhein-Westfalen treibt digitale Souveränität voran, indem sie den Weg frei macht: für Investitionen, für Technologietransfer und für kluge Köpfe mit guten Ideen. Mein Ziel: Technologische Entwicklungen steuern und industrielle Wertschöpfung erhalten. Und deshalb bedeutet digitale Souveränität für mich: moderne Industriepolitik für Deutschland und Europa.

**Ein Essay von Hendrik Wüst, Ministerpräsident des Landes Nordrhein-Westfalen, MdL**



# Navigate What's Next

*Stimmen der DIGITAL X 2026*

„Wir müssen das Thema KI und den Umgang und die Arbeit mit ihr auch in die Bildung bringen, zu den Schülern und zu den Lehrern. Das finde ich wichtiger als so manche Jahreszahl im Geschichtsunterricht. Gleichzeitig brauchen wir auch eine Art Beratungskultur für die älteren Generationen, um sie im Alltag mit der KI unterstützen zu können. Da kommt eine Menge Arbeit auf uns zu."

Dr. Angela Merkel
Bundeskanzlerin a.D.

„Wir müssen neue Stärken entwickeln, um wieder an Momentum zu gewinnen. Und können gleichzeitig auf etabliertes Know-How aufbauen, um die Jahrhundertchance KI für uns bestmöglich zu nutzen."

Dr. Roland Busch
President und CEO, Siemens

„Durch Technik haben wir sehr viel im Griff, wir haben den Blick aufs große Ganze, und das weltweit. Die größte Schwachstelle – die 90 Prozent aller Angriffe erst möglich macht – ist weiterhin der Mensch."

Robert Mallinson
Co-CEO, Rohde & Schwarz Networks and Cybersecurity GmbH

„KI wird dann wertvoll, wenn drei Elemente zusammenkommen: Die Ambition eines Unternehmens und seiner Mitarbeiter. Die Intelligenz eines Unternehmens. Und drittens Vertrauen in die Technologie, damit die Skalierung ermöglicht wird."

Michael Locher-Tjoa
General Manager SME&C D-A-CH, Microsoft

„Wir leben in einer gleichzeitig spannenden wie auch gefährlichen Zeit. Aber wir können die Gefahren bannen, indem wir Schritt für Schritt gemeinsam gehen. Denn kein Land und kein Unternehmen allein kann bei KI die Führung übernehmen."

Nick Tzitzon
Vice Chairman, ServiceNow

„Der Trend bei KI geht klar weg von Pilotprojekten hin zu verschiedensten Business Cases: Sei es für mehr Umsatz, effizientere Prozesse oder eine höhere Kundenzufriedenheit."

Alexander Wallner
CEO EMEA Central, Salesforce

„Viele Mittelständler meinen, sie hätten nicht die Ressourcen und Kapazitäten, um KI in der IT abbilden zu können. Jedoch hätten gerade diese Unternehmen große Vorteile: Flexibilität und Mitarbeiternähe – um Strukturen einfacher zu verändern und Prozesse und Hierarchien schneller anzupassen, als es bei großen Konzernen der Fall ist."

Florian Kunzke
Global Director AI Strategy, SAP

„Wir brauchen eine Balance, eine Allianz zwischen europäischen Tech-Playern wie der Telekom, die garantieren, dass das System sicher und souverän ist, und amerikanischen oder chinesischen Herstellern, die für die Innovationen in der Software sorgen."

Uwe Peter
Senior Vice President und Geschäftsführer, Cisco Deutschland





„Wir dürfen bei all der rasanten Entwicklung von KI nicht vergessen: Der Mensch muss weiterhin die Verantwortung tragen für die Ergebnisse. Und er darf der KI nur so viele Fähigkeiten geben, wie er ihr vertrauensvoll in die Hände legen kann."

Roman Howe
Head of Central and Eastern Europe, Anthropic

„Europa hat keine wirkliche Idee von der Zukunft für sich selbst, außer bürokratischen Antworten und nicklichen Reformen. Wenn wir gegen die Großmächte bestehen wollen, muss Europa sich als politische Institution weiterentwickeln – hin zu so etwas wie den Vereinigten Staaten von Europa."

Dr. Robert Habeck
Ehem. Vizekanzler & Bundeswirtschaftsminister a. D.

„Die große Herausforderung ist: Die Entwicklung von KI wieder einzubremsen – um überhaupt verstehen zu können, was technologisch gerade passiert."

Prof. Yuval Noah Harari
Historiker, Philosoph, Autor, Sapienship

„Ich sehe eine immer stärker um sich greifende Epidemie der Angst vor der Zukunft, die von den etablierten Parteien nicht wirklich eingefangen wird. Wir brauchen wieder eine echte Vision von der Zukunft – die nicht aus Parolen der Vergangenheit besteht – und Durchhaltevermögen, um aus den aktuellen Krisen wieder herauszukommen."

Florence Gaub
Research Director, NATO Defense College

„Wir leben in revolutionären Zeiten, aber nehmen die Revolution nicht an. Stattdessen sehen wir nur Probleme. Wir sollten lieber von Herausforderungen sprechen – und an der Größe der Herausforderungen wachsen. Diesen Mut und diesen Glauben an Veränderbarkeit brauchen wir ganz dringend."

Richard David Precht
Philosoph, Publizist und Autor

„Bei KI in Unternehmen geht es darum, Routineaufgaben auszulagern, um den Menschen, die das Geschäft weiterentwickeln, mehr Raum zu schaffen. Wichtig ist Vertrauen in die Technologie, um diesen Schritt nach vorne mitgehen zu können."

Dr. Maximilian Ahrens
Managing Director T Digital, Deutsche Telekom Geschäftskunden GmbH

„Wir haben uns lange verlassen auf unsere physischen Absicherungen, auf Kameras und Zäune. Jetzt gibt es neue Bedrohungen, digital und auch aus der Luft, etwa was am Leipziger Flughafen passiert ist. Darauf müssen wir uns einstellen."

Dr. Klaus Michel
Geschäftsführer, Advisory Board Member, Airbus Defence and Space GmbH

„Nicht nur die Politik, auch jedes Unternehmen – und sei es noch so klein –, muss auf Gefahren und Bedrohungen eingestellt sein. Der Staat alleine könnte das gar nicht bewerkstelligen, hier sind wir alle in der Gesamtverantwortung."

Dr. Marie-Agnes Strack-Zimmermann
Vorsitzende des Ausschusses für Sicherheit und Verteidigung (SEDE), Europäisches Parlament

## Gegen die Übermacht

Frankreichs Regierung trennt sich von Teams und Zoom, mehr als eine halbe Million Schüler im Großraum Paris arbeiten auf der Plattform einer deutschen Firma. Sensible Daten sollen nicht außerhalb Europas gespeichert werden.

Von
Alexandra Föderl-Schmid

Eigentlich müsste er sich beim US-Präsidenten Donald Trump bedanken. „Für mein Geschäft ist der Trump-Effekt toll“, sagt Anfang 2026 der Mitbegründer und Chef der französischen IT-Firma Leviia, William Méauzoone, und lacht. Aber sogleich wird er ernst und fügt hinzu: „Persönlich machen mir diese Entwicklungen Angst. Aber dieser Trump-Effekt bewirkt wirklich etwas, ein Push vom Diskutieren zum Tun.“

Seit zwei, drei Monaten wird die IT-Firma mit Sitz nahe Paris von Anfragen geradezu überrollt. Leviia ist in Frankreich Partner von Nextcloud, einem Unternehmen mit Sitz in Stuttgart, das eine vollständig auf Open-Source-basierte Kollaborationsplattform anbietet. Die Daten bleiben auf den eigenen Servern oder bei einem der lokalen Cloud-Partner wie Leviia, das Speicherzentren in Marseille und Lyon betreibt – was Nähe und Kontrolle gewährleistet. Die Daten fließen also nicht in die USA ab oder werden zum Training von KI-Modellen genutzt.

Seit Donald Trump in Washington sein Amt angetreten hat und sich die Bosse der Techkonzerne um den US-Präsidenten scharen, ist das Misstrauen nicht nur bei französischen Unternehmen und Behörden gewachsen. Besteht ein Risiko, dass der US-Präsident Cloud-Anbietern aus geopolitischen Erwägungen vorschreiben könnte, ihre Dienste in Europa abzuschalten? Was ist, wenn aus politischen oder wirtschaftlichen Gründen einfach der Zugriff auf Daten verweigert wird? Oder die eigenen Daten anderweitig benutzt werden?

Bisher sei es bei Fragen, ob US-Produkte zum Einsatz kommen und wo die Daten gespeichert werden, „vor allem um Ideologie gegangen“, sagt Leviia-Chef Méauzoone. „Aber jetzt beginnen auch große, sehr große französische Unternehmen, Angst zu bekommen. Und sie wollen rasch Lösungen haben.“ Er schätzt, dass mehr als ein Dutzend der an der Pariser Börse im Aktienindex CAC gelisteten führenden 40 Unternehmen konkrete Umstiegsmöglichkeiten prüft oder schon konkrete Schritte veranlasst hat. Namen dürfe er keine nennen. „Viele sind vom ersten Tag an Microsoft-Kunden, fragen sich aber jetzt, ob sie dort noch Sicherheit haben.“

Kräftig unterstützt wird diese Weg-von-den-USA-Bewegung in Frankreich durch die Regierung. Präsident Emmanuel Macron setzte sich, wie bei einem Treffen der EU-Staats- und Regierungschefs im Februar, für eine Verringerung der technologischen Abhängigkeit von den USA und China ein. Französische Behörden scheuen sich auch nicht, gegen Elon Musk vorzugehen. Ermittler durchsuchten Anfang Februar das Pariser Büro seiner Plattform X, Musk wurde im Anschluss vorgeladen. Die Pariser Staatsanwaltschaft ermittelt gegen X wegen des Vorwurfs, dass Algorithmen in dem sozialen Netzwerk verändert worden sein sollen, um rechtsextremen Inhalten mehr Aufmerksamkeit zu bescheren. Es gibt auch außerdem Vorwürfe wegen Holocaustleugnung und sexualisierter Abbildungen.

Während anderswo noch diskutiert wird, macht Paris Ernst mit seinem Vorgehen gegen US-Techkonzerne und setzt das um, was in Brüssel gefordert wird: mehr digitale Souveränität. Konkret heißt das: Die französische Regierung will Zoom und Teams nicht mehr nutzen. Zum Einsatz kommt künftig nur noch Visio, eine mit französischer Technologie entwickelte quelloffene Software. „Wir können nicht das Risiko eingehen, dass unser wissenschaftlicher Austausch, unsere sensiblen Daten und unsere strategischen Innovationen nicht europäischen Akteuren ausgesetzt werden“, sagte David Amiel, Minister für den öffentlichen Dienst. Er sieht darin „eine Versicherung gegen zukünftige Bedrohungen und eine Chance für unsere Unternehmen“. Bis Ende 2027 soll dieser Wechsel vollzogen sein.

Weiter ist man da schon in der Region Île-de-France. Die Revolution in Frankreich hat diesmal in den Schulen begonnen. Vor eineinhalb Jahren startete die Verwaltung im Großraum Paris damit, Microsoft-Software schrittweise durch Angebote französischer Firmen zu ersetzen. Französischen Unternehmen wie Worldline und Docaposte kümmern sich um die Verwaltung von E-Mails und Schülerdaten, die auf den Servern von Leviia gespeichert sind.

„Für uns ist vor allem Datenschutz sehr wichtig, da geht es um sensible Informationen von Minderjährigen. Wir wollten bewusst in Schulen andere Produkte als die von Microsoft anbieten“, sagt Bernard Giry, Leiter der digitalen Transformation der Region Île-de-France. Mit der Umstellung wurde aber noch etwas anderes bezweckt: „Wir wollten die Arbeitsmöglichkeiten zwischen Lehrern und Schülern verändern und leicht zugängliche, kollaborative Plattformen.“

Inzwischen arbeiten bereits etwa 550.000 Schülerinnen und Schüler, Lehrer und Beschäftigte der Schulverwaltung mit Monlycée, einer gemeinsamen Plattform, die alle Dienste integriert. Auf den ersten Blick sieht die Oberfläche wie ein Angebot von Microsoft aus: Mit der von Nextcloud entwickelten und von Leviia eingeführten Software können Schüler im Großraum Paris auf dieser Lernplattform gemeinsam Dokumente bearbeiten und teilen, Lehrer können Unterrichtsmaterialien hochladen.

Die Open-Source-Software ist modular aufgebaut und über Handy oder Tablet genauso nutzbar wie auf einem Laptop. „Unser Ziel ist es, ein bekanntes Nutzererlebnis ohne jeglichen Komfortverlust zu bieten“, sagt Leviia-Chef Méauzoone. Er verhehlt auch nicht, dass damit ein pädagogischer Effekt angestrebt wird: dass sich Kinder an andere Produkte als jene aus den USA gewöhnen.

„STEIN FÜR STEIN BAUEN WIR ALTERNATIVEN AUF.“

Auch Giry, der für die IT-Infrastruktur des Großraums Paris zuständig ist, sieht einen Trump-Effekt: „Tatsächlich gibt es in Frankreich diesen Effekt, wir wollen nicht mehr so abhängig von den Amerikanern sein. Baustein für Baustein bauen wir Alternativen auf. Aber wir haben schon vor zwei Jahren, also vor Donald Trump, zu planen begonnen.“ Denn man könne nicht so von einem Tag auf den anderen Microsoft-Programme abschalten, die Migration der Daten dauert. Er selbst nutzt für das Interview auch noch Teams. „Es ist auch nicht so, dass alle Lösungen schon existieren. Wir müssen schrittweise vorgehen. In unserem Bereich gibt es aber die Notwendigkeit, dass alles funktioniert, 365 Tage im Jahr.“

Bisher läuft alles in den Schulen im Großraum Paris. Die Umstellung gilt als Vorzeigebeispiel, weitere Regionen und Kommunen in Frankreich wollen folgen. Auch Chamonix, Grenoble, Ville-la-Grand und Lyon ersetzen in der Verwaltung Microsoft Office schritt-

weise durch freie und quelloffene Software. Das französische Energie- und das Bildungsministerium sind ebenfalls dabei umzustellen.

Das 2016 in Stuttgart gegründete Unternehmen Nextcloud sieht ein deutlich wachsendes Interesse in ganz Europa, wenngleich Deutschland noch im Rückstand ist. Einzig Schleswig-Holstein ist gerade dabei, auf Open-Source-Anbieter umzustellen. Frankreich oder auch Österreich, wo das Wirtschaftsministerium auf Nextcloud setzt, sind da schon weiter. 2025 haben sich die Anfragen im Vergleich zum Jahr davor verdreifacht, sagt Unternehmenschef Frank Karlitschek und spricht ebenfalls von einem „Trump-Effekt“, der die Unabhängigkeitsbestrebungen beschleunige.

Der Pariser Behördenvertreter Bernard Giry sieht aber noch einen anderen Grund: Kostendruck. Verwaltungseinrichtungen in Frankreich wie auch Unternehmen sehen sich mit Kostensteigerungen durch Preiserhöhungen etwa bei Microsoft konfrontiert und fühlen sich letztlich auch ausgeliefert. Nach Angaben des für die öffentliche Verwaltung zuständigen Ministeriums führt die Abschaffung kostenpflichtiger Softwarelizenzen zu „erheblichen Einsparungen“. Schätzungen zufolge kann rund eine Million Euro eingespart werden, wenn 100000 Nutzer auf ein Lizenzprodukt verzichten. In der Region Île-de-France werden nach Angaben von Giry pro Jahr 140 Millionen Euro für die IT nur in Schulen ausgegeben.

In Frankreich gilt das Projekt Île-de-France als wegweisend im Kampf gegen die Vorherrschaft der US-Techkonzerne. Für Leviia-Chef Méauzoone ist es „ein großartiger Anwendungsfall“, weil man mit mehr als einer halben Million Nutzern zeigen könne, dass es auch ohne Microsoft und Co. geht. Und so ist er sich sicher: „Wir haben eine große Zukunft vor uns.“



ERSCHIENEN IN DER SZ VOM 14.02.2026





***Wie Staat und Sozialträger digital vernetzt werden können***

# Kitaplatz, Elterngeld, Hebamme: Wer staatliche Leistungen sucht, landet im digitalen Flickenteppich. Eine Studie für die Stiftung Mercator zeigt, wie eine gemeinsame Infrastruktur das ändern könnte.

VON
GABRIEL RINALDI

Wer in Deutschland einen Kitaplatz sucht, Elterngeld beantragen oder eine Hebamme finden will, landet oft in einem digitalen Flickenteppich. Henning Tillmann, Informatiker und früheres Digitalbeiratsmitglied der Bundesregierung, hat im Auftrag der Stiftung Mercator eine Vorlaufstudie zu einem Konzept für eine digitale Daseinsvorsorge (Dida) vorgelegt.

Das Dokument skizziert, wie ein technisches Netzwerk die zersplitterte Landschaft digitaler Angebote von Staat, Sozialwirtschaft und Zivilgesellschaft verbinden könnte – und welche Institution es dafür bräuchte. Grundlage sind mehr als 40 Expertengespräche mit Anbietern, Verwaltung, Wohlfahrtsorganisationen, Denkfabriken und Unternehmen.

Das zentrale Defizit der digitalen Daseinsvorsorge sei nicht ein Mangel an Angeboten, sondern ein Mangel an Interoperabilität, Auffindbarkeit und verbindender Infrastruktur. Wer Leistungen in Anspruch nehmen will, stößt häufig auf Insellösungen: kommunale Portale, Chatbots, PDF-Listen, Suchmaschinentreffer, Social-Media-Empfehlungen.

Der Befund: Fast alles funktioniere nur, „wenn man bereits weiß, wonach man suchen muss“, heißt es in der Studie. Für Anbieter sei die Lage fragmentiert, mit geringer Sichtbarkeit und kaum technischer Anschlussfähigkeit an staatliche Systeme.

Dida soll nicht als weiteres Portal ansetzen, sondern als technische Infrastruktur. Mit standardisierten Schnittstellen, gemeinsamen Datenmodellen, Verzeichnislogik und verbindlichen Regeln für Interoperabilität. Tillmann greift dafür ein Bild auf, das aus Debatten um den Deutschland-Stack bekannt ist: Dida solle die „Straßen und Schienen“ zwischen bislang getrennten Diensten bauen, die „Städte“ – also die einzelnen Angebote – blieben eigenständig.

Statt dass sich Nutzende durch Zuständigkeiten, Paragrafen und Formulare kämpfen, soll Dida den Zugang entlang konkreter Lebenssituationen wie „Ich werde Mutter“ oder „Ich pflege Angehörige“ organisieren – und die jeweils relevanten Angebote zu einer zusammenhängenden Nutzerreise bündeln.

Die technische Vernetzung sei besonders über den Wohlfahrtsverband hinaus kaum ein Thema. „In den Gesprächen stellte sich heraus, dass in diese Zielrichtung bisher überhaupt nicht gedacht wurde“, sagte Tillmann SZ Dossier. Die potenziellen Synergieeffekte seien aber erkannt. „Wer in der digitalen Welt nicht Teil der Big-Tech-Plattformökonomie ist, kann nur vernetzt bestehen.“

Der konkreteste Teil der Studie betrifft die Umsetzung: Ein reiner Standard entfalte keine Wirkung, solange er nicht implementiert werde, schreibt Tillmann. Er plädiert deshalb für eine eigene Dida-Serviceagentur, die das Netzwerk aufbauen, ausbauen und betreiben soll. Als Vorbild für die institutionelle Aufstellung wird explizit die Bundesagentur für Sprunginnovationen (Sprind) genannt.

Die Agentur soll in drei Phasen arbeiten. Zunächst analysiert sie bestehende Kooperationen und identifiziert Synergien. Dann entwickelt sie Spezifikationen, Governance-Regeln und erste Referenzimplementierungen. Anschließend beginnt das Onboarding. Es folgt nach rund zwei Jahren der produktionsreife Regelbetrieb. Schon zum Start soll mindestens ein Pilotportal entstehen.

Tillmann rechnet als Leitlinie mit acht Vollzeitäquivalenten zu Beginn, 24 in der Aufbauphase und 60 zum Regelbetrieb. Das Jahresbudget steigt entsprechend von 1,65 Millionen Euro über vier auf 10,4 Millionen Euro. Zur Finanzierung schlägt er einen Mix aus öffentlicher Anschubfinanzierung, philanthropischen Mitteln, EU-Programmen und später auch Beiträgen kommerzieller Anbieter im Netzwerk vor.

DIE QUER-
EINSTEIGERIN
BEKAM GLEICH ZWEI
JOBANGEBOTE

Für Identität und Einwilligung setzt das Konzept auf die geplante Eudi-Wallet. Nutzende könnten sich damit bei angeschlossenen Diensten anmelden, ohne überall neue Konten anzulegen. Die Wallet soll aber keine Zugangsvoraussetzung werden – niedrigschwellige Zugänge müssten erhalten bleiben.

In einer späteren Ausbaustufe könnte Dida als standardisierte Schnittstelle funktionieren, über die KI-Chatbots gezielt auf geprüfte Angebote der Daseinsvorsorge zugreifen können, statt sich auf unstrukturierte Websuchen zu verlassen. Denkbar seien zudem „Lebenslagen-Agenten“, die mit Einwilligung Datentransfers zwischen Diensten orchestrieren, Fristen überwachen und proaktiv erinnern.

Um auch analoge Anbieter einzubinden, sieht das Konzept einen vertrauenswürdigen KI-Generator vor: Musikschulen oder Sportvereine könnten dort wöchentlich ihre Stunden- oder Belegungspläne per Drag-and-drop hochladen. Daraus generiert die KI automatisch maschinenlesbare Schnittstellen, über die Portale passende Angebote für konkrete Anfragen finden könnten.

Zwei Risiken nennt die Studie offen. Erstens die chronische Überlastung nicht-staatlicher Anbieter, für die jede zusätzliche Digitalisierungspflicht mit Kernaufgaben konkurriert. Als Gegenbeispiel führt Tillmann jedoch Doctolib an: Auch die ambulante Versorgung galt lange als schwer digitalisierbar, bis eine Plattform Terminlogik und Kommunikationslast reduzierte.

„Das zentrale Argument ist hier also die Vereinfachung und die Abnahme von Verwaltungsaufwand“, sagte er SZ Dossier. Anders als Doctolib mit einem geschlossenen System müsse aber direkt offen und interoperabel agiert werden. Als zweites Risiko nennt er die Abhängigkeit von großen Plattformen, der Dida durch offene Standards begegnen würde.

Die Vorlaufstudie versteht er ausdrücklich als Einstieg, benennt aber klare nächste Schritte: politische Anschlussfähigkeit herstellen, Pilotsektoren auswählen, Mindeststandards definieren, ein technisches Minimalmodell entwickeln. Zum Deutschland-Stack würde Tillmann einen „Konnektor“ entwickeln, um staatliche und nicht-staatliche Angebote erstmals in Prozessketten zu verbinden.

„Im letzten Jahr gab es bereits erste positive Signale“, sagte er. Die wirklichen Gespräche würden aber erst nach der Veröffentlichung stattfinden. Er sei hoffnungsvoll: „Wer Ja zum Deutschland-Stack für die Verwaltung sagt, kann schlecht Nein zur digitalen Daseinsvorsorge sagen.“





ERSCHIENEN IM SZ-DOSSIER VOM 23.04.2026

# „Der Erfolg des KI-Pakts entscheidet sich an der Infrastruktur“

*Die beiden De-Cix-Manager Ivo Ivanov und Sudhir Kunder erklären, was der KI-Pakt mit Indien bringen soll, was Deutschland von dem Land lernen kann, und wie die Sicherheit von Internet-Knotenpunkten verbessert werden kann.*

Von
Matthias Punz

De-Cix betreibt in Frankfurt einen der wichtigsten Internetknoten der Welt und ist inzwischen in mehr als 60 Märkten auf mehreren Kontinenten aktiv. Das Unternehmen organisiert Umschlagplätze für den Datenverkehr. Dort verbinden sich Internetanbieter, Cloud-Dienste, Streamingplattformen, Unternehmen und andere Netzbetreiber direkt miteinander, damit Daten von einem Netz ins andere gelangen.

„WIR HABEN ECHTE DIGITALE CHAMPIONS."

De-Cix-Chef Ivo Ivanov war im Februar Teil einer deutschen Delegation in Indien, als dort ein deutsch-indischer KI- und Digitalpakt beschlossen wurde. Sudhir Kunder, Chief Business Officer von De-Cix India, war in Neu-Delhi ebenfalls dabei.

Im Interview mit SZ Dossier erklären sie, was aus den politischen Ankündigungen konkret geworden ist – und was Deutschland von Indien lernen kann.

**SZ: Herr Ivanov, Deutschland und Indien sprechen seit ein paar Monaten intensiv über KI und digitale Zusammenarbeit. Eine echte strategische Partnerschaft oder vor allem der Versuch, die Abhängigkeit von den USA und China zu verringern?**

*Ivanov:* Ich halte diesen deutsch-indischen KI-Pakt für strategisch sehr sinnvoll. In den Gesprächen habe ich auf beiden Seiten ein großes Engagement erlebt und auch die Bereitschaft indischer Partner, auf unterschiedlichen Ebenen zusammenzuarbeiten. Aber der Erfolg eines solchen Pakts entscheidet sich nicht durch Absichtserklärungen. Er entscheidet sich an der Infrastruktur, die KI im Alltag tatsächlich ermöglicht.

**Was ist denn konkret aus dem KI-Pakt geworden? Man hört öffentlich wenig. Der indische Digitalminister sollte im April nach Berlin kommen, war dann aber nicht da. Welche Schritte gab es in den Monaten zuvor?**

*Kunder*: Ich gehe davon aus, dass der Besuch noch stattfinden wird. In Indien laufen in mehreren Bundesstaaten Wahlen, solche Prioritäten können Termine verschieben. Für uns als De-Cix India ist entscheidend, dass sich die Nachfrage seit diesen Gesprächen klar erhöht hat. Wir gehen in eine Expansionsphase und planen derzeit zusätzliche Präsenz in rund elf Rechenzentren in Indien.

**Trotzdem noch einmal konkret: Gab es nach dem Roundtable der Wirtschaft in Neu-Delhi weitere Treffen oder konkrete politische Schritte?**

*Ivanov:* Von unserer Seite aus gab es vor allem Beiträge zu zwei Projekten in Deutschland, die nicht unmittelbar Teil des KI-Pakts sind, aber eng damit zusammenhängen: zur Rechenzentrumsstrategie auf Bundesebene und zu entsprechenden Diskussionen auf Landesebene in Hessen. Dabei geht es darum, Genehmigungs- und Verwaltungsprozesse zu beschleunigen, Investitionen in Rechenzentren zu erleichtern und digitale Infrastruktur in Deutschland stärker zu verteilen. Das ist für KI entscheidend.

**Hat Deutschland eine starke Stimme in der internationalen Digitaldebatte?**

*Ivanov:* Deutschland kann lauter werden. Wir haben echte digitale Champions. De-Cix ist im Bereich Interconnection weltweit führend, in Deutschland entstanden und inzwischen auf mehr als 60 Märkten aktiv. SAP ist ein weiteres Beispiel. Auch die Schwarz-Gruppe mit Stackit zeigt, dass in Europa souveräne digitale Infrastruktur entstehen kann. Ich würde mir wünschen, dass politische Akteure solche Beispiele stärker sichtbar machen. Europa kann ein souveräner Partner sein – nicht isoliert, sondern auf Augenhöhe mit den USA, Asien und insbesondere Indien.

„EUROPA KANN EIN SOUVERÄNER PARTNER SEIN."

**Bedeutet digitale Souveränität in Indien etwas anderes als in Europa? In Europa geht es oft um die Frage, ob möglichst alles von europäischen Unternehmen kommen soll.**

*Kunder:* In Indien hat das Thema zuletzt deutlich an Dringlichkeit gewonnen. Ein wichtiges Beispiel war Nayara Energy. Aufgrund der geopolitischen Spannungen waren Microsofts Systeme im Unternehmen plötzlich nicht mehr nutzbar. Das hat der Debatte über souveräne Clouds und souveräne KI einen starken Schub gegeben. Wettbewerber, die sonst gegeneinander arbeiten, haben sich unter einem Dach zusammengeschlossen, um indische digitale Infrastruktur voranzubringen.

Gleichzeitig sehen wir derzeit massive Investitionen in digitale Infrastruktur. Google hat Milliardeninvestitionen in Visakhapatnam angekündigt, unter anderem in Unterseekabel, Landestationen und KI-basierte Infrastruktur. Auch Meta will viele Milliarden investieren. Mit dabei ist aber das indische Unternehmen AdaniConneX. Indien geht es bei digitaler Souveränität nicht nur um Schutz, sondern um den Aufbau eigener technologischer Leistungsfähigkeit.

**Ein Beispiel ist das indische Zahlungssystem UPI. In Indien kann man am Straßenstand per Smartphone zahlen, während Deutschland noch sehr an Karten und Bargeld hängt. Was kann Deutschland lernen?**

*Kunder:* Die technologische Adoption war in diesem Bereich revolutionär. UPI ist inzwischen auch in anderen Ländern nutzbar. Man kann an bestimmten Orten im Ausland mit dem indischen System bezahlen. Der Moment, als Volker Wissing in Delhi bei einem Obstverkäufer einkaufte und erstaunt war, dass die Zahlung per Mobiltelefon abgewickelt wurde, wurde in Indien bekannt.

Die Durchdringung mit mobilen Diensten ist generell enorm. Viele Menschen besitzen mehr als ein Gerät. Ein großer Teil der Datennutzung kommt inzwischen aus ländlichen Regionen. Programme wie BharatNet sollen digitale öffentliche Infrastruktur landesweit verfügbar machen.

*Ivano*v: UPI ist ein gutes Beispiel für eine offene Plattform mit massiver Skalierbarkeit. In Indien wurde das System früh ausgerollt, praktisch genutzt, weiterentwickelt und dann infrastrukturell abgesichert. In Deutschland läuft die Reihenfolge oft andersherum: Erst kommen lange Diskussionen zwischen vielen Stakeholdern, dann der Anspruch, alles perfekt zu machen, und erst sehr spät der Rollout.

**Die geopolitische Lage wird unsicherer. Es gibt mehr Konflikte, mehr Druck auf kritische Infrastruktur. Wie verwundbar sind Internetknoten in einer solchen Welt?**

*Ivanov:* Gerade angesichts geopolitischer Risiken brauchen wir digitale Infrastruktur, die lokal verteilt und zugleich global integriert ist: so lokal wie möglich, so global wie nötig.

„DAS INTERNET DER NÄCHSTEN GENERATION WIRD ÜBERALL SEIN."

Internetknoten sind gerade in einer solchen Welt ein wichtiger Teil der Antwort. Wenn Kabel zwischen Asien, Indien, dem Nahen Osten und Europa ausfallen, dauert eine Reparatur oft Wochen oder Monate. Netzbetreiber, die nicht redundant angebunden sind, sehen dann Ausfälle. Wer über De-Cix verbunden ist, profitiert von alternativen Pfaden. Die Wege werden länger, aber sie funktionieren weiterhin.

**Wie müssen sich Netzknoten in den kommenden Jahren verändern?**

*Ivanov:* Sie müssen stärker auf unterschiedliche Branchen zugeschnittene Dienste anbieten. Es geht nicht mehr nur um Telekommunikationsanbieter, Internetprovider, Cloud- und Netzbetreiber. Auch Unternehmen aus Finanzwirtschaft, Automobilindustrie, Gesundheitswesen, Logistik oder Handel brauchen direkte, sichere und performante digitale Verbindungen. Dafür entwickeln wir Dienste wie Multi-Cloud-Routing, Cloud Exchanges oder geschlossene Nutzergruppen für besonders sichere Umgebungen. Zudem geht es darum, Infrastruktur noch dezentraler anzubieten.

**Inwiefern?**

*Ivanov:* Digitale Infrastruktur wird nicht nur in den großen Hubs wie Frankfurt, Mumbai, Singapur oder New York gebraucht, sondern näher an den Orten, an denen Daten entstehen und genutzt werden: in Fabriken, entlang von Autobahnen, in Businessparks, an Edge-Standorten. Das Internet der nächsten Generation wird überall sein.

Und dann gibt es noch eine langfristige Vision: digitale Infrastruktur im Weltraum. De-Cix arbeitet an einem Konzept für einen Space Internet Exchange. Unser Traum ist, eines Tages den ersten Internetknoten im Weltraum zu betreiben.

**Herr Kunder, zum Schluss der Blick nach Indien: Wie schnell kann sich die digitale Infrastruktur dort in den kommenden Jahren entwickeln?**

*Kunder:* Indien steht vor einem massiven Ausbau. Die aktuelle Rechenzentrumskapazität liegt ungefähr bei 1,4 bis 1,6 Gigawatt. Mit den angekündigten Investitionen sehen wir bis 2030 oder früher eine Größenordnung von 4,5 bis 5 Gigawatt. Gleichzeitig wächst das gesamte Ökosystem: Glasfaser, Edge-Rechenzentren, KI-Anwendungen, 5G und IoT im Unternehmenseinsatz.

Die Voraussetzungen sind da: Kapital, Infrastruktur, Skalierung, eine junge Bevölkerung, hohe mobile Nutzung und eine große technische Workforce. Ich glaube, die nächsten zehn Jahre werden Indiens Jahrzehnt – getrieben von Technologie.





ERSCHIENEN IM SZ-DOSSIER VOM 26.05.2026

## *„Wir werden den Cyberdome für Deutschland bauen“*

Zur Münchner Sicherheitskonferenz spricht BSI-Chefin Claudia Plattner mit SZ Dossier über die konkrete Ausgestaltung des Cyberdome. Und darüber, welche anderen Strategien die IT-Sicherheit stärken sollen.

INTERVIEW VON
MATTHIAS PUNZ UND GABRIEL RINALDI

Claudia Plattner hat ein neues Spielzeug mitgebracht. Die BSI-Präsidentin zeigt ein Rad aus Pappe, das verschiedene politische Herausforderungen wie Abhängigkeit und Geopolitik am Rand anführt und im Inneren die Rolle der Cybersicherheit hervorhebt. Ihre Botschaft: Technologie und Digitalisierung sind mittlerweile Dreh- und Angelpunkt der Weltordnung. Deshalb will das Bundesamt für Sicherheit in der Informationstechnik (BSI) nun Tempo bei der automatisierten Cyberabwehr machen. Im Interview mit SZ Dossier spricht Plattner am Rande der Münchner Sicherheitskonferenz (MSC) über die Ausgestaltung des Cyberdome und führt erstmals konkrete Details aus.

**SZ: Frau Plattner, bei der MSC ging es sehr viel um hybride Bedrohungen in verschiedensten Ausprägungen. Was ist die alarmierendste Entwicklung der vergangenen Monate?**

*Claudia Plattner:* Es gibt nicht die eine Entwicklung. Aber: Zahlreiche Machtgleichgewichte verschieben sich und das hat viel mit dem Thema Technologie zu tun. Man muss Technologie beherrschen, um militärisch und auch wirtschaftlich erfolgreich zu sein.

**Innenminister Alexander Dobrindt (CSU) hat den „Cyberdome“ angekündigt, den er in Zusammenarbeit mit Israel aufspannen will. Das BSI war zu Gesprächen in Israel und es gab eine gemeinsame Übung. Was ist Ihre Rolle bei dem Vorhaben?**

Wir werden diejenigen sein, die den Cyberdome für Deutschland bauen. Den Auftrag haben wir und tun das auch sehr gerne. Wir fangen nicht bei null an, sondern haben schon einiges, was wir gut nutzen können. Die Grundidee ist, Cyberangriffe automatisiert abzuwehren.

**Was muss neu entwickelt werden und was ist schon da?**

Wir haben sehr gute Grundlagen, und die wollen wir weiterentwickeln und ausbauen. Im BSI bündeln wir bereits jetzt Kräfte, Ressourcen und Expertise für den Aufbau eines Cyberdomes: etwa in den Bereichen Lagebeobachtung, Threat Intelligence, Vorfallsbearbeitung und Schutz kritischer Infrastrukturen.

Beim Cyberdome setzen wir zudem auf Public-Private-Partnerships. Dabei wird es unter anderem darum gehen, Informationen miteinander zu teilen. Auch die Zusammenarbeit mit anderen Behörden und Ländern spielt eine Rolle. Wir denken das sehr groß, haben viele Ideen und stoßen auf massives Interesse. Viele wollen ihren Teil zu mehr Cybersicherheit in Deutschland beitragen.

„WIR DENKEN DAS SEHR GROSS, HABEN VIELE IDEEN UND STOSSEN AUF MASSIVES INTERESSE.“

**Wie soll eine automatisierte Cyberabwehr funktionieren, wenn es kein zentrales Lagebild in Deutschland gibt?**

In puncto Lagebild haben wir nach wie vor das große Ganze im Blick: Unser langfristig verfolgtes Ziel eines gesamtstaatlichen, automatisierten Lagebilds in Echtzeit wird im Cyberdome Wirklichkeit. Wir werden deutlich mehr Daten zur Verfügung haben als heute, mit denen wir unser Lagebild substanziell anreichern werden. Wir sind dazu in sehr vielen Gesprächen mit Unternehmen und Kritis-Betreibern, die etwas beisteuern wollen.

Natürlich wollen die auch was zurückbekommen, aber das ist voll in unserem Sinne: Wenn wir etwa ein Angriffsmuster erkennen, wollen wir das ja an alle zurückspielen und so gemeinsam den Schutz für alle, die beim Cyberdome mitmachen, erhöhen. Wir denken das Lagebild also viel systematischer und ganzheitlicher als nur die Summe aller aktuellen Fälle. Wir wollen datenbasiert erfassen, wo welche Bedrohungen sind, aber auch, wie wir die Zahlen wieder nach unten bekommen.

**Welche konkreten Bestandteile wird der Cyberdome haben?**

Wir gehen bislang von vier Dimensionen aus. Über Sensorik, Detektion und Monitoring erhalten wir Daten und ein Lagebild, das wir dann analysieren. Im dritten Schritt folgt die Aktion, die eigentliche Schutzmaßnahme. Ein wesentlicher Bestandteil ist dann die Kommunikation dazu, also etwa die Weitergabe der gewonnenen Informationen.

**Wie läuft das bei der Aktion ab? Auch automatisiert, oder muss ein Mensch einen Knopf drücken?**

Viele dieser Schritte werden wir automatisieren können, für andere werden und wollen wir definitiv menschliche Kontrolle einbauen.

**Werden israelische Unternehmen am Cyberdome beteiligt sein? Wie stellen Sie sicher, dass keine sensiblen Daten abfließen?**

Wir sind zunächst mal noch in der Konzeptionsphase. Das gilt auch für Firmen, mit denen wir künftig arbeiten werden. Wir werden in jedem Fall sicherstellen, dass das in unserem Sinne und mit der entsprechenden Datensicherheit und der entsprechenden Sorgfalt gemacht wird. Darauf können Sie sich verlassen, das ist unser Job.

**Wann wird der Cyberdome starten?**

Ich gehe hier von Iterationen aus: Zunächst werden wir das, was wir bereits haben, skalieren, um im Laufe des Jahres auch noch neue Features zu liefern, um den Cyberdome Stück für Stück immer weiter aufzuspannen.

**Brauchen Sie Gesetzesänderungen, um loszulegen? Beispielsweise bei der aktiven Cyberabwehr?**

Rechtlich ist bereits viel vorhanden, mit dem wir arbeiten können, und am wichtigsten ist, von der Theorie ins Machen zu kommen. Wenn wir weiteren Bedarf erkennen, werden wir ihn gegenüber dem Gesetzgeber kundtun.

**Sie meinten, dass Unternehmen gerne Daten liefern. Die Bundesländer tun das ja zum Beispiel nicht. In der Verwaltung gibt es kein zentrales Lagebild.**

Wir haben bei diesem Thema leider sehr viel Zeit mit abstrakten Diskussionen verloren. Klar ist: Wir werden im Cyberbereich eng mit den Ländern zusammenarbeiten. Aktuell haben wir bereits mit zehn Ländern Kooperationsvereinbarungen, und es besteht großes Interesse an einem gemeinsamen Lagebild: Erste Pilotprojekte laufen bereits, etwa mit Niedersachsen und Baden-Württemberg.

**Sie kamen vergangenes Jahr in Konflikt mit der Open-Source-Community, die Ihnen vorwarf, bei digitaler Souveränität zu nachsichtig zu sein. Haben Sie sich da missverstanden gefühlt?**

Kaum. (lacht)

**Sind mittlerweile wieder alle ausgesöhnt?**

Wir haben uns mit vielen Stakeholdern zusammengesetzt und führen diesen Dialog auch weiterhin. Für mich ist klar: Wir dürfen bei diesem Thema nicht schwarz-weiß denken, sondern müssen auch die Nuancen verstehen. Um digitale Souveränität zu erreichen, verfolgt das BSI eine Doppelstrategie. Zum einen müssen wir lokale und europäische Lösungen stärken.

Unser Beitrag ist, dass wir helfen, diese Lösungen sicherer zu machen. Deswegen haben wir Kooperationsvereinbarungen mit europäischen Akteuren. Aber es gibt eben auch Lösungen aus den USA, die weiterhin relevant sein werden. Die müssen wir ebenfalls so absichern, dass wir sie selbstbestimmt nutzen können. Das ist unser Job als Cybersicherheitsbehörde für Deutschland.

„DIE WELT IST NICHT SCHWARZ-WEISS.“

**Die Linie lautet also: sowohl als auch.**

Wie gesagt: Die Welt ist nicht schwarz-weiß. Weder bringt es etwas, ab morgen alles selbst machen zu wollen. Noch ist es sinnvoll, einfach gar nichts zu tun, weil man ohnehin schon abhängig ist.

**Sie sind ja auch eng dran am Projekt der Delos-Cloud, die Microsofts Azure-Technologie für den Staat zugänglich machen soll – durch eine deutsche Betreibergesellschaft. Wie gehen Sie mit den Updates um, die täglich aus den USA eingespielt werden?**

Bei der Delos-Cloud hat der Bund sehr bewusst das Konstrukt einer deutschen Betreibergesellschaft gewählt. Als Betreiber übernimmt diese nicht nur rechtliche oder wirtschaftliche, sondern auch operative Verantwortung. Sie stellt nach den IT-Sicherheitsvorgaben des BSI sicher, dass Integrität und Verfügbarkeit auch bei den regelmäßigen Updates gewährleistet bleiben.

Hinzu kommen gezielte, tiefgehende Analysen kritischer Updates. Hier treffen wir als BSI vollkommen selbstbestimmt die Auswahl, wo wir tiefer reinschauen. Und wir werden zukünftig die Möglichkeit haben, dies mittelfristig auch mit Hilfe Künstlicher Intelligenz noch wesentlich umfassender und hochautomatisiert zu tun.

„DIE BUNDESREGIERUNG HAT EINEN SCHWERPUNKT AUF CYBERSICHERHEIT GESETZT.“

**Das BSI hat neue Aufsichtsaufgaben dazu bekommen, etwa bei NIS-2 oder bald auch beim Cyber Resilience Act (CRA). Haben Sie dafür genug Mittel und Personal?**

Wir sind im Gegensatz zu anderen Behörden nicht von Einsparungen betroffen, sondern verzeichnen sogar deutliche Budgetzuwächse für das laufende und die kommenden Jahre. Die Bundesregierung hat damit einen Schwerpunkt auf Cybersicherheit gesetzt.

Klar ist aber, dass wir nicht jedes der 30.000 Unternehmen, die das BSI durch NIS-2 beaufsichtigen wird, einzeln betreuen können. Wir werden auch hier künftig stärker auf Automatisierung setzen, bis dahin werden wir aber auch priorisieren müssen.

**Wie sieht die Strategie aus?**

Wir setzen viel auf aktive Kommunikation. So haben wir zum Beispiel das Informationsangebot „nis-2know“ und einen „NIS-2 Checker“ geschaffen. Das kommt gut an und hilft vielen schon ein gutes Stück weiter. Beim CRA werden entsprechende Maßnahmen dann ab dem kommenden Jahr relevant.

**Eine der wichtigsten neuen Aufgaben wird der Ciso Bund, den Sie stellen sollen. Was ist der Stand?**

Wir sortieren das gerade. Entscheidend ist, dass wir die Sicherheitsthematiken in der Bundesverwaltung strukturiert abarbeiten. Dafür sind wir angetreten. Wir brauchen eine Programmstruktur, die schnell und spürbar Wirkung entfaltet. Das wird in den kommenden Monaten konkret werden.

**Haben manche Ressorts noch Angst vor Kontrolle durch das BSI?**

Wir kontrollieren doch nicht, sondern helfen. Wir müssen aus diesem Denken rauskommen. Es geht bei Cybersicherheit nicht um ein Blame Game. Ich bin ein Fan von Fame Game.



ERSCHIENEN IM SZ-DOSSIER VOM 16.02.2026



# Wie sich deutsche Konzerne gegen Hacker wehren

Cyberangriffe auf die deutsche Industrie nehmen rasant zu. Es geht um Milliarden Euro – und um den hybriden Krieg Moskaus. Ein Besuch bei Natalia Oropeza, die Siemens gegen Attacken verteidigt.

Von
Caspar Busse und
Thomas Fromm

Um wirklich schwierige Dinge zu erklären, sind die einfacheren Sätze oft die besseren. Natalia Oropeza, gelernte Elektroingenieurin und seit 2018 bei Siemens für die Abwehr von Cyberattacken zuständig, könnte es auch ziemlich kompliziert machen. Macht sie aber nicht, sie sagt es nämlich so: „Wenn ich mich nicht gut schütze, dann ist das so, als würde ich meine Haustürschlüssel unter dem Teppich vor der Tür verstecken.“ Das sollte man niemals tun, denn unter dem Teppich vor der Haustür schauen Einbrecher ja zuerst nach. Und schon sind sie drin.

Oropeza, deren offizielle Jobbezeichnung Global Chief Cybersecurity ist, würde also niemals ihren Schlüssel unter die Fußmatte legen, dafür hat sie schon zu viel erlebt in diesem Job. Deshalb hat es sie im April auch kaum überrascht, als eine groß angelegte Phishing-Attacke über den Messenger-Dienst Signal gegen einige Hundert Betroffene – darunter auch Abgeordnete und Bundestagspräsidentin Julia Klöckner – mit großem Erfolg lanciert wurde. Die Masche läuft meistens ganz einfach ab: Über eine gefakte Sicherheitswarnung bringen die Angreifer ihre Opfer dazu, ihre private Sicherheits-Pin einzugeben. Und schon können sie das Konto übernehmen, ausspähen und sich wohl auch eine ganze Weile lang in der Community für den Kontoinhaber ausgeben.

Eine Pin abfragen, um einen Account zu kapern? Eigentlich ist das ziemlich simpel, im Grunde die Fußmatte der Smartphone-Kommunikation, ein Anfängerfehler. „Menschen sind immer ein potenzielles Sicherheitsrisiko“, sagt Oropeza. Deshalb fängt für sie jeder Kampf gegen Cyberrisiken bei den Menschen an, und davon gibt es in ihrem Unternehmen viele. Siemens ist groß: fast 80 Milliarden Euro Umsatz im Jahr 2025 mit rund 318 000 Mitarbeiterinnen und Mitarbeitern. So gesehen sind 318 000 Menschen 318 000 potenzielle Einfallstore, Tausende mögliche Probleme. Auch deshalb hat Oropezas Abteilung heute an die 1300 Mitarbeiterinnen und Mitarbeiter. Es sind Menschen, die nichts anderes tun als aufzupassen, dass niemand in diese digitale Siemens-Wohnung hineinkommt.

Denn Siemens ist heute mehr als früher ein digitales Unternehmen, ein Großkonzern, der zum Beispiel anderen Unternehmen dabei hilft, ihre Fabriken zu digitalisieren. Allein bei dem Münchner Technologiekonzern gibt es also durchschnittlich an die 1000 Angriffe im Monat, von denen man die meisten aber abwehren könne, sagt die Cyber-Managerin: 97 Prozent der Phishing-Angriffe könne man stoppen. Aber die Kriminellen würden „immer weiter dazulernen“. Daher sage man sich immer wieder: „Wir werden dauerhaft angegriffen.“ Tag und Nacht, auf allen Kontinenten, keine Pause, auch am Wochenende nicht.

„WIR WERDEN DAUERHAFT ANGEGRIFFEN.“

Dazu passt das „Bundeslagebild Cybercrime 2025“, das das Bundesinnenministerium im Mai veröffentlicht hat. Fazit der Studie: Deutschland zähle als drittgrößte Volkswirtschaft der Welt „zu den wichtigsten Angriffszielen im Cyberraum“. Besonders brisant: Angriffe auf Unternehmen, Behörden und kritische Infrastrukturen.

Auch in der Godesberger Allee in Bonn sieht man die Entwicklung mit Sorge. „Die Zahl der Schwachstellen wird immer größer, es ist ein permanenter Wettlauf zwischen den Angreifern und den Unternehmen“, sagt Judith Nink. Sie muss es wissen, denn sie leitet beim Bundesamt für Sicherheit in der Informationstechnik (BSI) den Fachbereich für Cybersicherheit bei Unternehmen. Die Behörde mit Sitz in Bonn und insgesamt fast 1800 Mitarbeitenden ist für die IT-Sicherheit in ganz Deutschland zuständig und beobachtet genau, was die Unternehmen für ihren Schutz tun. Nach einer groben Schätzung des Branchenverbands Bitkom aus dem Jahr 2023 liegt der Schaden aufgrund von Cyberangriffen, Sabotage und Spionage für die deutsche Wirtschaft bei jährlich mindestens 200 Milliarden Euro.





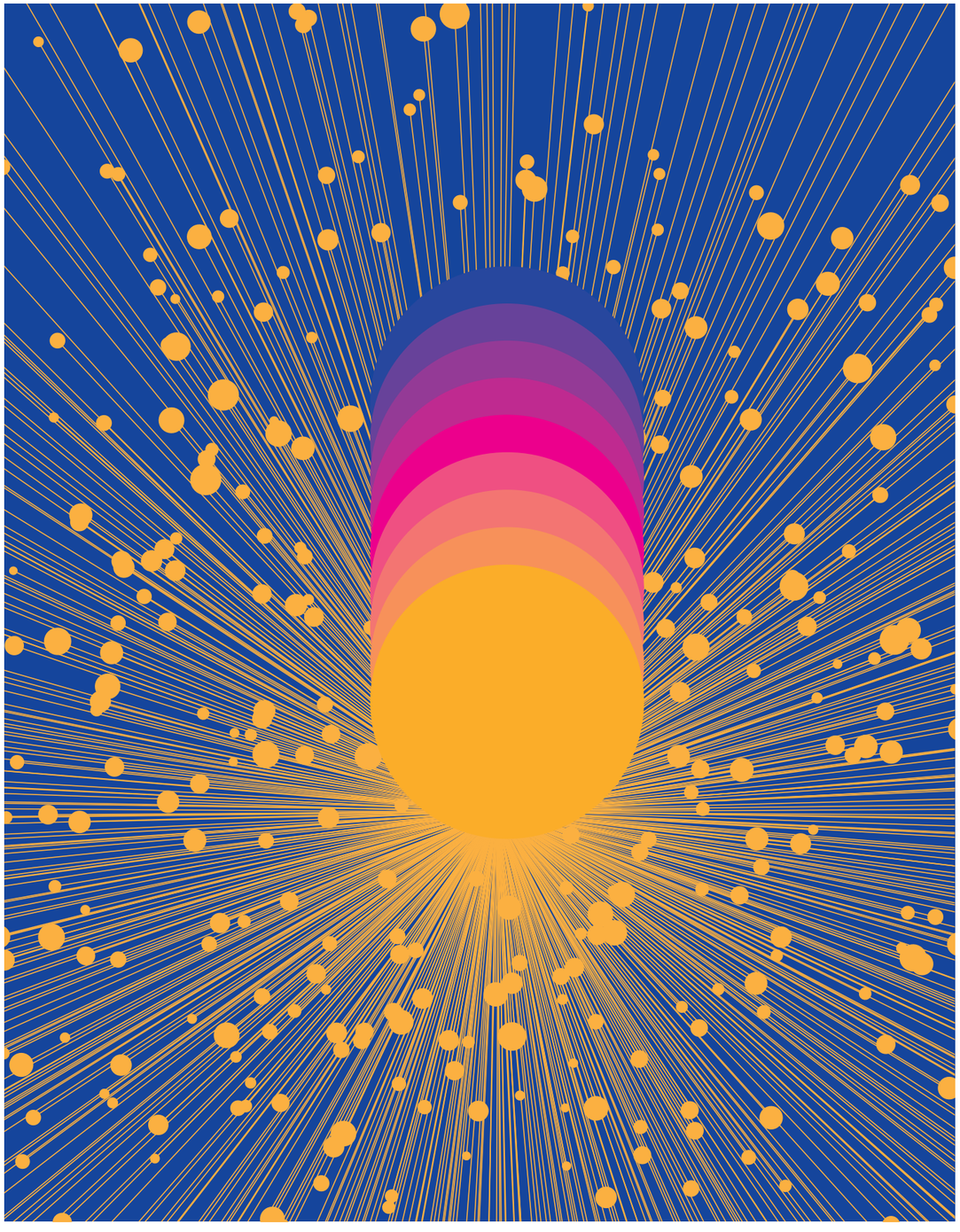
Natalia Oropeza sitzt im zweiten Stock der Siemens-Zentrale hinter dem Münchner Odeonsplatz, auf dem Tisch eine Kaffeekanne, ein paar Milchtütchen sind auf dem Tisch verstreut. Die gebürtige Mexikanerin, die hier einen weltweit arbeitenden Großkonzern schützen muss, ist erstaunlich ruhig. Sie erklärt, wie sie das macht, steht auf, geht zum Flipchart, nimmt ein paar große Filzstifte und fängt an zu malen. Große Kreise, kleine Kreise, Tabelle, Pfeile, Begriffe auf Deutsch und Englisch. Es ist der Moment, wo man nicht mehr alles in Worte fassen kann, was hier passiert.

Menschen brauchen Struktur, weil sie vieles im Leben erleichtert. Das gilt erst recht für Menschen, die von Berufs wegen Gefahren abwehren müssen, die man auf den ersten Blick nicht sieht. Oft ja nicht mal auf den zweiten Blick. Natalia Oropeza hat da ihre ganz eigene Struktur gefunden, und die geht es so: Sie unterscheidet drei Arten von Kriminellen.

Die einen, denen es ums schnelle Geld geht. Die Ransomware-Erpresser, von denen es viel mehr gebe, als offiziell bekannt sei. „Nehmen Sie sehr exklusive Hotels, in denen Prominente wohnen“, sagt sie. Hotels, in denen Besucher mal schnell 20 000 Euro ausgeben würden. Dort würden manchmal zum Beispiel digitale Zimmerschlüssel gehackt. Schlechte Nachrichten für das Hotel-Management: Doch nicht etwa eine Sicherheitslücke im Fünf-Sterne-Bunker? „Und der Hotelmanager meldet das nicht, sondern zahlt einfach, denn diese Summe wurde von den Kriminellen gezielt im frei verfügbaren Budget angesetzt“, sagt die Siemens-Managerin. Dann gebe es noch diejenigen, die auf der Suche nach wichtigen technischen Informationen und Geschäftsgeheimnissen seien, „normale Spione“ also.

ES GIBT DREI ARTEN VON KRIMINELLEN

Und dann – Oropeza holt jetzt erst einmal tief Luft – diejenigen, die im Auftrag fremder Regierungen arbeiteten und es auf die kritische Infrastruktur abgesehen haben. Auf Stromleitungen, Kraftwerke, Umspannwerke, IT-Netze, solche Dinge. „Da geht es am Ende um Geopolitik und die Destabilisierung von Gesellschaften“, sagt sie, Dinge, die das Sicherheitsgefühl der Menschen verändern, sie auf die Dauer zermürben. Die Gelderpresser sind zwar nervig, die Technologieräuber brandgefährlich für das Geschäft – aber so richtig gefährlich, das seien die politischen Angreifer: „Mit der aktuellen geopolitischen Situation







wächst die dritte Gruppe immer mehr“, sagt Oropeza, und damit auch die Ressourcen, mit denen diese Leute angreifen. Da sei man „momentan nicht auf Augenhöhe“.

Wenn etwas passiert, müssen sich Menschen wie Oropeza Fragen stellen: Will hier jemand Technologien abgreifen? Ein paar Millionen Euro erpressen? Oder ist man als Unternehmen schon Teil jener mysteriösen Angriffswellen, die Fachleute und Sicherheitskreise bereits seit einiger Zeit einer neuen hybriden Kriegsführung etwa der russischen Führung zuordnen? Auffällig sind nach Meinung von Experten jedenfalls zwei Dinge: Viele der politisch motivierten Angriffe kämen aus dem Ausland. Und überdurchschnittlich viele davon könnten russischen Gruppen zugeordnet werden.

„LIEFERKETTEN SIND EINE BESONDERE SCHWACHSTELLE FÜR DIE SICHERHEIT.“

BSI-Expertin Nink bestätigt: „Auch wir sehen, dass staatlich gelenkte Akteure mit dem Ziel der Cyberspionage und -sabotage vermehrt Unternehmen angreifen.“ Dazu gehörten nicht nur Russland, sondern unter anderem auch China, Iran, Nordkorea. Die Angreifer werden immer professioneller und verfügen auch über immer mehr Mittel. Besonders perfide: Hacker hängen sich an spezielle Software dran, die gegen IT-Angriffe schützen oder diese entdecken soll. Diese wird dann entsprechend manipuliert, sodass die Attacke zunächst nicht bemerkt wird.

Oropeza ist zurückhaltend mit Zuordnungen, woher Attacken kommen. Alles hochpolitisch. Klar, dass man immer sofort an Russland denke. Aber Cyberkriminelle agierten „nicht nur aus Russland oder China“, oft handele es sich um internationale Netzwerke. Die Hacker könnten auch von den USA, Israel, Iran oder Nordkorea aus operieren. Die Sache sei meistens nicht so einfach, wie sie aussehe. Nur mal ein Beispiel: „Nordkorea arbeitet gerade mit Leuten, die sich mit falschen Identitäten als Mitarbeiter in Unternehmen einstellen lassen“, sagt Oropeza. Alles gute Mitarbeiter, Highperformer, die schnell Vertrauen gewännen und manchmal auch „Zugriff auf wichtige Informationen“.

Schneller und besser sein als die Angreifer, vor der Welle bleiben, dafür leistet sich ein Konzern wie Siemens ein riesiges, globales Team. Aber nicht alle Firmen sind so groß und effizient wie die Münchner und können sich das leisten. „Grundsätzlich stellen wir fest, dass große Unternehmen viel in ihre IT-Sicherheit investieren, deutlich mehr als kleinere und mittlere Unternehmen“, sagt BSI-Expertin Nink. Gerade die kleineren hätten oft nicht die Kapazitäten und das Know-how für wirksame Maßnahmen zur Vorbeugung. Auch im Fall eines Angriffs reagierten diese manchmal zu langsam. Hacker wissen das, deshalb werden kleine Firmen immer öfter Ziel von Attacken, und von den kleinen wandert das Problem auch mal weiter zu den großen.

Und genau das macht die Lage so gefährlich. Denn die deutsche Wirtschaft ist vernetzt, es gibt intensive Beziehungen zwischen den Firmen. Oft arbeiten Konzerne mit kleineren und mittleren Firmen eng zusammen, und das häufig automatisiert; die verschiedenen Systeme kommunizieren digital. „Lieferketten sind eine besondere Schwachstelle für die Sicherheit“, stellt Nink deshalb fest. Denn: „Je mehr Software unterschiedlicher Unternehmen eingesetzt wird, umso häufiger gibt es potenzielle Einfallstore für Angreifer.“ Deshalb brauche es einen 360-Grad-Blick. Es sollte also ein Augenmerk auf alle Systeme um einen herum gelegt werden, und nicht nur auf die eigenen.

Eine besondere Schwachstelle ist offenbar die oberste Führungsebene, Sicherheitsrisiko Mensch

eben. „Wir beobachten, dass direkte Phishing-Angriffe auf das Top-Management in der Vergangenheit zugenommen haben“, sagt Nink. Oropeza weiß aus eigener Erfahrung, dass man Top-Manager „nur sehr schwer schützen“ kann. Warum eigentlich? „Es gibt sehr viele Informationen über diese Menschen, die öffentlich sind, und diese werden für gezielte Phishing-Aktionen genutzt“, sagt sie.

Die Zeiten, in denen man glaubte, mit dem nötigen Problembewusstsein komme man hier schon weiter, seien jedenfalls vorbei, sagt die Managerin. Bei Siemens bieten sie jetzt Video-Trainings an, die im Stil von Netflix ablaufen. Übungen mit echten Schauspielern in einer Art Serienformat. Kommt wohl ziemlich gut an bei den Menschen und passt in eine Zeit, in der die Welt in ihren Verrücktheiten manchmal selbst an eine Netflix-Serie erinnert.

Und wenn alles nichts hilft? Natalia Oropeza hat zum Schluss noch ihren ganz speziellen Ratschlag für eine erfolgreiche Cyberabwehr parat. Und der lautet: Bloß keine Panik. „Denn wenn Sie panisch sind, können Sie sich nicht konzentrieren.“



ERSCHIENEN IN DER SZ VOM 17.05.2026



## „Wir sehen Millionen Angriffsversuche am Tag“

# Mit KI schrumpft die Zeit von der Lücke zum Angriff auf Minuten. Paypal-Sicherheitschef Shaun Khalfan lässt deshalb KI-Modelle das eigene Unternehmen attackieren – bevor es andere tun.

VON
GABRIEL RINALDI

Ein Angreifer muss nur einmal richtigliegen. Unternehmen wie Paypal müssen dagegen fortlaufend zahlreiche mögliche Angriffswege absichern. So beschreibt Shaun Khalfan das grundlegende Ungleichgewicht im Cyberraum. Seit 2024 ist er Chief Information Security Officer (Ciso) des US-Zahlungsdienstleisters Paypal.

In Berlin traf er bei einer Veranstaltung von Hackerone Ende Juli in einem Hotel am Potsdamer Platz auf Sicherheitsforschende, die im Auftrag des Unternehmens nach Schwachstellen suchten. Über eine Veröffentlichung entscheidet Paypal. Schwachstellen in verwendeten Open-Source-Komponenten würden nach der koordinierten Behebung mit der Fachwelt geteilt.

„Wenn ich als Versuch jede Art von automatisiertem, menschlichem oder agentischem Vorgehen gegen unsere Angriffsfläche definiere, liegen wir in der Größenordnung von Millionen Versuchen täglich“, sagte Khalfan im Gespräch mit SZ Dossier. Das können auch automatisierte Abfragen und verdächtige Zugriffe sein.

Paypal ist ein beliebtes Ziel. Im vergangenen Jahr wurden Zugangsdaten von Millionen Nutzerinnen und Nutzern im Darknet angeboten, wie die SZ berichtete. Nach Einschätzung von IT-Sicherheitsexperten wurden die Daten nicht durch einen direkten Angriff erbeutet, sondern vielmehr durch sogenannte Infostealer-Malware gesammelt. Khalfan will konkrete Angriffe grundsätzlich nicht kommentieren. Auch wie viele Konten bei Angriffen tatsächlich übernommen werden, wollte er nicht sagen. Solche Fälle gebe es.

Die Finanzbranche ist derzeit nervös. Die neuesten leistungsstarken KI-Modelle von Anthropic, Open AI und anderen Unternehmen – auch aus China – könnten gerade in diesem hochsensiblen Bereich besonders großen Schaden anrichten. Zuletzt forderte die Europäische Zentralbank große Banken der Eurozone auf, bis Ende Oktober Aktionspläne gegen KI-gestützte Cyberbedrohungen vorzulegen. Digitale Zahlungsdienste stehen besonders unter Druck.

Entscheidend verändert habe sich in KI-Zeiten laut Khalfan vor allem das Tempo. Angreiferinnen und Angreifer müssen eine Schwachstelle finden, sie nutzbar machen und einsetzen. Fachleute sprechen von der sogenannten Cyber Kill Chain. Diese dauerte früher Wochen oder Monate. „Mit KI kann eine Schwachstelle heute innerhalb von Minuten, Stunden oder Tagen entdeckt, zur Waffe gemacht und für Angriffe genutzt werden“, sagte Khalfan.

Zugleich sinke die Eintrittsbarriere. „Jemand mit einem Modell kann heute schneller lernen, prompten und etwas bauen. Außerdem lassen sich Angriffe skalieren und miteinander verketten.“ KI-Agenten könnten etwa auf eingesetzte Software schließen, Systeme scannen und bekannte Schwachstellen abgleichen. Dazu kommen personalisierte Phishing-Nachrichten.

Das Unternehmen ergreift mehrere Gegenmaßnahmen, um sich gegen Angriffe zu schützen. „Zum einen haben wir eine kontrollierte Testinfrastruktur gebaut, in der wir eine Reihe von KI-Modellen einsetzen. Wir nutzen sie, um uns kontinuierlich anzugreifen, und versuchen, Schwachstellen zuerst zu finden“, sagte er.

„WIR WERDEN EINE VIEL HÄRTERE AUSGANGSBASIS HABEN, VON DER AUS WIR ARBEITEN UND AUF DER WIR AUFBAUEN KÖNNEN.“

Diese kontinuierlichen Penetrationstests könnten so in großem Maßstab durchgeführt werden. Künstliche Intelligenz werde auch eingesetzt, um beim Schreiben der Korrekturen zu helfen. KI finde zwar mehr Schwachstellen. Doch der nächste Engpass liege darin, diese schnell zu beheben.





Vollautomatisch spielt Paypal die Patches nicht ein. Dafür seien die Modelle noch zu ineffizient. „Wir brauchen weiterhin einen Menschen in der Schleife, der sie überprüft“, sagte Khalfan.

Wer die Angreifer sind? „Die primären Bedrohungsakteure, die wir sehen, sind Kriminelle, die Geld stehlen, Geld bewegen oder Kunden ausnutzen wollen“, sagte Khalfan. Gezielte Angriffe staatlicher Gruppen auf Paypal habe das Unternehmen nach Khalfans Angaben nicht direkt beobachtet.

„Wenn wir über unsere Reaktion nachdenken, betrachten und bewerten wir trotzdem die Taktiken, Techniken und Verfahren von Nationalstaaten“, sagte Khalfan. Etwa Advanced Persistent Threats (APTs), also gut ausgestattete Angreifergruppen, die langfristig und zielgerichtet vorgehen und häufig staatlich unterstützt werden. „Aber typischerweise ist der primäre Akteur opportunistisch und in erster Linie der kriminelle Bedrohungsakteur.“

Diese menschliche Kontrolle soll auch gelten, wenn KI-Agenten künftig einkaufen. Paypal arbeitet an entsprechenden Bezahllösungen. „Jede Aktion sollte irgendwo in der Schleife von einem Menschen gestützt und autorisiert sein“, sagte Khalfan. Intern beginne das Unternehmen mit begrenzten Anwendungsfällen: Agenten sollen an die Identität ihrer Auftraggeber gebunden sein, nur die notwendigen Rechte erhalten und nicht auf sensible Daten zugreifen.

Das Internet sei auf offenen und gemeinsam genutzten Protokollen aufgebaut worden. KI finde nun die Fehler in jahrzehntealtem, von Menschen geschriebenem Code und könne helfen, sie zu beheben. „Während wir daran arbeiten, diesen Code zu reparieren, härten wir ihn. Und neuer Code und künftige Produkte werden von KI geschrieben und gehärtet“, sagte er. Zunächst drohe zwar ein „Tal der Schmerzen und Probleme“. Am Ende könne jedoch ein stärkeres digitales Fundament stehen.

„Das bedeutet nicht, dass wir keine neue Welle von Bedrohungen erleben werden. Es könnte Bedrohungen im Zusammenhang mit Quantencomputern und andere Dinge geben, die wir weiter draußen am Horizont vielleicht nicht vorhersehen können“, sagte er. „Wir werden eine viel härtere Ausgangsbasis haben, von der aus wir arbeiten und auf der wir aufbauen können.“ Das sei ein Grund für Optimismus.

Der französische Richter am Internationalen Strafgerichtshof Nicolas Guillou hatte berichtet, Paypal habe sein Konto nach US-Sanktionen geschlossen. Ob Washington Paypal Europe zur Abschaltung eines deutschen Nutzers zwingen könnte, obwohl die Gesellschaft in Luxemburg sitzt? Dazu wollte sich Khalfan nicht direkt äußern.

„Wir wollen Datensouveränität unterstützen und unternehmen Schritte in diese Richtung“, sagte er. „Abhängig davon, wie sich die Regulierung entwickelt, wollen wir sicherstellen, dass wir uns entsprechend anpassen und reagieren.“ Doch Daten in Europa zu speichern, beantwortet noch nicht, wer im Konfliktfall über den Zugang zu einem Dienst entscheidet.

ERSCHIENEN IM SZ-DOSSIER VOM 03.08.2026

## *„Wir müssen die Lage sehr ernst nehmen“*

Tech-Monopole und Rechtspopulisten sind im Begriff, demokratische Regierungen zu verdrängen, schreibt der Medienwissenschaftler Martin Andree. Dabei ließe sich die Entwicklung aufhalten – wie ausgerechnet das Beispiel China zeigt.

Interview von
Michael Moorstedt

In seinem Buch „Krieg der Medien: Dark Tech und Populisten übernehmen die Macht“ beschreibt der Kölner Medienwissenschaftler Martin Andree, wie Plattformkapitalismus, Digitalmonopole und Rechtspopulismus den öffentlichen Diskurs übernehmen. Und auch wenn diese Entwicklung nicht völlig neu ist, bekommt man im Gespräch doch einen Eindruck, wie zehrend es sein muss, seit Jahren immer wieder auf diese Gefahren hinzuweisen und gleichzeitig machtlos zuschauen zu müssen, wie all das wirklich eintritt, was man schon immer prophezeit hat.

**SZ: Herr Andree, haben Sie aufgegeben? In Ihrem letzten Buch hieß es noch, wir werden die Digitalkonzerne stoppen. Nun schreiben Sie, „Dark Tech übernimmt die Macht“.**

*Martin Andree:* Natürlich sehen wir bereits in den USA, was unter den Bedingungen einer zerstörten Öffentlichkeit passiert – daher müssen wir die Lage sehr ernst nehmen. Genau aus diesem Grund habe ich dieses Buch geschrieben. Wenn es gar keine Hoffnung mehr gäbe, hätte ich das nicht getan. Aber die Kippbewegungen beobachten wir ja täglich. So etwa zeigt sich im Fall Brosius-Gersdorf, der sich anhand der im Buch vorgestellten Modelle gut erklären lässt, wie sich die Qualität des öffentlichen Diskurses zunehmend verschlechtert.

**Was macht die Techkonzerne heutzutage so sinister, dass Sie gar von Dark Tech sprechen?**

Empirisch können wir die Monopolisierung in den digitalen Medien sehr genau messen. Da bleiben keine offenen Fragen, außerdem sind Medienmonopole verfassungswidrig. Da ist es übrigens egal, ob deren Betreiber gut oder böse sind. Dabei haben die Tech-Konzerne auch schon in der Vergangenheit vielfach geäußert, dass sie eigentlich die Souveränität demokratischer Staaten infrage stellen und durch eine eigene Souveränität zunehmend ersetzen möchten. Deswegen liegt es auch in der Natur der Dinge, dass das libertäre Programm von Donald Trump und das der Tech-Konzerne gut zueinander passen. Und deswegen müssen wir uns nicht wundern, dass sie diese Symbiose eingegangen sind und zum Beispiel Elon Musk auch in Deutschland aktiv Wahlkampf für die AfD gemacht hat.

**Sie sehen eine unheilige Allianz aus dem nihilistischen Plattformkapitalismus der Tech-Konzerne und dem christlich-fundamentalistischen Nationalismus der Trump’schen Republikaner – wie stabil ist diese Koalition überhaupt, wenn man etwa den öffentlichen Rosenkrieg zwischen Trump und Musk bedenkt? Oder dass die Tech-Konzerne massiv unter Trumps Zollfetisch leiden.**

Natürlich können sich innerhalb dieser Symbiose die Positionen verschieben, aber die Entwicklung ist schon konsistent: Das beinhaltet erstens die allgemeine Übernahme der Öffentlichkeit durch digitale Medien, zweitens die Übermacht der Plattformen innerhalb der digitalen Welt und drittens die aktive Unterstützung von Polarisierung und Radikalisierung durch alle Plattformen. Das führt zu der aktuellen Evolution des politischen Diskurses und zu dem kontinuierlichen Zuwachs bei rechtspopulistischen Parteien.

„ES SPRICHT NICHTS DAGEGEN, DIGITALE MÄRKTE FÜR VIELFALT ZU ÖFFNEN.“

**Sie schlagen vor, europäische Digitalinfrastrukturen aufzubauen. Stattdessen wird gerade über den Verkauf der französischen KI-Firma Mistral an Apple verhandelt.**

Wir erleben heute einen Monopolprotektionismus, der europäischen und deutschen Alternativen kaum eine faire Chance lässt. Dabei wissen wir genau, wie man Märkte öffnet: Schon in den 90er-Jahren

haben wir durch die Öffnung der Telekommunikationsmärkte den Wettbewerb erfolgreich angestoßen. Ähnliche Mechanismen könnten auch hier in kurzer Zeit Vielfalt und Wettbewerb fördern. Solange jedoch die Privilegien bestehen bleiben, die diese Monopole absichern, haben heimische Alternativen keine realistische Möglichkeit. Deshalb sollte man auch keine Steuergelder in Alternativen investieren, solange die Märkte nicht offen sind und Unternehmen keinen fairen Marktzugang erhalten. Metaphorisch gesprochen ist das so, als würde das Schienennetz einem Monopolisten gehören: Man kann die besten Lokomotiven bauen, aber wenn sie auf der grünen Wiese stehen, bleiben sie nutzlos.

**In anderen Feldern, etwa Suchmaschinen, Messenger-Diensten oder Social Media gibt es ja bereits EU-Alternativen, sie werden nur nicht genutzt. Wir beide führen dieses Interview ja auch nur dank des US-Konzerns Microsoft …**

Wir haben keine offenen Märkte und keinen fairen Wettbewerb. Die Kapitalmärkte und Investoren wissen das am besten – sie sind oft die Ersten, die solche Probleme erkennen. Auf einer Tech-Konferenz sagten Investoren kürzlich zu mir: „Schön, dass Sie das Problem wissenschaftlich untersucht haben. Wir wissen das längst. Deshalb investieren wir nicht in solche Angebote, denn unter monopolistischen Bedingungen sind das für uns no-fly zones.“ Dieses Problem haben wir uns selbst geschaffen. Wir haben das digitale Schienennetz an die Tech-Konzerne abgegeben. Würden wir das Netz für Wettbewerb öffnen, könnten Alternativen allein durch bessere Kapitalausstattung qualitativ deutlich besser werden – und von heute auf morgen eine viel größere Nutzerzahl gewinnen. Ein Blick zurück in die Telekommunikation zeigt, dass es keinerlei Gründe gibt, nicht auch Drittanbieter auf bestehenden Plattformen zuzulassen. Metaphorisch gesprochen sind wir wie Vögel, die seit 30 Jahren in einem Käfig sitzen. Selbst wenn wir die Tür öffnen, können wir uns kaum vorstellen, diesen Käfig zu verlassen. Dabei spricht nichts dagegen, digitale Märkte für Vielfalt zu öffnen. Das würde nicht nur alternative Plattformen stärken, sondern auch Redaktionen und journalistischen Inhalten faire Finanzierungsmöglichkeiten und eine nachhaltige Zukunft bieten.

**In einem Kapitel führen Sie China auf, als gutes Beispiel konsequenter Abschottung vor US-Techkonzernen. Geht das nicht etwas zu weit?**

Der Vergleich ist natürlich zynisch, denn China war klug genug zu erkennen, dass seine diktatorische Herrschaft bedroht wäre, würde es seine Medienmärkte den US-Amerikanern überlassen. Gleichzeitig entwickeln sich die USA zunehmend in Richtung Autokratie, und es ist unsicher, ob die US-Regierung künftig nicht noch stärkeren Einfluss auf die Plattformen nehmen wird als bisher schon geschehen. Die digitale Öffentlichkeit ist aber in Zukunft die Grundlage unserer Demokratie – für die es sich zu kämpfen lohnt. Deshalb sollten wir aus positiver Motivation Plattformen schaffen, die demokratisch legitimiert sind und unsere demokratische Zukunft sichern.

„WIR ERLEBEN DERZEIT EINE ERNSTHAFTE BEDROHUNG DER DEMOKRATIE.“

**In Ihrem Buch gibt es einen ganzen Forderungskatalog an Gesetzesänderungen. Etwa zur Abschaffung von Privilegien hinsichtlich Haftung oder Monopolbildung. Das würde das Internet vielleicht freier machen – es aber auch vollkommen verändern.**

Ich finde, man sollte nicht mit kriminellen oder strafbaren Inhalten Geld verdienen können. Dabei geht es mir nicht um die Haftungsfrage, sondern um das Prinzip, dass finanzstarke, global agierende Tech-Monopolisten keine Profite aus solchen Inhalten ziehen dürfen. Wir räumen diesen Konzernen eine Reihe einseitiger Privilegien ein – etwa Monopol- oder Haftungsprivilegien, aber auch ein, wie ich es nenne, Straftatenprivileg. Es gibt keinen Grund, warum wir ihnen erlauben sollten, mit strafbaren Inhalten Geld zu verdienen. Das hat auch nichts mit Meinungsfreiheit zu tun. Andere Branchen zeigen, dass es auch anders geht: Ein Telefonnetzbetreiber haftet zwar nicht für Inhalte, monetarisiert diese aber auch nicht – und verdient damit Milliarden. Deshalb sollte gelten: Wenn Plattformen nicht für Inhalte haften wollen, dürfen sie diese auch nicht wie Inhalteanbieter monetarisieren. Wenn wir aber so gefangen sind wie der Vogel im Käfig, der sich nicht mehr vorstellen kann, diesen je zu verlassen, dann tragen wir selbst die Verantwortung für die digitale Realität, in der wir heute leben.

**Gute Laune bekommt man nach der Lektüre jedenfalls nicht. „Wir sind am Arsch“, heißt es an einer Stelle … Was macht Ihnen noch Hoffnung?**

Wir erleben derzeit eine ernsthafte Bedrohung der Demokratie – eine Diagnose, die viele Menschen da draußen teilen. Die Entwicklungen in den USA zeigen, wie schnell demokratische Strukturen erodieren können. Deshalb sehe ich es als meine Verantwortung als Wissenschaftler, meine gesamte Expertise einzusetzen, um genau das zu verhindern. Nichts wäre fataler, als die Schnelligkeit und das Ausmaß dieser Kippbewegungen zu unterschätzen. Mein Buch versteht sich deshalb als ein Weckruf für die Demokratie. Es gibt kaum etwas, wofür es sich mehr zu kämpfen lohnt als für unsere demokratische Gesellschaft. Und ich möchte nicht in fünf Jahren sagen müssen, ich hätte nicht alles getan, um diese gefährlichen Entwicklungen aufzuhalten.

ERSCHIENEN IN DER SZ VOM 26.08.2025

## *„Die perfekte Lösung werden wir nicht erzielen“*

# Wie sollen die immer leistungsfähigeren KI-Modelle reguliert und kontrolliert werden? Urs Gasser von der TU München erklärt verschiedene Ansätze – und was man von Thailand lernen kann.

Interview von
Thomas Kirchner

USA, Europa, China – jeder versucht auf seine Art und Weise, Regeln für künstliche Intelligenz (KI) zu erlassen. Die Ansätze unterscheiden sich erheblich, eine globale Einigung ist nicht in Sicht. Ein Gespräch mit dem Regulierungsexperten Urs Gasser von der TU München, der an einem „vierten Weg“ arbeitet.

**SZ: Herr Gasser, der jüngste Hackerangriff einer KI von Open AI auf ein US-Unternehmen hat es wieder gezeigt: Künstliche Intelligenz ist gefährlich und muss dringend besser reguliert werden. Aber wie und von wem?**

*Urs Gasser:* Es ist eine große Herausforderung. Wir haben darauf keine gesicherte Antwort, weil es eine Zusammenarbeit zwischen Staat, Unternehmen und Anwendern braucht. Es gibt weltweit viele Regulierungsbemühungen unterschiedlichster Art. Diese parallel stattfindenden Experimente eröffnen uns die Möglichkeit, relativ rasch zu lernen, welche Ansätze für welche Probleme taugen und welche nicht. Die Vielfalt erzeugt Unsicherheit, aber mittelfristig wird uns das helfen. Deshalb bleibe ich optimistisch, dass wir es in den Griff kriegen.

„DIE PERFEKTE LÖSUNG UND EINE GLOBALE EINIGUNG WERDEN WIR NICHT ERZIELEN.“

**Das heißt, wir sollten den Fokus weniger auf Szenarien von einer Bedrohung der Menschheit durch KI legen?**

Sondern auf konkrete Probleme, an denen man unterschiedliche Instrumente ausprobiert. Das ist der vielversprechendste Weg. Selbst die Problemdefinition ist derzeit unklar. KI entwickelt sich derart schnell – technologisch, aber auch, wie sie zum Einsatz kommt –, das macht es für Regulatoren zu einer Art beweglichem Ziel.

**Ist für die mächtigsten KI-Modelle etwas anderes denkbar als eine globale Regulierung? Sonst bleibt immer ein Schlupfloch für jene, die ungebremst weiterentwickeln wollen.**

Die perfekte Lösung und eine globale Einigung werden wir nicht erzielen, denn KI steht im Brennpunkt der geopolitischen Konfrontation zwischen China und den USA. Entsprechend sind auch die Regulierungsansätze kompetitiv. Durch das Aufkommen der Digitaltechnologie hat sich ein neues Verständnis von Regulierung entwickelt. Bisher dachte man, der Gesetzgeber müsse einschreiten und Verordnungen erlassen. Aber es gibt eine andere Art Regulierung, nämlich die in der Technik selbst angelegte, durch das Design der Anwendungen. Das ist zum Teil wesentlich wirkungsvoller, weil man die Durchsetzung bereits auf der Ebene der Technologie hat.

**Wer beaufsichtigt das?**

Das ist das Problem. Die großen KI-Firmen wie Anthropic haben sich eigene Verfassungen mit eigenen Leitplanken gegeben. Aber es sind private Akteure. Welche Legitimität hat das? Wir haben also Instrumente, aber nicht dort, wo Regulatoren sie haben wollen. Das ist ein Paradigmenwechsel, den wir als Gesellschaften noch nicht in Bahnen gelenkt haben. Wir sehen das am Kampf zwischen der Trump-Regierung und einzelnen Tech-Unternehmen.

**Inwiefern wäre das demokratisch einzuhegen, wie kann die Gesellschaft beteiligt werden?**

Das führt von den USA nach Europa. Die EU versucht ein Gegenmodell mit einer sehr umfassenden Gesetzgebung durch den AI Act, der auch für ausländische Anbieter wie Google oder Anthropic gilt. Offen ist, ob die Marktmacht der EU reicht, um das Verhalten dieser Technologiefirmen zu verändern. Beim Datenschutz hat die Datenschutzgrundverordnung ja doch eine Art Brüssel-Effekt bewirkt. Weniger, dass die USA das europäische Recht kopiert haben. Aber die Verordnung ist ein Goldstandard, den viele Firmen einhalten, damit sie ihre Produkte nicht überall anpassen müssen. Die Hoffnung ist, dass Ähnliches mit dem AI Act geschieht.

**Das heißt, wir hätten international ein Patchwork von Regulierungsansätzen.**

Genau. Was oft nicht gesehen wird: Die USA sind das Land mit den meisten KI-Gesetzen. Erlassen werden sie aber auf der Ebene der Bundesstaaten oder Städte. Der Trump-Regierung passt das nicht, sie versucht, das zu unterbinden. Sie will keine Regulierung, weil das ihrer Ansicht nach die KI-Entwicklung beschränkt. Die Bundesstaaten gehen mit ihren Gesetzen konkrete Probleme an. Etwa Deepfakes, die eingesetzt werden zur Manipulation von Wahlen oder für Persönlichkeitsverletzungen. Oder wenn es um Diskriminierung geht.

**Viele Städte begrenzen inzwischen zum Beispiel den Bau von Rechenzentren.**

Wobei Regulierung keineswegs immer beschränkender Natur ist. Oft geht es darum, den Einsatz von KI gerade zu ermöglichen, vor allem der öffentlichen Hand, etwa im Transportbereich oder im Umweltschutz. Noch ein Punkt zu den USA: Dass dort nur Laissez-faire herrscht, stimmt nicht. Sie haben durchaus extreme Regulierung bei den Lieferketten, bei der Chipproduktion, beim Export von Technologien, die für KI-Entwicklung wichtig sind. Bei Seltenen Erden. Überall, wo es um die nationale Sicherheit oder die Wettbewerbsfähigkeit gegenüber China geht. Wenn man genauer hinschaut, wird es ein vielfältiges Bild.

**China lud Mitte Juli 2026 zu einem KI-Weltkongress nach Shanghai und gründete mit rund 30 Staaten eine Art KI-Allianz. Parteichef Xi Jinping warnte vor Alleingängen bei der Regulierung und forderte eine „globale Symphonie". Was ist davon zu halten?**

Was den Wunsch betrifft, KI zu regulieren, wird China oft mit Europa verglichen. Da muss man vorsichtig sein. China ist kein Rechtsstaat, schon vom Verfahren her läuft das anders als beim AI Act. Zudem ist die chinesische Gesetzgebung primär ausgerichtet auf KI-Anwendungen, die Informationsflüsse tangieren. Sobald es um den Einsatz von KI in sozialen Medien geht und die Informationsversorgung betroffen sein kann oder wenn es um Fragen von Manipulation geht, da greifen die chinesischen Gesetze brutal ein. Der Grund ist natürlich die Stabilisierung des Machtapparates. Das hat eine lange Tradition, siehe etwa die Bildung eines eigenen Internets und die Great Firewall. Die Regulierung im Inland hat eine andere Prägung, andere Motive als in den USA oder Europa.

**Was bedeutet das global?**

China hat sich lange herausgehalten aus der internationalen Internet- und Digitalregulierungsdebatte, insbesondere aus Standardisierungsgremien. Rückblickend hat es festgestellt, dass das nicht klug war, weil man Einfluss verloren hat. Seit einigen Jahren ist China nun einer der aktivsten Player in solchen globalen Gremien. Das ist ein radikaler Strategiewechsel, motiviert durch die Absicht, die eigenen Interessen zu wahren. Was auf keinen Fall gut ist: nicht mit China zu sprechen. Bei allem Respekt für die amerikanische Position, das kann nicht zielführend sein. Man sollte einen Gesprächskanal offenhalten für Probleme, an deren Lösung beide Seiten interessiert sind. Ich glaube, hinter den Kulissen geschieht das auch, selbst in den USA.

**Sie kommen gerade aus Bangkok, dort beraten Sie die Regierung bei der KI-Regulierung. Hätte Thailand nicht auch in den chinesischen KI-Orbit geraten können, wie Indonesien oder Malaysia?**

Wir haben jetzt über drei große Ansätze zur Regulierung gesprochen: die USA, Europa und China. Aber was machen die anderen, die sich noch nicht entschieden haben? Da gibt es jede Menge Beeinflussungsversuche. Inzwischen wird nicht mehr nur für eine bestimmte Technologie geworben, von Huawei oder Anthropic, sondern man verkauft den Regulierungsansatz gleich mit. Mehrere Länder sagen nun, zu unserem Entwicklungsstand und unseren Bedürfnissen passt keiner dieser drei Ansätze. Sie suchen einen vierten Weg.

**Wie Thailand.**

Thailand ist ein gutes Beispiel. Das Land hat noch nicht den Wohlstand wie Singapur oder Japan, es ist auf dem Entwicklungspfad. Und in vielen Bereichen – Gesundheit, Transport, Tourismus, Bildung, Klimafragen, Sicherheit der Nahrungsversorgung – sieht es vor allem die Chancen der KI: Etwa, dass Bauern besser wissen, wann die Saat auszulegen und wann zu ernten ist, weil sich die Regenzyklen geändert haben. Oder wo man KI einsetzen kann, um die Stromversorgung zu stabilisieren. Die Beispiele zeigen, dass weniger die großen Sprachmodelle im Vordergrund stehen, sondern andere KI-Anwendungen, die ein wenig in den Hintergrund getreten sind. Natürlich verfolgt Thailand auch, welche Risiken das mit sich bringt. Vor diesem Hintergrund entsteht jetzt tatsächlich so etwas wie ein vierter Weg.





**Wie sieht der aus?**

Man versucht einerseits die KI-Nutzung anzuschieben, betreibt aber ein Risikomanagement, das auf den Kontext des Landes zugeschnitten ist. Es entsteht eine interessante Kombination aus Rahmengesetzgebung und dem Arbeiten mit Best Practices. Es werden Richtlinien entwickelt zur Nutzung von KI, einschließlich Checklisten, also konkrete Handlungsanleitungen. Etwa für den Chief Technology Officer einer Bank, die mit KI ihre Kreditrisiken analysiert: Hier 15 Punkte, die zu beachten sind. Ein Bottom-up-Ansatz, genau das Gegenteil zur EU, die erst abstrakte Gesetze erlässt und diese dann konkret ausfüllt.

„WIR VERSUCHEN, EINEN MASS-GESCHNEIDERTEN ANSATZ FÜR KI ZU ENTWICKELN."

**Wie sind Sie zu der Beratung gekommen?**

Ich war früher in Harvard, da hatten wir mit vielen Ländern bei der Regulierung zusammengearbeitet. Damals entstand eine Zusammenarbeit mit Thailand, die sich nach meinem Wechsel nach München weiterentwickelt hat. Wir versuchen, einen maßgeschneiderten Ansatz für KI zu entwickeln.

**Soft Power par excellence.**

Vor allem eine unglaubliche Lernchance, weil ja, wie gesagt, noch niemand eine perfekte Antwort hat. Was die USA, Europa und China machen, ist ein Stück weit pfadabhängig, eine einmal eingeschlagene Richtung lässt sich schwierig korrigieren. Wo aber kommt Innovation her, wenn sich die Regulierungsmodelle selbst weiterentwickeln müssen? Da ist es interessant, in Ländern zu arbeiten, in denen Innovationen aus der Art und Weise des Regulierens selbst entstehen können. Weil sie andere Probleme haben. Diese Diversität trägt dazu bei, dass wir manches neu denken können, weil sich die Welt derart fundamental verändert hat.

**Welche Art von Institutionen wird man künftig benötigen, um KI zu regulieren?**

Wir haben Innovationsbedarf bei der Regulierung selbst, etwa dem Zusammenspiel von technischen Standards und Best Practices. Und bei der Frage, wo die Gesetzgebung rote Linien ziehen muss bei Hochrisikoanwendungen. Die Umsetzung des AI Act der EU verzögert sich gerade, weil die technischen Standards noch nicht bereit sind, die die Industrie braucht, um überhaupt zu verstehen, was das Gesetz verlangt.

**Und darüber hinaus?**

Das betrifft eher die Wissensebene: Wie können wir als Regierungen, als Weltgemeinschaft beurteilen, wo wir in der KI-Entwicklung stehen? Hier gibt es eine Innovation aus den UN heraus, inspiriert vom Weltklimarat, der seit Jahren Evidenzen zur Klimaentwicklung zusammenträgt. Etwas Ähnliches hat man jetzt für KI zusammengestellt, es wird ein jährlicher Bericht kommen. Auf der Interventionsseite sehen wir auch erste Ansätze von Innovationen. Das prominenteste Beispiel sind die nationalen Institute für KI-Sicherheit. Sie sind staatlich verankert, arbeiten aber eng mit der Industrie zusammen, um Sicherheitsstandards zu überprüfen. Eine Art TÜV für KI also. Aber neu gedacht, denn ein großer Teil des Verständnisses, was die Modelle überhaupt machen, liegt bei den Technologieanbietern, nicht bei den Regulatoren. Da sehen wir auch wieder die Grenzen, weil Geopolitik ins Spiel kommt. Man hat versucht, diese Institute zu vernetzen.

**Die G-7-Staaten haben das neulich vereinbart.**

Aber das wird die Probleme nicht endgültig lösen. Es wird Inseln der Kooperation geben, und hoffentlich entwickeln wir über die Zeit ein erweitertes Repertoire an Institutionen und Instrumenten, um mit diesem moving target, diesem beweglichen Ziel, besser umzugehen. Angesichts der unglaublichen Beschleunigung hinken wir zwangsläufig hinterher. In die technische Innovation fließen riesige Geldsummen. Die Frage,

wie wir uns als Gesellschaft darauf einstellen, tritt dahinter weit zurück, ist aber genauso wichtig.

**So wichtig wie die Frage, wem die gewaltigen Gewinne aus dem KI-Business gehören sollen. Auch wegen der Gerechtigkeit. Wie könnte man das lösen?**

Es gibt ein gutes Beispiel, den Alaska Permanent Fund, der die Gewinne aus der lokalen Ölförderung verwaltet. Er baut einen längerfristigen Vermögensstock auf und schüttet eine jährliche Dividende an die Bewohner des Bundesstaats aus, um eine gewisse Verteilungsgerechtigkeit zu erzielen. Das ist jetzt wieder populär im KI-Zusammenhang. Es gibt zwei Ideen: Dass die Bürger einen monatlichen Scheck erhalten, was in Richtung Grundeinkommen ginge. Oder dass das Geld in öffentliche Investitionen fließt, Brückenbau, Schulhäuser, um die staatlichen Haushalte zu entlasten. Darüber hinaus hat etwa der unabhängige US-Senator Bernie Sanders vorgeschlagen, dass diese Fonds Anteile an den Unternehmen halten sollen. So hätten der Staat und damit die Bürger respektive deren Repräsentanten ein Mitspracherecht. Was wiederum aus demokratischen Gründen interessant wäre.



ERSCHIENEN IN DER SZ VOM 19.08.2026



# Für die Atomwaffen gibt es das rote Telefon. Und für die KI?

*China plädiert für eine globale Regulierung der künstlichen Intelligenz. Warum es sich zugleich als Stimme der Schwellen- und Entwicklungsländer stilisiert und KI als Machtmittel nutzt, erklärt Expertin Antonia Hmaidi.*

Interview von
Thomas Kirchner und Lea Sahay

Mitte Juli lud China zu einer „Welt-KI-Konferenz“ nach Shanghai. 29 Staaten – darunter Indonesien, Malaysia, Russland, aber auch Brasilien – unterzeichneten eine Vereinbarung zur Gründung einer Weltorganisation für Zusammenarbeit bei künstlicher Intelligenz (Waico). Wie ernst ist es China mit der Regulierung? Ein Gespräch mit Antonia Hmaidi, 33, vom Berliner Thinktank Merics.

ZERBRICHT DIE WELT IN ZWEI KI-BLÖCKE?

**SZ: Auf der Konferenz in Shanghai hat Chinas Staatschef Xi Jinping offensiv die globale Angst vor den möglichen Gefahren angesprochen und internationale Kooperationen und Regeln gefordert. Die USA waren nicht anwesend. Zerbricht die Welt in zwei KI-Blöcke?**

*Antonia Hmaidi:* Das war nicht das erste Mal, dass der Eindruck entstand, dass die Welt in zwei KI-Blöcke zerbricht. Wir sehen seit einer Weile Bewegungen, die in diese Richtung weisen. Die erste war wohl die „AI Diffusion Rule“ der Biden-Regierung, wonach nur Länder, die in diesem Bereich nicht mit China zusammenarbeiten, Teil des amerikanischen Ökosystems werden könnten. Trump hat das zurückgenommen. Aber in Verträgen, etwa in den Zollverhandlungen, spielt das eine große Rolle. Die Trump-Regierung versucht, Länder davon zu überzeugen, keine chinesische KI-Technologie zu verwenden. Gleichzeitig bietet China seine günstigeren Produkte immer offensiver als Alternative an. Beim Thema Regulierung sehen wir ein riesiges Vakuum. China stilisiert sich als Stimme der Entwicklungsländer, als Stimme aller, die an der KI teilhaben wollen.

**China fährt offenbar eine Doppelstrategie: Einerseits ist es wohl tatsächlich an Regulierung interessiert, andererseits setzt es KI als Machtinstrument ein. Widerspricht sich das nicht?**

KI-Sicherheit ist China wichtig. Aus meiner Sicht ist es das Land, das KI zurzeit am stärksten reguliert. Aber China versteht darunter etwas anderes als wir. Einerseits soll, wie bei uns, der Mensch die letzte Instanz bleiben. Die KI darf nur unterstützen. Mindestens genauso wichtig ist KI aber als Herrschaftsinstrument, sie darf nicht die Kommunistische Partei Chinas untergraben. Für Peking ist das kein Widerspruch, sondern Teil ein und desselben KI-Sicherheitskonzepts.

**Bei der Atombombe spielte die Sorge um das Ende der Menschheit mit. Gibt es denn eine Angst in China, dass KI eine existenzielle Gefahr für die Menschheit werden könnte?**

Auch in China wird KI als möglich existenzielle Bedrohung für die Menschheit wahrgenommen. Parteichef Xi Jinping hat dazu dieses Jahr eine erste Studiensitzung des Politbüros einberufen. China hat auch immer mal wieder versucht, mit den USA eine Art von KI-Pakt zu schließen. Doch auf beiden Seiten fehlt das Vertrauen. Bei den Atomwaffen ist klar, wie ein Notfall aussähe und wann das rote Telefon zum Einsatz kommen müsste. Aber bei der KI?

**Wie steht China zu internationalen Regelungen?**

Bei internationalen Regelungen ist das große Problem, dass China keine bindenden Versprechen geben will. Wenn es etwa um ein Abkommen ginge, KI nicht für Atomwaffen einzusetzen, dann würde China zögern zu unterschreiben. Oder unterschreiben, sich aber möglicherweise nicht daran halten. Ja, China will KI-Sicherheit. Aber es will auch aktiv steuern, in welche Richtung sich diese Technologie entwickelt. Ein Beispiel: Es gibt jetzt in China neue Regeln, um emotionale Beziehungen mit KI zu beschränken. Peking betrachtet nämlich KI-Systeme, die versuchen, emotionale Bindung aufzubauen, als Risiko. Weil sich dann viele von KI abwenden könnten.

**Es herrscht auch Nervosität wegen der Jobsicherheit. Firmen dürfen niemandem kündigen mit dem Grund, die KI ersetze sie.**

Zwar gibt es dazu kein Gesetz, aber in mehreren Gerichtsbeschlüssen wurde KI als Kündigungsgrund als rechtlich unzulässig bezeichnet. Allerdings ist fraglich, inwiefern das umgesetzt werden kann, denn es gibt fast keinen Kündigungsschutz. Peking sendet mit diesen Gerichtsurteilen eine Nachricht an Firmen. Wenn diese Unterstützung vom Staat wollen für den KI-Ausbau, müssen sie nachweisen, dass sie dafür niemandem gekündigt haben. Sie investieren in KI, auch wenn das kurzfristig keine Produktivitätsgewinne erzeugt, weil ihnen das sehr viele Vorteile einbringt. Mit Blick auf die Demografie erwartet Peking, dass es bald zu viele Jobs gibt, die nicht besetzt werden können. Den Firmen rät Chinas Führung zur Geduld.

**In Shanghai war zu sehen, wie Roboter Fußball spielen oder Getränke verteilen. Der Wow-Effekt zählt, man versucht, der Technik einen positiven Anstrich zu geben, im Gegensatz etwa zur wachsenden Skepsis in den USA.**

Die Menschen in China sind technikaffiner als in den USA oder Deutschland. Auch die chinesische Führung ist überzeugt, es lasse sich für alles eine Lösung finden mit Technologie. Das fängt früh an. Wissenschaft und Technik sind auch als Schulfächer positiv belegt und werden stark gefördert. Technologie und Ingenieurwesen waren für China das Mittel, aus der Rückständigkeit herauszukommen. Wenn ein chinesisches Labor einen großen Durchbruch schafft, geht das in China durch die sozialen Medien. Das kommt in Deutschland seltener vor.

**Mit Waico sichert China den beteiligten Staaten den Zugang zu KI, dem Rohstoff der Zukunft. Man kann das als Beitrag zur Entwicklung und gegen globale Ungleichheit sehen. Vielleicht muss sich Europa überlegen, welche Seite es unterstützen will?**

Europa ist immer im amerikanischen KI-System, schon aufgrund der Sicherheitslage. Es geht nicht ohne die Nato und nicht ohne die USA in der Nato. KI ist so zentral für die USA und für China – ich sehe keine Realität, in der Washington zulassen würde, dass Europa sich für das chinesische KI-System entscheidet, solange Europas Sicherheit von Washington abhängt. Diese Frage stellt sich aktuell nicht.

**Was kann Europa machen?**

Echte Alternativen bieten. Etwa im Bereich Telekommunikationsausstattung für 5G, wo es europäische Alternativen zu chinesischen Herstellern wie Huawei gibt.

**Siemens und andere europäische Firmen nutzen schon günstige chinesische KI, lässt sich das unterbinden?**

Sie nutzen offene chinesische Modelle mit „offenen Gewichten“, bei denen also das erlernte „Wissen“ frei zugänglich ist. Hoffentlich hosten sie das lokal. Aber sie legen sich nicht langfristig fest und können schnell das Modell verändern. Bisher verdienen chinesische Anbieter eher indirekt an ihren KI-Modellen. Die Frage ist, was passiert, wenn sie auch mit den Modellen selbst Geld machen wollen. Alibaba bietet seine aktuellste KI schon nicht mehr mit offenen Gewichten an

„WAS WIR GERADE ZU DIGITALER SOUVERÄNITÄT DISKUTIEREN, IST ZU BEGRÜSSEN.“

**Was wäre die Gefahr bei der Nutzung chinesischer Modelle, was könnte passieren?**

Die Modelle sind schon jetzt so unkontrollierbar, dass es sehr schwierig ist, sicherzustellen, dass sie in allen Situationen das machen, was man möchte. Die Firma, die das Modell trainiert, könnte einen Spionage-Bot einbauen, und aufgrund der Unberechenbarkeit von KI-Modellen wäre das sehr schwer zu erkennen.







Dazu kommt die langfristige Abhängigkeit: Wenn es zu einem plötzlichen Modellwechsel kommt, etwa weg von offenen Gewichten, kann das Firmen Probleme bereiten. Oder wenn die KI sich signifikant verbessert, Peking diese Fähigkeiten jedoch im Land behalten will.

„DAS VERTRAUEN IST SO GERING“

**Sie sagten, im Zweifel würde sich China vielleicht nicht an eine Regulierung der fortschrittlichsten Modelle halten. Ist eine internationale Lösung dann überhaupt möglich?**

Aktuell wäre meines Erachtens eine internationale Regulierung, die unabhängig überprüft wird, die einzige Option. Das Vertrauen ist so gering, vor allem zwischen China und den USA, aber auch zwischen Europa und China. Die Einhaltung von Regeln für Atomwaffen ist relativ einfach zu prüfen, da die Anlagen identifiziert werden können. Bei KI ist das viel schwieriger. Die großen amerikanischen Firmen erlauben nicht einmal der eigenen Regierung, die Modelle auf Herz und Nieren zu prüfen.

**Auch UN-Generalsekretär António Guterres trat in Shanghai auf – und lobte China überschwänglich. Was hat das zu bedeuten?**

Die USA haben sich stark zurückgezogen aus den UN. Allein deshalb ist Chinas Rolle dort wichtiger geworden. Ich denke aber nicht, dass daraus etwas Großes entsteht. Die UN kämpfen derzeit mit vielen Problemen, es werden kaum Entscheidungen getroffen. Gleichzeitig war China bisher wenig erfolgreich mit den eigenen internationalen Organisationen, die es gegründet hat.

**Wer macht mit bei Waico? Lässt sich ein Muster erkennen?**

Es sind vor allem Länder, die schon jetzt technologisch mit China zusammenarbeiten. Malaysia zum Beispiel. Dazu Schwellen- und Entwicklungsländer, die sich sorgen, dass sie über den Preis oder durch die US-Politik von den positiven Effekten der künstlichen Intelligenz ausgeschlossen werden.

**Lässt sich aus der Entwicklung denn auch etwas Gutes herauslesen, etwa für Europa?**

Was wir gerade zu digitaler Souveränität diskutieren, ist zu begrüßen. Die Gesetzesentwürfe, etwa zum Chips Act 2.0 und zum Cloud and AI Development Act, zwei Gesetzesentwürfe für die Förderung europäischer Technologie in diesem Bereich, sind auch viel schneller gekommen als erwartet. Da ist ein neuer Druck zu beobachten. Positiv ist auch, dass die EU über neue Instrumente zum Schutz und der Diversifizierung des Handels nachdenkt. Ich glaube, dass es noch nicht zu spät ist, wenn wir sie tatsächlich anwenden. Deutschland als größte Volkswirtschaft spielt dafür eine herausragende Rolle. Insgesamt gilt: Die EU hat in akuten Krisen ihre Handlungsfähigkeit unter Beweis gestellt. Was die Reaktion auf langfristige Entwicklungen anbelangt, gibt es aber Aufholbedarf.

ERSCHIENEN IN DER SZ VOM 28.07.2026

# „Es ist nicht einfach, aber wir sollten es tun“

Der Italiener Lorenzo Masia leitet das Münchner Institut für Robotik und Maschinen-intelligenz. Für ihn ist klar: Forschung und Industrie müssen viel enger zusammen-arbeiten, auch um Europas Souveränität zu stärken.

Von
Helmut Martin-Jung

Wenn es der Kaffee, den er servieren lässt, nicht schon verraten hätte – ein kurzer, aber starker Espresso –, wäre es der Akzent gewesen, der Lorenzo Masia als Italiener ausweist. Seit dem Frühjahr führt der gebürtige Römer das Munich Institute of Robotics and Machine Intelligence, kurz Mirmi. Er hat das Erbe von Sami Haddadin angetreten, den man einst an die TU München (TUM) geholt hatte.

Obwohl: Erbe, das wird im Gespräch schnell deutlich, ist womöglich nicht der richtige Ausdruck. Masia, 48, will gestalten, will Dinge verändern. Etwa das Verhältnis zwischen Forschung und Industrie. „Wenn ein Unternehmen eine neue Produktionslinie aufbauen will und dafür ein KI-Grundlagenmodell braucht, könnten wir das machen – das hat dann natürlich seinen Preis“, sagt er. Regulatorisch sei das „nicht einfach, aber wir sollten es tun“.

Masia stimmt auch dem Präsidenten der TU München, Thomas Hofmann, zu, der vor einigen Wochen in einem Interview gefordert hatte, Forschung sollte stärker militärisch genutzt werden. „Ich habe ja zwei Jahre am Massachusetts Institute of Technology in Boston gearbeitet, dem MIT“, sagt Masia, „da wird der Großteil der Forschung vom Militär finanziert.“ Die sogenannte Dual-Use-Strategie müsse daher überarbeitet werden.

Dual Use bezeichnet Entwicklungen, die sowohl zivil als auch militärisch genutzt werden können. „Wir produzieren keine Waffen, aber wir forschen an Dingen wie Prothesen und Exoskeletten, die auch von Veteranen mit Kriegsverletzungen genutzt werden können.“ Das Institut solle keine Angriffswaffen entwickeln, man sei ja nicht im Krieg und werde es hoffentlich auch nicht sein. Falls aber der Fall eintrete, „muss man neu überlegen. Dann kann die Wissenschaft eine entscheidende Rolle spielen“.

Ein wichtiges Anliegen ist Masia die technologische Souveränität. Es gebe derzeit zwei große Blöcke: die USA, die technologisch führend sind, und Asien. „Europas Problem ist, dass die Firmen oft isoliert arbeiten, nicht zentralisiert sind.“ Die Universitäten sollten Möglichkeiten zur Bildung einer Intelligenzia schaffen, die in diesem Sinne arbeitet.

Eine offene Flanke zeigt Europa derzeit bei der Abwehr von Drohnen – das ist ebenfalls eine Technologie, mit der sich die Münchner Robotik-Experten befassen. „Es gibt schon gute Firmen in diesem Bereich“, sagt Masia, „aber wenn es um Massenproduktion geht, um große Investitionen, da sind die USA und China erheblich weiter.“ Aber Europa werde eine Antwort finden, da sei er sehr sicher, daran werde schon gearbeitet, das werde nicht mehr jahrelang dauern.

EUROPA ZEIGT BEI DER DROHNENABWEHR DERZEIT EINE OFFENE FLANKE

Masias Spezialgebiet ist allerdings Technologie, die Menschen mit körperlichen Einschränkungen oder Älteren hilft, im Alltag zurechtzukommen. Dinge wie Exoskelette und Exoanzüge, an denen an seinem Lehrstuhl geforscht wird, können aber auch Beschäftigten in der Industrie körperlich anstrengende Tätigkeiten erleichtern. In Deutschland wird diese Technologie bis dato hauptsächlich in Kliniken eingesetzt, zum Beispiel nach Schlaganfällen. Damit könnten Patienten länger trainieren als ohne die technische Unterstützung und so Bewegungsabläufe schneller wieder erlernen. Man kooperiere dazu mit der medizinischen Fakultät der TUM. „Wir denken aber auch darüber nach, in den Bereich Wellness zu expandieren.“

Viel von dieser Arbeit findet im Geriatronik-Zentrum in Garmisch-Partenkirchen statt. Geriatronik steht für Technik, die älteren Menschen unter anderem dabei helfen soll, länger in der gewohnten Umgebung zu wohnen. Der Assistenzroboter „Garmi“ ist dabei das wichtigste Projekt. Erst kürzlich sind die Forscher in ein neues Gebäude gezogen, das mehr Platz bietet als das alte Haus im Stadtzentrum. Die ursprünglichen Pläne für einen Neubau liegen zwar derzeit wegen Finanzierungsproblemen auf Eis. Dennoch geht es voran: Insgesamt sechs neue Stellen für Professoren sollen besetzt werden.

SPÜRT ER DRUCK, FORSCHUNG IN PRODUKTE UMZUSETZEN?

Wie viel Druck spürt einer wie er, Forschung in Produkte umzusetzen? „Ganz ehrlich, als Professor gar keinen.“ Er habe in Heidelberg auch ein Start-up gegründet, das Exoskelette für Schlaganfall-Rehabilitation entwickelt. „Aber man muss sich entscheiden, ob man Tennis- oder Fußballprofi sein will.“ Er spiele Tennis, sei Wissenschaftler. „Aber wenn jemand aus meiner Gruppe, aus dem Labor ein Start-up gründen will – volle Unterstützung.“ Andere Professoren sähen es als natürlichen Weg an, ihre Forschung in einem Unternehmen zu kommerzialisieren. Für ihn in seiner Rolle als geschäftsführender Direktor von Mirmi und Professor wäre die Belastung zu groß, sagt er.

An Arbeit für ihn mangelt es ja wirklich nicht. „Wir sind eine führende Uni, diese Position will ich halten.“ Vernetztes Lernen und künstliche Intelligenz sollen noch ausgebaut werden. In seinem ersten Jahr in München habe er den Bereich KI konsolidiert. Die KI-Fabrik, bisher im Deutschen Museum angesiedelt, soll mittelfristig ins Siemens-Technologiezentrum in Garching im Norden von München ziehen, wo auch Masias Büro ist.

Dort, in dem weitläufigen Gelände am nördlichen Stadtrand von München, findet sie bereits statt, die Zusammenarbeit zwischen Forschung und Industrie, von der Masia so überzeugt ist. „Firmen sollten uns als Forschungs- und Entwicklungspartner sehen.“ Es sei zwar gut, wenn die Forschung frei und transparent ist, aber „es braucht auch mehr Synergie zwischen Forschung und Industrie“. Darauf will er hinaus: auf eine Mixtur aus Forschung und Industrie, die den strategischen Zielen des Landes dient, so wie er das in seinen zwei Jahren am MIT erlebt hat. „Ich verstehe das als meine Pflicht.“



ERSCHIENEN IN DER SZ VOM 02.11.2026



## *„Wir müssen zurück zu einer Kultur des Machens“*

Martin Keller, Präsident der Helmholtz-Gemeinschaft, hat lange in den USA gelebt. Zurück in Deutschland ist er nun erstaunt: darüber, wie man hierzulande eigene Stärken verkennt und jedes Risiko meidet.

INTERVIEW VON ELISABETH DOSTERT

Martin Keller, 60, hat viele Jahrzehnte in den USA gelebt und zuletzt ein Forschungszentrum für erneuerbare Energien geleitet. Seit November ist er Präsident der Helmholtz-Gemeinschaft mit rund 48 000 Mitarbeitenden und 18 Forschungszentren. Zur Gemeinschaft gehören das Forschungszentrum Jülich, das Deutsche Krebsforschungszentrum und das Karlsruher Institut für Technologie. Es sei schon eine Umstellung gewesen, wieder in Deutschland zu leben, sagt Keller. „Es dauert hier alles länger, manches ist komplizierter." Was das für Wirtschaft und Forschung bedeutet? Zeit für ein Gespräch, kurz bevor sich die führende Industrie Ende April auf der Hannover-Messe trifft.

**SZ: Herr Keller, Sie haben drei Jahrzehnte in den USA gelebt. Seit November 2025 sind Sie Präsident der Helmholtz-Gemeinschaft. Sind Sie vor Donald Trump geflohen?**

*Martin Keller:* Nein. Meine Entscheidung fiel schon vor seiner Wahl. Nach der Wahl wäre es mir schwerer gefallen, die USA zu verlassen, aus Loyalität zu meinen Kollegen und Kolleginnen. Bis November 2025 habe ich zehn Jahre lang das nationale US-Forschungszentrum für erneuerbare Energien in Golden im Bundesstaat Colorado geleitet, das National Renewable Energy Laboratory, das NREL. In Trumps erster Amtszeit haben wir uns ganz gut geschlagen und waren sehr erfolgreich, wir waren eines der weltweit führenden Institute für erneuerbare Energien. Jetzt ist es noch mal schwieriger geworden. Trump mag die Erneuerbaren nicht. Auch das Institut ist mittlerweile umbenannt in National Laboratory of the Rockies.

**Am NREL arbeiten Menschen aus vielen Nationen. Die Einwanderungsbehörde ICE geht rigoros gegen Migranten vor, blieb Ihr Institut davon verschont?**

Nein. Das NREL hat viele Mitarbeiter aus dem asiatischen Raum. Ein Kollege aus Indien wurde von ICE-Leuten aufgegriffen. Er hatte keine Papiere dabei, weil er sie für seine Green Card, sein unbefristetes Arbeitsvisum, eingereicht hatte. Er blieb einen halben Tag verschwunden, niemand wusste, wo er war. Er kam dann in mein Büro und sagte: „Martin, ich halte es hier nicht mehr aus." Als meine Frau und ich die USA verlassen haben, fragten viele, ob sie nicht mitkommen können. Die Einwanderungspolitik von Trump ist für Deutschland eine Chance, Top-Leute für die Forschung zu gewinnen.

**Seit ein paar Monaten führen Sie die Helmholtz-Gemeinschaft. Kommen Sie sich manchmal wie ein Entwicklungshelfer vor?**

Nein, nein, nein. Aber es ist schon eine große Umstellung. Deutschland ist anders. Es dauert hier alles länger, manches ist komplizierter. Es gibt viele Meetings, da wird viel geredet, aber wenig umgesetzt. Aber wir brauchen uns in Deutschland nicht zu verstecken. Wir müssen gewisse Sachen besser machen. Wenn wir gewisse Sachen nicht anpacken, wird Deutschland noch mehr Schwierigkeiten bekommen, und zwar ganz schnell.

**Was meinen Sie denn konkret?**

In Deutschland fehlt die Aufbruchstimmung, bestimmte Dinge anzugehen, zum Beispiel die Entbürokratisierung. Wir müssen in die Gänge kommen, wir müssen zurück zu einer Kultur des Machens. Das wird nicht einfach. Das war auch ein Anreiz für mich, nach Deutschland zurückzukommen. Es gibt Sachen, die laufen hier wirklich gut, und Sachen, die wirklich nervig sind.

**Was läuft in Deutschland denn gut?**

Das deutsche Forschungssystem hat große Stärken. Die Förderung ist langfristig angelegt, das macht Projekte planbar. Aber das reicht nicht. In Deutschland dauert immer alles super lang. Die Forschung in den USA kommt schneller zu Ergebnissen, weil die Institute schon früh mit der Industrie im Rahmen von öffentlich-privaten Partnerschaften zusammenarbeiten. Das NREL hat über solche Projekte mit Unternehmen wie Exxon Mobil, Shell oder HP zuletzt 170 Millionen Dollar eingeholt. Und das ist keine Auftragsforschung im Dienste der Konzerne. So sollte auch die Hightech-Agenda der Bundesregierung umgesetzt werden.

**Wo sind denn die USA besonders flott?**

Bei künstlicher Intelligenz.

**Es gibt Leute, die sagen, die deutsche Forschung ist so gut, weil sie unabhängig von Konzernen ist.**

Forschung muss frei sein. Die Gefahr besteht ja schon, dass Donald Trump sagt, es gibt jetzt kein Geld mehr für Solarenergie. So was darf in Deutschland nicht passieren, da müssen wir aufpassen. Aber das ist kein Grund, nicht mit der Industrie zusammenzuarbeiten, Wissenschaft wird über Steuergeld finanziert. Wenn Wissenschaftler mit Firmen kooperieren wollen, sollten sie das tun. Es ist auch nicht verwerflich, wenn jemand eine Firma gründet. Das sollte man feiern. Wissenschaftlerinnen und Wissenschaftler haben auch gute Ideen.

„DAS PRINZIP DER FREIEN MARKTWIRTSCHAFT IN DEMOKRATISCHEN SYSTEMEN FUNKTIONIERT NICHT, WENN NICHT ALLE FAIR SPIELEN, UND DAS TUN SIE JA NICHT."

**Und wenn die Start-ups dann richtig viel Geld brauchen, holen sie es sich bei US-Investoren oder ziehen gleich ganz in die USA.**

Das ist oft so. Das Misstrauen steckt schon im Wort. Geld für junge Unternehmen heißt in Deutschland Risikokapital. In der Start-up-Mentalität können wir in Deutschland besser werden. Wenn jemand in den USA eine Firma gegründet hat und pleitegeht, wird er dafür gelobt, dass er es versucht hat. Wenn ein Gründer in Deutschland pleitegeht, ist das ein Makel.

**Diese Geschichte erzählt man sich auch schon seit Jahrzehnten.**

Das stimmt. Was mich in Deutschland wirklich beunruhigt, ist dieses Streben nach finanzieller Sicherheit. Die Leute wollen kein Risiko eingehen. Nach der Promotion wollen sie am liebsten eine feste Stelle. Und umziehen für einen Job wollen manche lieber auch nicht. Da denken Amerikaner ganz anders. Meine Kinder auch. Eine meiner Töchter ist für einen Job von den USA nach Deutschland gezogen, mein Sohn arbeitet in Australien. Mit der Mentalität, im Leben möglichst wenige Risiken einzugehen, wird es Deutschland nicht schaffen.

**Wie wollen Sie das ändern?**

In kleinen Schritten. Für die Forschung, beispielsweise, ist eine stabile Förderung wichtig. Darauf müssen wir aber aufsetzen und schneller werden nach dem Darpa-Prinzip.

**Darpa wie die Forschungseinrichtung des US-Verteidigungsministeriums?**

Ja. Wir müssen Hochrisikofelder identifizieren, Prioritäten setzen und Meilensteine definieren. Da müssen wir zwei, drei Jahre mit aller Kraft darauf hinarbeiten – Forschung und Industrie gemeinsam. Wenn es dann nicht funktioniert, muss man auch den Mut haben, ein Projekt aufzugeben und die Mittel umzuschichten. Stop-and-go. Forschung dient dazu, die Wettbewerbsfähigkeit europäischer Firmen zu stärken.

**Was kann Deutschland denn noch wirklich gut?**

Bei Klimatechnologien beispielsweise spielt Deutschland vorne mit, etwa in der Geothermie. Wir

sind gut in Grid-Technologien, also in der Vernetzung von Energiesystemen. Zum Beispiel erforschen wir am Helmholtz-Zentrum in Berlin neue Materialien für Solarzellen mit deutlich höherer Leistung, das interessiert Trump nicht. Wir sind Vorreiter in Fusionstechnologien für die Energieversorgung. Aber wir müssen aufpassen, sonst passiert uns das Gleiche wie in der Solarindustrie, die fast komplett in China angesiedelt ist. Die haben die Wertschöpfungskette vollständig integriert von den Rohstoffen für die Solarzellen bis zu den Paneelen. Wir müssen aufpassen, dass uns das nicht auch bei Batterien und Elektrolyseuren passiert. Das ist ja auch das, was Trump will, vollständig integrierte Wertschöpfungsketten im eigenen Einflussgebiet.

„ICH WAR SEHR ENTTÄUSCHT, WIE SCHNELL SICH DIE TECH-GIGANTEN DONALD TRUMP UNTERWORFEN HABEN.“

**Geben Sie Trump jetzt gerade recht?**

Ich halte nichts von „America First“. Die Welt ist total vernetzt, man kann nicht alles in den USA machen. Das funktioniert nicht, auch nicht mit Strafzöllen. Wir müssen Partnerschaften mit Ländern schließen, die demokratische Werte teilen. Die Diskussion um sichere Lieferketten ist richtig. Für bestimmte Produkte, zum Beispiel Seltene Erden, braucht es staatliche Garantien für Abnahmemenge und Preise. Firmen brauchen für eine gewisse Zeit einen sicheren Markt. Das Prinzip der freien Marktwirtschaft in demokratischen Systemen funktioniert nicht, wenn nicht alle fair spielen, und das tun sie ja nicht. Wenn ein Staat alle Preise unterbietet und Wettbewerber aus dem Markt drängt, wie in der Solarindustrie geschehen, ist das nicht fair. Wir brauchen starke Partnerschaften, auch in der Forschung, sonst begeben wir uns schnell in Abhängigkeit von ein oder zwei Ländern. Das dürfen wir nicht erlauben. Die Forschung steht ganz am Anfang der Wertschöpfungskette.

**Es wird auch viel über digitale Souveränität gesprochen. Wie souverän ist Deutschland?**

Da muss ich jetzt etwas ausholen. Wissenschaftler wollen ja Erkenntnisse der Welt zur Verfügung stellen, etwa durch Publikationen und Patente. Da sind sie wie Künstler, die wollen auch, dass ihre Werke gesehen werden. Wissenschaftler erzeugen Wissen nicht um des Wissens willen, sie wollen das Wissen den Leuten vermitteln. Und sie erzeugen Daten, die sie natürlich der Welt zur Verfügung stellen. So lief das bislang.

**Und jetzt?**

Selbst Daten von Messungen, die negativ waren, sind mittlerweile wichtig, weil sie in die neuen Language-Modelle einfließen und die KI-Modelle verbessern. Es gibt gewisse Länder, die greifen alle Daten ab mit offiziellen und inoffiziellen Methoden. In Deutschland gibt es jede Menge sehr guter Datensätze, die über Jahrzehnte gesammelt wurden, zum Beispiel Umweltdaten oder Daten aus dem Bereich der Materialwissenschaft. Daher stellt sich die Frage: Ist unser bisheriger Ansatz, Datensätze komplett zu veröffentlichen, der richtige Weg?

**Was denken Sie?**

Ich denke, wir sollten je nach Art des Datensatzes handeln. Die Helmholtz-Gemeinschaft verfügt beispielsweise über Daten für ein Tsunami-Frühwarnsystem. Solche Daten müssen wir natürlich sofort veröffentlichen, denn da hilft es ja nicht, wenn wir drei Wochen warten. Aber sollten wir in allen Forschungsbereichen sämtliche Daten sofort veröffentlichen? Wahrscheinlich nicht, es gibt ja auch Sicherheitsaspekte. KI wird die Erforschung neuer Materialien und Moleküle komplett verändern. Autonome Labore, die KI und Robotik verbinden, werden eigenständig Experimente durchführen und Vorschläge liefern und dann die Materialien synthetisieren. Das sehen wir schon jetzt. Wir müssen uns gut überlegen, welche Daten wir wann mit wem teilen.

**Bitte konkreter. Welche Daten sollten wir auf keinen Fall teilen?**

Das lässt sich nicht pauschal beantworten und hängt immer vom Einzelfall ab. Aber zum Beispiel mit Daten über kritische Infrastrukturen oder mit Daten zur Entwicklung von Schlüsseltechnologien, wie Quanten- oder Chiptechnologien, sollten wir natürlich sehr verantwortungsvoll umgehen.

**Was muss geschehen?**

Wir brauchen KI-Basecamps, Basislager für die Entwicklung neuer Language-Models für bestimmte Industrien, Materialien, Umwelt und Medizin. Die Art und Weise, wie wir neue Medikamente entwickeln, wird sich völlig verändern. Die KI stellt alles auf den Kopf. Trump will solche Modelle mit den Techkonzernen entwickeln. Die Frage ist, trauen wir denen? Geben wir denen unsere Daten, um ihre Sprachmodelle zu trainieren, und bekommen wir dafür etwas zurück und zu welchen Konditionen? Vor fünf Jahren hätte ich gesagt, ganz klar, wir müssen mit Hyperscalern wie Google, Amazon und Microsoft zusammenarbeiten, wir haben keine andere Wahl.

**Und heute?**

Wir müssen in Europa gemeinsam unsere eigenen KI-Modelle bauen. Wir haben einen Super-Satz an Daten. Warum machen wir keine KI in Deutschland? Das ist wirklich kritisch. Wenn wir das nicht tun, werden wir es bereuen. Das ist ein No-Brainer.

**Sind die US-Hyperscaler eine Gefahr für Europa?**

Ich weiß es nicht. Wir wissen nicht, wie das Geschäftsmodell der Amerikaner am Ende aussehen wird. Meine alten Kollegen versichern mir immer, dass das alles open source, also öffentlich zugänglich sein wird. Wenn das der Fall ist, würde ich sagen, schließen wir uns mit denen zusammen. Aber ich bin mir nicht sicher, ob es der Fall sein wird. Mein altes Institut hat gut mit Microsoft und Google zusammengearbeitet. Wenn Sie mich vor einigen Jahren gefragt hätten, hätte ich gesagt, wir müssen auf alle Fälle kooperieren mit den Amerikanern.

**Was lässt Sie nun zweifeln?**

Ich war sehr enttäuscht, wie schnell sich die Tech-Giganten Trump unterworfen haben. Das macht mir Angst. Ich dachte, die treten stärker für die Werte ein, die sie früher vertreten haben, zum Beispiel Diversität.

**Und warum tun sie es nicht?**

Ganz einfach. Vier Buchstaben. Es geht nur ums Geld.

ERSCHIENEN IN DER SZ VOM 19.04.2026

# IMPRESSUM

*Süddeutsche Zeitung Langstrecke*

VERLAG
Süddeutsche Zeitung GmbH
Hultschiner Straße 8
81677 München

Dies ist eine Anzeigensonderveröffentlichung der Süddeutschen Zeitung GmbH in Kooperation mit Telekom Deutschland. Die Süddeutsche Zeitung ist weder für den Inhalt der Anzeige noch für ggf. angegebene Produkte verantwortlich.

Danke an das Team von SZ Institut.

**REDAKTION UND KOORDINATION**
Dirk von Gehlen, *Michael Neißendorfer**, Andreas Freitag

**GRAFIK**
*Erica Lefstad und Carina Müller (studio MLLR)*

**ILLUSTRATIONEN**
*Erica Lefstad und Carina Müller (studio MLLR)*

**PROJEKTKOORDINATION TELEKOM**
*Tatjana Geierhaas*

**DRUCK**
novaconcept schorsch GmbH,
95326 Kulmbach

** freie/r Mitarbeiter/in*

MEHR ZUR LANGSTRECKE UNTER
*sz.de/langstrecke*

SONDERAUSGABE IN ZUSAMMENARBEIT
MIT TELEKOM



Bestellen Sie alle seit 2015
erschienenen Ausgaben der *SZ Langstrecke*
**› sz.de/langstrecke**

Süddeutsche Zeitung
LANGSTRECKE

JETZT
abonnieren


TRUST
THE T
Souveräne Cloud, AI
und Security-Lösungen
für jedes Business.
Für mehr Infos
hier scannen.
AI