SWP-Aktuell
NR. 48 NOVEMBER 2025

Europas Cybersicherheit hängt an den USA

Wie europäische Regierungen mehr Verantwortung übernehmen können

Alexandra Paulus

Die Cybersicherheit von Politik, Wirtschaft und Gesellschaft in Europa ist stark abhängig von den Vereinigten Staaten. Konkret dominieren US-amerikanische Unternehmen den weltweiten Markt für Cybersicherheits-Anwendungen ebenso wie für Informationen über entsprechende Bedrohungen. Bei der Gewinnung von Letzteren spielt auch das Militär des Landes eine Rolle. Außerdem leistet die Regierung in Washington finanzielle Unterstützung für Schwachstellen-Datenbanken und das Open-Source-Ökosystem. Was zunächst nach technischen Einzelaspekten klingt, bedeutet in der Summe, dass Europas Handlungsfähigkeit in diesem Bereich begrenzt ist und es auch mit einem eigenen »EuroStack« noch bliebe. Diese Abhängigkeiten können in verschiedenen Situationen zum Problem werden – wenn die US-Regierung ihre finanzielle Unterstützung für Cybersicherheit beendet, wenn sie ihre politischen Prioritäten ändert oder in einem Konflikt mit Europa die Dependenz offen als Waffe einsetzt. Deutsche und europäische Entscheidungsträger:innen sollten jetzt gezielt Maßnahmen ergreifen, um die Abhängigkeiten zu reduzieren und so die Cybersicherheit in Europa langfristig zu schützen.

Wirtschaft und Gesellschaft in Deutschland wie Europa sind so stark digitalisiert, dass Cybersicherheit eine Grundvoraussetzung für funktionierende Demokratien und gedeihende Ökonomien ist. Angesichts der aktuellen Spannungen im transatlantischen Verhältnis tritt dabei ein Aspekt in den Vordergrund, der bisher kaum berücksichtigt wurde: Das globale Cybersicherheits-Ökosystem ist in hohem Maße von den USA abhängig. Dieses Ökosystem umfasst Personen, Unternehmen und Nichtregierungsorganisationen, die einen Beitrag dazu leisten, dass sichere Software entwickelt, Systeme und Geräte vor Bedrohungen geschützt, bekannt gewordene Software-Schwachstellen geschlossen und Informationen über individuelle Bedrohungsakteur:innen gesammelt und geteilt werden. Die Abhängigkeit besteht dabei von Unternehmen mit Sitz in den Vereinigten Staaten oder direkt von der Regierung in Washington. Hervorzuheben ist, dass sich immer mehr US-amerikanische Technologiefirmen der Administration von Präsident Donald Trump stark annähern, was Bedenken über eine mögli-

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

che Unzuverlässigkeit für Europa nährt. Vorstellbar ist auch, dass eine solche wirtschaftliche Dependenz in Zukunft politisch instrumentalisiert werden könnte.

Europas Abhängigkeiten von den USA im Bereich Cybersicherheit sind dabei grundlegender Natur und betreffen nicht nur einzelne Aspekte, die aktuell die öffentliche Debatte dominieren. Viel Aufmerksamkeit erhält zurzeit vor allem die Abhängigkeit von Cloud-Diensten, Software-as-a-Service-Diensten wie Microsoft 365 oder Sicherheitsupdates für Software-Produkte. Die Sorge ist, dass US-Stellen entsprechende Updates zurückhalten oder den Zugang zu den genannten Diensten unterbrechen könnten. In diesem Zusammenhang wird häufig die Forderung laut, Europa müsse seinen eigenen »Tech-Stack« entwickeln — also ein Set wichtiger Hardware- und Software-Produkte wie Betriebssysteme und Anwendungen.

Doch selbst wenn es gelänge, einen solchen »EuroStack« zu entwickeln, blieben viele Informationen, Prozesse und Märkte im Bereich Cybersicherheit weiterhin US-dominiert, wie im Folgenden ausgeführt wird. Diese Abhängigkeiten werden zum Problem, wenn die Regierung in Washington sie gezielt ausnutzt oder politische Entscheidungen in den USA schmerzhafte Konsequenzen für Europa haben.

Die Abhängigkeit des Cybersicherheits-Ökosystems von den USA

Sowohl US-Unternehmen als auch die US-Regierung nehmen eine zentrale Rolle im globalen Cybersicherheits-Ökosystem ein. Fünf Aspekte sind hier besonders bedeutsam.

US-Unternehmen beherrschen den Markt für Cybersicherheits-Anwendungen. Zunächst beherrschen Unternehmen aus den Vereinigten Staaten den europäischen Markt für Cybersicherheits-Software, der für die Cybersicherheit von Gesellschaft und Wirtschaft besonders wichtig ist. Zu den betreffenden Anwendungen zählen etwa:

- Anti-Viren-Software, die bekannte Schadsoftware blockiert,
- »firewalls«, die unerwünschten Netzwerkverkehr abwehren,
- »Endpoint Detection and Response« (EDR)-Anwendungen, die Endgeräte (wie Computer oder Mobiltelefone) beobachten, um ungewöhnliches Verhalten festzustellen, oder
- »Security Information and Event Management« (SIEM)-Systeme, die Informationen über Vorfälle im gesamten Netzwerk einer Organisation zusammenführen.

Europäische Anwender:innen dieser Produkte nutzen vor allem solche von US-Unternehmen wie Broadcom, Cloudflare, IBM und Microsoft. Zwar gibt es auch Anbieter außerhalb der Vereinigten Staaten, die solche Anwendungen zur Verfügung stellen. Ein Wechsel wäre allerdings mit hohem Aufwand verbunden.

US-Unternehmen dominieren den Markt für Informationen über Cybersicherheits-Bedrohungen. Um eigene Systeme und Geräte vor Cybersicherheits-Bedrohungen zu schützen, benötigt IT-Fachpersonal neben entsprechenden Anwendungen und den unten beschriebenen Informationen über Schwachstellen auch Informationen über aktuelle und potentielle Bedrohungen (sogenannte Cyber Threat Intelligence, kurz CTI). Denn CTI erlaubt es, die aktuelle Risikolage zu beurteilen und Entscheidungen über Schutzmaßnahmen zu treffen.

Auch der Markt für CTI wird von US-amerikanischen Unternehmen beherrscht, darunter CrowdStrike, IBM, Google (Mandiant) und Recorded Future. Große Firmen, die auch andere Cybersicherheits-Produkte anbieten — besonders solche, die Daten über Vorfälle sammeln, wie EDR oder SIEM — können leichter CTI bereitstellen. Entsprechend bevorteilt der Markt vertikal integrierte Unternehmen, die verschiedene Produkte entlang der Wertschöpfungskette in ihrem Portfolio haben. Zwar gibt es CTI-Anbieter außerhalb der USA, doch diese haben nur kleine Marktanteile oder dürften, wie im Fall des russischen Unternehmens Kaspersky, aus politischen Gründen für europäische Anwender:innen nicht in Frage kommen.

Ohne die CTI der führenden US-Unternehmen würde somit europäisches IT-Fachpersonal den Zugriff auf Informationen über besonders fortgeschrittene Bedrohungsakteur:innen verlieren. Damit entfiele die Datengrundlage, um Ressourcen für Cybersicherheit gezielt einzusetzen.

US-Streitkräfte sammeln Erkenntnisse über Cyberbedrohungen. Neben Unternehmen generiert auch das Militär der Vereinigten Staaten CTI. Konkret führt das US Cyber Command sogenannte »hunt forward«-Operationen durch, bei denen Angehörige des US-Militärs auf Einladung eines Partnerstaats in dessen Netzen nach Bedrohungen suchen.

Europäische Staaten profitieren in verschiedener Weise von diesen Erkenntnissen. Erstens dann, wenn das Cyber Command unmittelbar gegen gegnerische Infrastruktur vorgeht oder US-Anbieter von Cybersicherheits-Anwendungen ihre Produkte auf Basis der betreffenden Informationen verbessern. Zweitens haben sich bisherige »hunt forward«-Operationen auf Europa konzentriert, vor allem das Baltikum und Südosteuropa, und so europäischen Staaten auf direktem Wege wertvolle CTI verschafft. Drittens hat das US-Militär die erhaltenen Informationen stellenweise mit weiteren europäischen Verbündeten geteilt und einige davon veröffentlicht. Es ist anzunehmen, dass die so gesammelten Erkenntnisse eine Informationsquelle für die Verteidigung europäischer Staaten darstellen.

Die US-Regierung finanziert Schwachstellen-Datenbanken. Aufgrund der schieren Anzahl an Software-Produkten und der in ihnen entdeckten Schwachstellen ist es wichtig, dass dasselbe Problem nicht mehrfach erfasst wird und alle Instanzen, die an der Behebung von Schwachstellen beteiligt sind, sich leicht verständigen können. Dafür braucht es ein weltweit einheitliches System zur Identifikation und Benennung von Schwachstellen. Diese Funktion übernimmt die Common Vulnerabilities and Exposures (CVE)-Datenbank.

Sie wird von der gemeinnützigen US-Organisation MITRE betrieben, die wiederum von der Cybersecurity and Infrastructure Security Agency (CISA) finanziert wird, der im Geschäftsbereich des Washingtoner Heimatschutzministeriums liegenden nationalen Cybersicherheits-Behörde. Wenn eine Schwachstelle entdeckt wird, wird geprüft, ob sie bisher unbekannt ist. Falls ja, wird dafür eine neue CVE-Nummer vergeben. Wenn der Hersteller ein Software-Update oder eine andere Abhilfemaßnahme entwickelt hat, veröffentlicht er einen Sicherheitshinweis (security advisory), in dem er sich auf die CVE-Nummer bezieht.

Auf Basis der CVE-Datenbank betreibt die US-amerikanische Standardisierungsbehörde National Institute of Standards and Technology (NIST), die zum Geschäftsbereich des Handelsministeriums gehört, die National Vulnerability Database (NVD). Diese Datenbank verwendet die CVE-Nummern als Grundlage und reichert sie um weitere Informationen an, etwa zur Kritikalität oder zur Grundursache der Schwachstelle. Viele Cybersicherheits-Anwendungen beziehen die maschinenlesbaren NVD-Daten und verteilen sie automatisiert an Endnutzer:innen weiter.

Ohne die CVE-Datenbank würde sich das Schließen von Software-Schwachstellen weltweit mutmaßlich verzögern. Bedrohungsakteur:innen könnten dies ausnutzen und mehr Cyberangriffe durchführen. Automatisierte Werkzeuge liefen weniger zuverlässig und würden fehlerhafte Meldungen produzieren. Ohne die NVD-Informationen würden zahlreiche Cybersicherheits-Anwendungen ihre Datengrundlage verlieren und Cybersicherheits-Teams automatisierte Arbeitsabläufe einbüßen.

Die US-Regierung unterstützt die Sicherheit von Open-Source-Software. Open-Source-Software (OSS) bildet das Fundament des modernen Software-Ökosystems. Die große Mehrheit aller Software-Anwendungen enthält OSS-Komponenten. Wenn ein Software-Produkt eine Komponente verwendet, die wiederum eine Schwachstelle enthält, ist die Chance hoch, dass Letztere auch

bei den Endnutzer:innen des Produkts zum Problem werden kann. Somit ist die Sicherheit kritischer OSS-Komponenten entscheidend für die Sicherheit darauf basierender (offener oder proprietärer) Software-Anwendungen.

Einige dieser vielgenutzten Komponenten werden von Einzelpersonen in ihrer Freizeit gepflegt, entsprechend sind ihre Ressourcen für IT-Sicherheit begrenzt. Die US-Regierung füllt teilweise diese Fähigkeitslücke, indem sie die Absicherung von wichtigen OSS-Projekten finanziell fördert. Mittel kommen dabei von der interministeriellen Open-Source Software Security Initiative (OS3I), von CISA, der National Science Foundation (NSF, die Grundlagenforschung unterstützt), und der militärischen Forschungsagentur DARPA. Die Regierung in Washington leistet so einen bedeutenden Beitrag zur Absicherung wichtiger OSS-Komponenten.

Cybersicherheits-Abhängigkeiten als Problem: Drei Szenarien

In der Summe ergibt sich ein Bild, in dem kritische Stellen des globalen Cybersicherheits-Ökosystems — Europa eingeschlossen — von den USA abhängig sind. Interdependenzen sind üblich in einer globalisierten Welt, doch mit Blick auf das aktuelle transatlantische Verhältnis sind drei Szenarien denkbar, in denen diese Abhängigkeiten zum Problem für Europa werden könnten. Bisher ist keines davon vollständig eingetreten, doch die US-Regierung hat bereits Entscheidungen getroffen, die in Richtung der ersten beiden Szenarien deuten.

Szenario 1: Washington beendet die finanzielle Unterstützung für Cybersicherheits-Projekte. Ein wahrscheinliches Szenario ist, dass die US-Regierung ihre Unterstützung für Cybersicherheits-Projekte beendet oder reduziert. Schließlich stehen unter der Trump-Administration und speziell durch das neugeschaffene Department of Government Efficiency (DOGE) alle staatlichen Ausgaben auf dem Prüfstand, und gerade CISA und die Cybersicherheits-Stellen des US-Außenministeriums haben schon spürbare Kürzungen erfahren.

Ohne die Unterstützung der US-Regierung würde es zahlreichen OSS-Projekten an Mitteln fehlen, die sie vor allem zur Absicherung ihrer Produkte und Komponenten einsetzen. Dies würde mittelbar auch alle proprietären Software-Produkte betreffen, die die jeweiligen OSS-Komponenten nutzen. Bereits im März 2025 ging die Trump-Administration einen ersten Schritt in diese Richtung, als sie dem Open Technology Fund (OTF) die Mittel entzog. Der OTF unterstützt diverse OSS-Projekte für sichere Kommunikation und Internetfreiheit, etwa die verschlüsselte Messenger-App Signal. Er ging gerichtlich gegen die Kürzung vor und bekam Recht, bislang ist jedoch unklar, ob die US-Regierung die Zahlungen wieder aufgenommen hat.

Ähnliches trug sich im Fall der CVE-Datenbank zu. Im April informierte MITRE darüber, dass Washington die finanzielle Unterstützung für den Betrieb der Schwachstellen-Datenbank kurzfristig einstellen werde und MITRE deren Betrieb daher nicht mehr gewährleisten könne. Wohl auch als Reaktion auf den globalen Aufschrei in der Cybersicherheits-Branche ruderte die Trump-Regierung am Folgetag zurück und verkündete, dass die Finanzierung weiterlaufen werde — allerdings nur für elf Monate und in begrenztem Umfang.

In beiden Fällen ist das Cybersicherheits-Ökosystem augenscheinlich noch einmal mit dem Schrecken davongekommen. Doch sollte die US-Regierung ihre finanzielle Unterstützung für Cybersicherheit zurückfahren, wären die Auswirkungen weltweit — und damit auch in Europa — zu spüren. Schwächere Sicherheitsmaßnahmen in OSS-Projekten und zudem ein enorm erhöhter Koordinationsaufwand beim Finden, Mitteilen und Schließen von Schwachstellen wären die Folge.

Szenario 2: Die US-Regierung ändert ihre politischen Prioritäten. Denkbar ist außerdem, dass die Führung in Washington ihre politischen Prioritäten ändert, indem sie

etwa einen noch stärkeren Fokus auf die Rivalität mit China legt. Eine Abkehr von Europa und ein Ressourcenabzug weg von russischen Bedrohungen wären womöglich die Folge.

Konkret könnten sich in einem solchen Fall die »hunt forward«-Operationen des Cyber Command von Europa hin zu Staaten im chinesischen Einflussbereich verlagern. Europa würde dann weniger Informationen über russische Cyberaktivitäten erhalten. Ähnliches könnte auch für kommerzielle CTI gelten, da viele Anbieter US-amerikanische Behörden zu ihrer Kundschaft zählen. Sollten diese keine Informationen über russische Cyberaktivitäten mehr nachfragen, würde das Angebot daran sinken — zum Leidwesen europäischer Staaten, die absehbar weiterhin Bedrohungsakteur:innen mit Verbindungen zur russischen organisierten Kriminalität und/oder dem russischen Staat ausgesetzt sein werden.

Im März 2025 sorgten Berichte für Aufregung, nach denen ein solches Szenario keine Zukunftsmusik mehr wäre. Wie es hieß, habe US-Verteidigungsminister Pete Hegseth das Cyber Command angewiesen, die Planung von Cyberoperationen gegen Russland auszusetzen. Zudem habe CISA seinem Personal aufgetragen, Informationen über russische Cyberbedrohungen nicht mehr zu verfolgen. Spätere Dementi beider Organisationen stellen die Richtigkeit dieser Berichte in Frage; nichtsdestotrotz haben die dadurch ausgelösten Diskussionen illustriert, wie leicht ein solcher Wechsel der politischen Prioritäten vollzogen werden könnte und welch tiefgreifende Auswirkungen er hätte.

Szenario 3: Die US-Regierung setzt die Abhängigkeiten gezielt gegen Europa ein. Im dritten Szenario setzt Washington die Abhängigkeiten Europas gezielt als Waffe gegen den Kontinent ein, etwa um Zugeständnisse auf anderen Politikfeldern wie der Sicherheits- und Verteidigungspolitik zu erzielen — oder im Rahmen einer fundamentalen Verschlechterung der transatlantischen Beziehungen. Dieses Szenario ist weniger wahrscheinlich als die beiden erstgenannten, im Lichte von Auseinandersetzungen der jüngeren Zeit allerdings denkbar.

In einem solchen Fall könnte Washington, zusätzlich zu den unter Szenario 2 genannten Punkten, die marktbeherrschende Stellung von US-amerikanischen Unternehmen für Cybersicherheits-Anwendungen ausnutzen. So ließen sich diese Sektoren etwa mit Ausfuhrbeschränkungen belegen, um Europas Zugriff auf entsprechende Produkte zu unterbrechen. In der Vergangenheit hatte die US-Regierung beispielsweise den Export von Verschlüsselungssoftware stark begrenzt, und im Oktober kündigte Präsident Trump Exportkontrollen für »kritische Software« gegenüber China an. Sollte dieses Instrument auch genutzt werden, um den Export von Cybersicherheits-Anwendungen nach Europa einzuschränken, müssten sich europäische Nutzer:innen kurzfristig umorientieren und blieben vorübergehend ungeschützt.

Mögliche Auswirkungen

Wenn Schwachstellen erst verzögert geschlossen würden, OSS-Projekte ihre Sicherheitsmaßnahmen reduzieren müssten, Cybersicherheits-Anwendungen ausfielen und Informationen über den Hauptbedrohungsakteur ausblieben, hätte dies tiefgreifende Auswirkungen für Europa. Angriffe wären leichter durchzuführen — ob durch Kriminelle oder etwa gegnerische Nachrichtendienste oder Streitkräfte.

Dies muss vor dem Hintergrund betrachtet werden, dass die Cybersicherheits-Lage in Deutschland seit Jahren angespannt ist und entsprechende Vorfälle zunehmen. Betroffen sind Privatpersonen ebenso wie große und kleine Wirtschaftsunternehmen, darunter kritische Infrastrukturen wie zuletzt Flughäfen. Und auch politische Institutionen und die Bundeswehr geraten regelmäßig ins Visier. So hat etwa Ransomware die Handlungsfähigkeit zahlreicher deutscher Kommunen bereits über Monate beeinträchtigt, und die öffentliche Verwaltung steht europaweit im Fokus von Angriffen. Zudem wurden eine Universität sowie

Zulieferer der Bundeswehr Ziel von Cyberoperationen für Spionagezwecke.

IT-Personal in ganz Europa ist auf die genannten Teile des globalen Cybersicherheits-Ökosystems angewiesen, um Organisationen und einzelne Endnutzer:innen vor entsprechenden Bedrohungen zu schützen. Wenn IT-Fachleute auf die genannten Dienste und Informationen keinen Zugriff mehr hätten bzw. immer mehr Sand ins Getriebe des Ökosystems geworfen würde, könnte das zu mehr erfolgreichen Cyberangriffen auf europäische Ziele führen. Entsprechend würde sich die Bedrohungslage wohl in allen drei Szenarien stark verschärfen.

Handlungsmöglichkeiten für die deutsche und europäische Politik

Entscheidungsträger:innen der europäischen Politik sollten die genannten Abhängigkeiten keineswegs als langfristig gegeben hinnehmen. Vielmehr kann sich Europa in vielen Fällen davon befreien, um für die drei skizzierten Szenarien gerüstet zu sein. Und auch wenn diese negativen Zukunftsentwürfe nicht eintreten sollten, würde ein Europa, das mehr Verantwortung für das globale Cybersicherheits-Ökosystem übernimmt, die Sicherheitslage von Politik, Wirtschaft und Gesellschaft auf dem eigenen Kontinent und darüber hinaus stärken. Drei Schritte sind dafür entscheidend.

Informationen über Cyberbedrohungen sammeln

Um die Abhängigkeit von US-amerikanischen CTI-Anbietern zu reduzieren, könnten öffentliche Beschaffungsvorhaben in Europa — sofern die geltenden Regeln dies zulassen — bevorzugt europäische CTI-Anbieter berücksichtigen. Alternativ ließe sich auf europäischer Ebene ein Rechtsrahmen dafür schaffen, wie Unternehmen die Bedrohungsindikatoren von Cybersicherheits-Vorfällen mit Regierungsstellen teilen — ähnlich dem Cybersecurity Information Sharing Act der USA (der allerdings im Oktober ausgelaufen ist). Auch ohne gesetzliche Regelung könnten die europäischen Cybersicherheits-Behörden stärker den Kontakt zu CTI-Anbietern suchen und Vernetzungsmöglichkeiten fördern; ebenso könnten sie auf Forschungsprojekte wie das European Repository of Cyber Incidents (EuRepoC, dessen Konsortium auch die SWP angehört) zurückgreifen.

Um einen möglichen Wegfall der »hunt forward«-Operationen des US Cyber Command zu kompensieren, sollten die EU-Mitgliedstaaten selbst solche Einsätze durchführen. Bereits 2018 wurde mit Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) ein entsprechendes EU-Projekt eingerichtet. Dabei handelt es sich um ein sogenanntes PESCO-Projekt, in dem EU-Mitgliedstaaten und Partnerstaaten enger im Bereich Sicherheits- und Verteidigungspolitik zusammenarbeiten. Litauen leitet dieses Projekt, an dem elf weitere Staaten beteiligt sind (Deutschland nicht). Allerdings hat es bisher nur zwei Missionen in Moldau durchgeführt.

CRRT bietet einen Rahmen für Mitglied- und Partnerstaaten der EU, um Cyberoperationen durchzuführen, sowohl auf Einladung von Drittstaaten als auch zur Unterstützung untereinander. Deutschland sollte sich dem Projekt anschließen, damit Fachleute des Bundesamts für Sicherheit in der Informationstechnik (BSI) es unterstützen und so einen Beitrag zum Sammeln von CTI leisten können.

Rechtssicherheit für Sicherheitsforschende schaffen

Im Zusammenhang mit dem Sammeln von CTI sollte die Bundesregierung auch die Rechtslage für Sicherheitsforschende verbessern. Bis heute ist diese Tätigkeit in vielen Staaten von Rechtsunsicherheit geprägt, wenn sie nicht sogar kriminalisiert wird. Für Deutschland liegen dazu seit Jahren Reformvorschläge auf dem Tisch. Die letzte Bundesregierung hatte sich die nötige Anpassung des Strafrechts vorgenommen, doch das Ende der Ampel-Koalition kam einer Einigung zuvor. Die aktuelle Bundes-

regierung hegt bisher keine entsprechenden Pläne. Das sollte sie jedoch tun, um sicherzustellen, dass Schwachstellen in für Europa wichtigen Software-Produkten gemeldet werden.

In das Cybersicherheits-Ökosystem investieren

Verglichen mit diesen Abhängigkeiten sind die von der US-amerikanischen Regierung finanzierten Schwachstellen-Datenbanken zwar ein enorm wichtiger »single point of failure«, aber Europa könnte hier leicht an die Stelle der USA treten. Ähnliches gilt für deren Rolle als Finanzier von Projekten zur OSS-Sicherheit.

So könnten etwa die Agentur der Europäischen Union für Cybersicherheit (ENISA) oder das BSI, gegebenenfalls zusammen mit weiteren nationalen Cybersicherheits-Agenturen in Europa, die Finanzierung der CVE-Datenbank übernehmen. Eine Alternative zur US-amerikanischen NVD ist mit der European Union Vulnerability Database (EUVD) schon im Mai 2025 gestartet. ENISA ist bemüht, die Initiative als komplementär zur NVD darzustellen, doch sie könnte die US-Datenbank perspektivisch auch ersetzen. Allerdings baut die EUVD aktuell, genau wie NVD, auf Material der CVE-Datenbank auf, was eine langfristige Sicherung dieser Informationsquelle umso dringlicher macht.

Um ein Wegbrechen der US-Finanzierung des OSS-Ökosystems abzufedern, sollte Europa hier Finanzierungsvehikel an den Start bringen, die die Sicherheit von OSS-Projekten unterstützen. Ein wichtiges Vorbild dafür ist die vom Bundeswirtschaftsministerium unterstützte Sovereign Tech Agency. Mit einem jährlichen Budget von 17 Millionen Euro im Jahr 2024 ist diese Initiative bisher in ihrer Wirkmacht eher schwach. Daher sollten entweder weitere EU-Staaten die Agentur unterstützen oder ein europäisches Pendant aufsetzen.

Sollte die US-Regierung die finanzielle Unterstützung von Cybersicherheits-Projekten einstellen, ließen sich die negativen Auswirkungen also mit eigenen Investitionen vergleichsweise einfach entschärfen. Diese wären auch in den anderen beiden der skizzierten Szenarien sinnvoll und sollten daher priorisiert werden.

Weitergehende Herausforderungen

Aus den genannten Abhängigkeiten könnte sich Europa also befreien. Schwerer hingegen wiegt die Tatsache, dass Unternehmen aus den Vereinigten Staaten den Markt für Cybersicherheits-Anwendungen dominieren. Zwar gibt es hier auch kleinere europäische Player, doch sorgen Netzwerkeffekte dafür, dass die US-amerikanischen Firmen ihre beherrschende Position voraussichtlich behalten werden. Das könnte Europa sowohl im Fall veränderter politischer Prioritäten in Washington zu spüren bekommen als auch bei dem Szenario, dass die US-Regierung diese Abhängigkeit gezielt gegen den Kontinent einsetzt. Gefragt sind hier langfristige Schritte wie die Förderung von OSS und die Unterstützung eines Tech-Ökosystems in Europa.

Gleichzeitig können aus dieser Abhängigkeit jedoch auch andere Hebel erwachsen. So sollten europäische Entscheidungsträger:innen prüfen, wann es sich hierbei um eine wechselseitige Dependenz handelt. So sind etwa große CTI-Anbieter durchaus darauf angewiesen, über ihre Kundschaft Daten zu globalen Cyberbedrohungen zu erhalten. Im Szenario eines Konflikts hätte Europa also zusätzliche Instrumente zur Hand, etwa Marktzugangsbeschränkungen.

Zudem stehen Deutschland und Europa vor weiteren Herausforderungen. Erstens ist die starke Abhängigkeit von US-Unternehmen nicht nur in den drei genannten Szenarien problematisch, sondern auch dann, wenn entsprechende Firmen vom Markt verschwinden (etwa weil sie Konkurs anmelden). Mit dieser Möglichkeit sollten sich europäische Entscheider:innen und Anwender:innen ebenfalls beschäftigen.

Und auch wenn die Debatte um Abhängigkeiten von den USA derzeit Konjunktur hat, so bestehen — zweitens — weiterhin

immense Abhängigkeiten von China, die als noch problematischer gelten als jene von den Vereinigten Staaten, etwa im Bereich seltener Erden für die Halbleiterproduktion. Verbunden damit ist drittens die Frage, wem sich Europa zuwenden möchte, wenn es sich von den USA abwendet, solange ein »EuroStack« noch Zukunftsmusik ist. Wenn etwa Software-Anbieter aus China und Russland nicht in Frage kommen, bleiben neben europäischen Herstellern vor allem solche aus Israel, Kanada, Australien und dem asiatischen Raum.

Gleichzeitig lehrt die Erfahrung, dass der Abbau solcher Abhängigkeiten politische Entschlossenheit, Ressourcen und Zeit erfordert. Und selbst wenn dies gegeben ist, wird das Ziel nicht immer erreicht, wie der Fall chinesischer Netzwerkinfrastruktur-Technologie zeigt. Politische Entscheidungsträger:innen in Berlin und Brüssel sollten die genannten Empfehlungen daher zügig angehen, um die eigene Handlungsfähigkeit langfristig sicherzustellen.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
DOI: 10.18449/2025A48

Dr. Alexandra Paulus ist Wissenschaftlerin in der Forschungsgruppe Sicherheitspolitik und Ko-Koordinierende Leiterin des Forschungsclusters Cybersicherheit und Digitalpolitik.