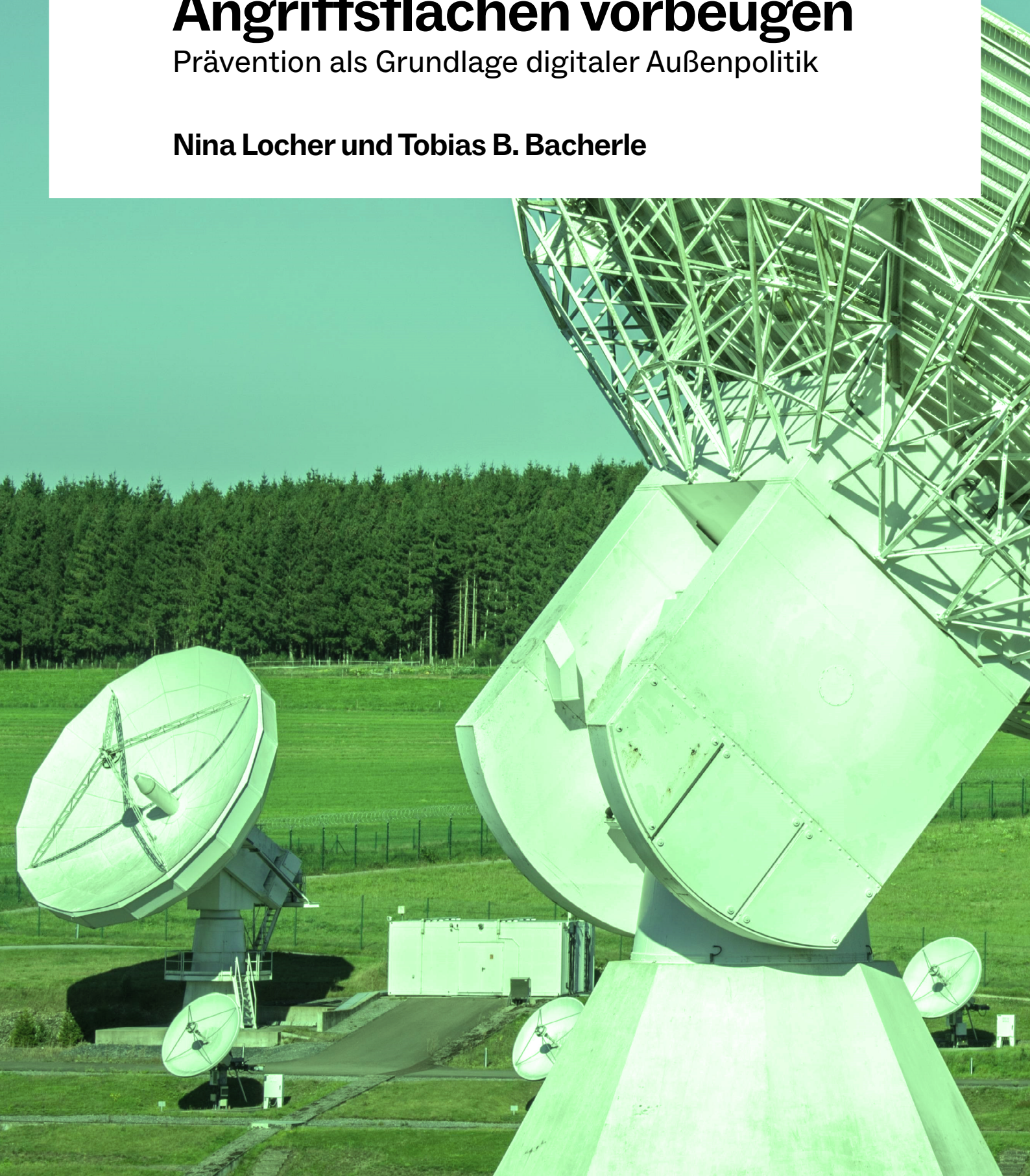
Dimensionen digitaler Außenpolitik

böllpaper

Teil 1: Angriffsflächen vorbeugen

Prävention als Grundlage digitaler Außenpolitik

Nina Locher und Tobias B. Bacherle



Teil 1:
Angriffsflächen vorbeugen

Prävention als Grundlage digitaler Außenpolitik

Ein Policy Paper von Nina Locher und Tobias B. Bacherle

HEINRICH BÖLL STIFTUNG

Inhalt

Zusammenfassung

Digitalpolitik ist zu einem zentralen Schauplatz geopolitischer Auseinandersetzungen geworden. Längst haben sich Kämpfe um Macht und Einfluss von Staaten und nationalen Interessen, kriegerische Auseinandersetzungen, aber auch die Verteidigung der sowie die Angriffe auf Freiheits- und Menschenrechte in den digitalen Raum verlagert. Im Zentrum dieser Auseinandersetzungen stehen Cybersicherheit, Manipulation, Desinformation. Doch die Logik im digitalen Raum ist eine andere als in kinetischen Konflikten: Sicherheit kann es nur gemeinsam geben, denn Sicherheitslücken und Angriffsflächen bedrohen nie Einzelne, sondern immer alle.

Um dieser geopolitischen Dimension der Digitalpolitik gerecht zu werden und in einem umkämpften digitalen Umfeld bestehen zu können, braucht digitale Außenpolitik eine klare Linie. In diesem ersten von drei Policy Papers zeigen wir auf, welche Grundlagen in nationaler und europäischer Politik gelegt werden müssen, damit Deutschland und Europa international erfolgreich agieren können.

Eine Säule der digitalen Außenpolitik muss sein, präventiv anzusetzen. Es ist das zentrale Ziel, die digitale Handlungsfähigkeit Deutschlands und Europas, nach innen wie nach außen zu sichern. Digitale Souveränität ist dabei keine Frage von Autarkie, sondern von Entscheidungsfreiheit: Staaten müssen in der Lage sein, digitale Infrastrukturen, Dienste und Kommunikationsräume auch in geopolitisch angespannten Situationen zuverlässig betreiben, wechseln oder ersetzen zu können.

Hierfür müssen einseitige Abhängigkeiten, wie sie beispielsweise bei Clouddiensten, Online-Plattformen und Satellitenkommunikation bestehen, identifiziert und diversifiziert werden, denn sie können als geopolitisches Druckmittel gegen Europa eingesetzt werden. Auch bestehende gegenseitige Abhängigkeiten und eigene Stärken in digitalen Wertschöpfungsketten müssen analysiert sowie strategisch betrachtet und eingesetzt werden.

Die nationale Dimension und Grundlagen für eine wirksame digitale Außenpolitik, die vorausschauend vor einem Angriff ansetzt, verbinden daher drei Handlungsfelder:

Erstens geht es darum, Abhängigkeiten zu reduzieren und die Resilienz zu erhöhen, insbesondere in kritischen Infrastrukturen, Lieferketten und digitalen Basisdiensten.

Zweitens sollten souveräne digitale Anbieter und Lösungen gestärkt werden, etwa durch Investitionen in Open-Source-Lösungen, gezielte staatliche Nachfrage, vorkommerzielle Auftragsvergabe (*Precommercial Procurement*) und eine Stärkung der Sovereign Tech Agency.

Drittens müssen digitale Sicherheit und Freiheitsrechte konsequent geschützt werden, da Verschlüsselung, geschlossene Sicherheitslücken und der Schutz der digitalen Öffentlichkeit Grundvoraussetzungen für Sicherheit, Vertrauen und internationale Glaubwürdigkeit sind.

Digitale Außenpolitik ist keine technische Spezialfrage, sondern eine zentrale Voraussetzung integrierter Sicherheit. Wer Freiheitsrechte im digitalen Raum schwächt oder Sicherheitslücken absichtlich offen hält, untergräbt nicht nur die eigene Resilienz, sondern auch die außenpolitische Glaubwürdigkeit Deutschlands. Prävention, Resilienz und der Schutz digitaler Rechte müssen daher leitende Prinzipien deutscher und europäischer digitaler Außenpolitik sein.

1 Digitale Außen- und Geopolitik beginnt im Inneren

In geopolitisch angespannten Zeiten sind Cybersicherheit und digitale Souveränität in aller Munde. Doch während gerade in sicherheitspolitischen Debatten teilweise von internationalem Wettrüsten im Digitalen wahlweise geträumt oder davor gewarnt wird, ist die Logik im digitalen Raum eigentlich eine andere: Sicherheit kann nicht selektiv an nationalen oder administrativen Grenzen gewährleistet werden, Schwachstellen und Einfallstore schwächen immer alle. Insbesondere bei breit genutzten Standards, Protokollen und Open-Source-Infrastruktur gilt bereits seit Langem die Prämisse integrierter Sicherheit. Wenn digitale Systeme miteinander verflochten sind und gemeinsam genutzt werden, entstehen keine abgeschotteten Sicherheitsräume, sondern geteilte Verwundbarkeiten. Damit wird digitale Infrastruktur zu einem sicherheitspolitischen Gemeingut und ihre Stabilität zu einer Frage kollektiver staatlicher Handlungsfähigkeit.

1.1 Die Macht digitaler Infrastrukturen

Abhängigkeiten von digitalen Infrastrukturen, Plattformen und Diensten schränken die strategische Autonomie von Staaten ein. Diese Logik hat unmittelbare außenpolitische Konsequenzen. Besonders deutlich wird dies bei der starken Konzentration zentraler digitaler Dienste bei wenigen, überwiegend US-amerikanischen Tech-Konzernen (Paulus 2025). Ihre enge Verquickung mit der Trump-Administration und deren unberechenbares Vermengen von politischen Forderungen über gewohnte Verhandlungspakete hinaus machen deutlich, wie digitale Abhängigkeiten außenpolitische Verhandlungsfähigkeit begrenzen.

Hinzu kommt die große Bedeutung sozialer Plattformen für die Organisation demokratischer Öffentlichkeit im digitalen Raum (Eisenegger 2021). Soziale Medien sind eine Art kritische Infrastruktur für die Demokratie (Hausding 2025). Sie strukturieren politische Meinungsbildung und einen globalen Informationsraum, z. B. indem sie internationale Menschenrechtsbewegungen bei der Mobilisation unterstützen, nationale Entwicklungen mit der Diaspora kommunizieren oder als Plattformen der diplomatischen Kommunikation genutzt werden. Zugleich nehmen Foreign Information and Manipulation and Interference (FIMI), d. h. ausländische Einmischung und Manipulation der Öffentlichkeit, wie beispielsweise systematische Desinformationskampagnen wie die prorussische Doppelgänger-Kampagne zu (Frühwirth/Smirnova 2024). Bei dieser Kampagne wurden Nachrichtenseiten abgewandelt, gefälscht und nachgebaut sowie falsche Artikel verbreitet, um irreführende und falsche Informationen zu streuen, das Vertrauen in die demokratischen Institutionen in Deutschland zu schwächen und Deutschland politisch zu destabilisieren.

Gleichzeitig kontrollieren die Plattformen auch selbst die Distribution von Informationen. Indem sie Sichtbarkeit, Reichweite und Verteilung politischer Inhalte strategisch beeinflussen können, erhalten Plattformbetreiber wie Elon Musk und Regierungen, die auf sie Einfluss nehmen, erheblichen (außen-)politischen Einfluss. Die Organisation digitaler Öffentlichkeit wird damit zu einem politischen, geostrategischen und ökonomischen Machtfaktor. Der Bundestagswahlkampf 2025, bei dem Elon Musik auf X für die AfD warb, während er mindestens seine Tweets bevorzugt ausspielen ließ, steht exemplarisch für den außenpolitischen Einfluss sozialer Medien in den Händen mächtiger Milliardäre. Aber auch TikTok fiel früh durch entsprechende Beeinflussung von politischen Inhalten auf (Reuter/Köder 2019).

1.2 Digitale Systeme in Zeiten hybrider Bedrohungen am Laufen halten

Die Handlungsfähigkeit digitaler Systeme äußert sich im Besonderen darin, ob sie auch im Krisenfall funktionieren, d. h. souverän sind. Bei der Funktionsfähigkeit geht es in erster Linie darum, dass Systeme grundlegend ihren Zweck erfüllen und hierbei zuverlässig sind, also weder abgeschaltet noch von Dritten missbraucht werden können. In vielen Fällen ist darüber hinaus jedoch auch entscheidend, wie sie diesen Zweck erfüllen. Beispielsweise stellt sich bei sozialen Plattformen und anderen informationsverteilenden Plattformen die Frage, wie die zugrunde liegenden Algorithmen und Verteilmechanismen funktionieren und wie diese überprüft werden können. Dafür müssen Datenzugänge existieren, mit denen Anomalien und Manipulationen festgestellt werden können.

Digitale Souveränität betrifft mehr als Software, Daten oder Plattformen. Digitale Systeme sind auf physische Komponenten angewiesen, von Halbleitern und Servern über Telekommunikationshardware bis hin zu Rohstoffen. Ihre Produktion basiert in großen Teilen auf Systemen der Ausbeutung des Globalen Südens. Einseitige Abhängigkeiten von Rohstoffen, insbesondere von seltenen Erden, stellen nicht nur ein wirtschaftliches Risiko dar, sondern machen strategisch verwundbar bis hin zur Erpressbarkeit und beschränken Deutschlands geopolitische Handlungsfähigkeit. In den letzten Jahren hat sich diese Vulnerabilität durch die russische Vollinvasion in der Ukraine und die Abhängigkeit von russischem Gas, aber auch chinesische Ausfuhrbeschränkungen deutlich gezeigt. Besonders deutlich ist diese Verwundbarkeit im Bereich der Halbleiter und Chips, die für digitale Hardwareprodukte wie beispielsweise Handys benötigt werden.

Doch solche Interdependenzen sind sicherheitspolitisch ambivalent. Sie machen Europa einerseits anfällig für Störungen und politischen Druck. Andererseits eröffnen diese globalen Wertschöpfungsketten auch strategische Hebel für Europa, die außen- und sicherheitspolitisch genutzt werden können. Digitale Außenpolitik muss deshalb nicht nur Abhängigkeiten reduzieren, sondern auch eigene Stärken in globalen Wertschöpfungsketten systematisch analysieren und gemeinsam mit Partnern politisch übersetzen.

2 Prävention als Voraussetzung kohärenter digitaler Außenpolitik

Digitale Außenpolitik ist dann wirksam, wenn sie auch präventiv ansetzt. Angriffsflächen im Bereich der Lieferketten, digitaler Abhängigkeiten und Schwachstellen in der IT-Sicherheit entstehen nicht erst im Moment des Angriffs, sondern dort, wo Abhängigkeiten, Monopole und ungeschlossene Sicherheitslücken bestehen. Für eine verbesserte Handlungsfähigkeit sind die Identifizierung und Verringerung dieser Vulnerabilitäten essenziell, um schneller, besser und entschiedener auf Angriffe reagieren zu können. Im Sinne der Verschränkung innerer und äußerer sowie integrierter Sicherheit ist Prävention ein Schlüssel für mehr Widerstandsfähigkeit und Resilienz.

2.1 Digitale Souveränität als Entscheidungs- und Handlungsfähigkeit

Zentrales Instrument dieser Prävention ist digitale Souveränität. Prävention zielt dabei nicht auf vollständige Autarkie, sondern die Fähigkeit von Staaten, Institutionen und Gesellschaften, digitale Systeme selbstbestimmt, sicher und verlässlich zu nutzen, zu kontrollieren und im Bedarfsfall zu wechseln. Digitale Souveränität ist damit eine Voraussetzung für außenpolitische Entscheidungsfreiheit. So besteht die Sorge, dass externe Akteure durch die Kontrolle über bestimmte Aspekte eines digitalen Produkts oder einer digitalen Anwendung, wie etwa chinesische Komponenten in der 5G-Telekommunikationsinfrastruktur, die Funktionalität unserer Systeme beeinflussen können (Fokuhl et al. 2025). Vorzusorgen heißt deshalb auch, zu gewährleisten, dass es im tatsächlichen Fall einer Abschaltung oder gar Zerstörung von digitalen Infrastrukturen Alternativen gibt, die im Notfall bereitstehen, fehlerfrei die wichtigsten Funktionen des Staates zu übernehmen.

Die Bundesregierung definierte digitale Souveränität 2020 als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“ (Der Beauftragte der Bundesregierung für Informationssicherheit/IT Planungsrat/IT Rat 2020: 1). Auf dem von Deutschland und Frankreich ausgerichteten europäischen Souveränitätsgipfel am 18. November 2025 einigten sich alle 27 EU-Staaten auf eine gemeinsame Erklärung für europäische digitale Souveränität (Digital Austria 2025). Diese geht noch darüber hinaus und bezieht sich auf „die Fähigkeit von Einzelpersonen, Unternehmen und Institutionen in Europa, in der digitalen Welt unabhängig zu handeln und autonome Entscheidungen über die Nutzung, Steuerung und Entwicklung digitaler Systeme zu treffen, ohne sich übermäßig auf externe Akteure verlassen zu müssen, um unsere europäischen Demokratien und unsere europäischen Werte zu schützen“. Digitale Souveränität umfasst dabei mehrere Kernaspekte. Dazu gehören die Entwicklung

vertrauenswürdiger Technologien, die Hoheit über die eigenen Daten, hohe Sicherheitsstandards, Selbstbestimmung über den entscheidenden rechtlichen Rahmen sowie die technologische Flexibilität für den Wechsel zwischen Produkten und Systemen ohne Vendor Lock-in: Bei Abhängigkeit von einem einzelnen Anbieter könnten sonst Produkte nur unter hohen Kosten gewechselt werden.

Wenn Entscheidungen über digitale Systeme nicht mehr ohne externe Akteure getroffen werden können, ist der Punkt gekommen, an dem sich Digitalpolitik und Außenpolitik in der Frage der Souveränität verzahnen. Das erkennt auch die Nationale Sicherheitsstrategie 2023 an: „Entscheidend für unsere Widerstands- und Wettbewerbsfähigkeit ist eine hohe Innovationskraft, weshalb wir technologische und digitale Souveränität als wesentlichen Bestandteil Integrierter Sicherheit betrachten. Diese Souveränität ermöglicht es uns, Schlüsseltechnologien international im Einklang mit unseren Werten mitzugestalten und anzuwenden“ (Die Bundesregierung 2023: 57).

2.2 Digitale Abhängigkeiten als außenpolitische Verwundbarkeit

Wenn zentrale digitale Systeme nicht ohne externe Akteure betrieben, angepasst oder ersetzt werden können, entstehen außenpolitische Risiken. Abhängigkeiten von einzelnen Anbietern, Staaten oder privaten Akteuren können gezielt als politisches Druckmittel genutzt werden und schränken die Fähigkeit ein, eigenständig außen- und sicherheitspolitische Entscheidungen zu treffen. Ein besonders prägnantes Beispiel hierfür ist die Abhängigkeit der Ukraine vom US-amerikanischen Satellitensystem Starlink (Poirier 2025: 1). Starlink ist ein elementarer Teil der ukrainischen Landesverteidigung. Aufgrund aktuell unzureichender Alternativen souveräner Satelliteninfrastruktur für die Ukraine ist das Land gegenwärtig auf das Wohlwollen von Elon Musk angewiesen. Wenige Monate nach der Übernahme der Regierungsgeschäfte nutzten die USA unter Trump diese Abhängigkeit als Druckmittel in den Verhandlungen um ein Rohstoffabkommen. Nach Berichten drohten Unterhändler, Starlink einzuschränken (Shalal/Roulette 2025). Gravierend war diese Drohung insbesondere vor dem Hintergrund, dass kurze Zeit später, am 7. März 2025, die Trump-Regierung den Zugang der Ukraine zu Daten der MAXAR-Aufklärungssatelliten einstellte (Körömi 2025).

Digitale Außenpolitik erfordert im Sinne der Vorsorge eine Stärkung digitaler Souveränität, um eigenständig, frei und sicher handeln zu können. Insbesondere aber folgt diesem Umstand die Anforderung, echte und funktionsfähige Alternativen und Redundanzen in kritischen Infrastrukturen für einen Notfall bereithalten zu können.

2.3 Der Schutz vor Eingriffen in digitale Infrastruktur

Digitale Systeme sind auf komplexe, global organisierte Wertschöpfungsketten angewiesen. Spätestens seit der COVID-19-Pandemie wird Lieferkettenresilienz eine deutlich größere Aufmerksamkeit zuteil. Das ist auch für die digitale Infrastruktur, Anwendungen und digitale Dienste wichtig. Lieferkettenresilienz wird bestimmt sowohl von direkten geo- und sicherheitspolitischen Risiken und vorsätzlichen Interventionen als auch von herkömmlichen Risikobewertungen wie Supportfähigkeit, Monopolisierung und fremdverschuldeten Ausfällen.

Viele digitale Produkte und Dienste werden heute als integrierte Komplettlösungen bereitgestellt und bleiben für Anwender*innen faktisch eine Blackbox. Das gilt besonders, wenn mehrere Ebenen zu einem Stack gebündelt werden, etwa wenn Software, Hosting und Managed-Cloud-Betrieb als untrennbare Einheit verkauft werden. Gleichzeitig sind auch proprietäre Produkte in hohem Maße von Open-Source-Basiskomponenten abhängig. So betraf eine 2021 bekannt gewordene Sicherheitslücke der Open-Source-Bibliothek log4J laut einer Liste, auf die auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) verwies, mehr als 140 Produkte, darunter zahlreiche von proprietären Anbietern wie VMware (BSI 2021: 2). Unter anderem wurden Angriffe über das Spiel Minecraft auf Server festgestellt (Beuth 2021); die Homepage des Bundesrechnungshofs (Knop 2021) und Systeme des belgischen Militärs mussten zeitweise offline genommen werden (Briegleb 2021). Das zeigt: Auch und gerade dann, wenn die Basisinfrastruktur nicht von den Unternehmen entwickelt wird, die das Endprodukt vertreiben, muss diese gepflegt werden.

Für Nutzende bleibt dabei oft unklar, wie sich das Produkt oder der Dienst eigentlich zusammensetzt und funktioniert. Was im Alltag für den Nutzenden häufig kein Problem darstellt und gleichzeitig das Geschäftsgeheimnis im Interesse des Diensteanbieters schützt, wird bei kritischer Infrastruktur, bei der Organisation einer digitalen Öffentlichkeit sowie im Ernstfall eines Angriffs zunehmend zu einem Sicherheitsrisiko.

2.4 Digitale Sicherheit

Die Verschränkung von innerer und äußerer Sicherheit macht deutlich, dass digitale Außenpolitik auch bei innerer Sicherheit ansetzen muss. Der Lagebericht des BSI zur IT-Sicherheit in Deutschland 2025 machte zuletzt in Zahlen sichtbar, wie stark die Gefahrenlage gestiegen ist. Täglich entstehen laut BSI durchschnittlich 119 neue Schwachstellen, also bisher unbekannte Sicherheitslücken in Software, digitalen Endgeräten oder Anwendungen, die Angreifer ausnutzen können, um unbefugt in Systeme einzudringen. Viele davon bleiben offen (BSI 2025).

Alle paar Wochen diskutiert der Deutsche Bundestag in einer aktuellen Stunde einen akuten Fall eines hybriden Angriffs. Inmitten des Bruchs der Ampelregierung forderte BKA-Präsident Holger Münch im Dezember 2024 eine Zeitenwende der inneren Sicherheit (Münch 2024). Auf eine solche Zeitenwende haben sich CDU, CSU und SPD im Koalitionsvertrag geeinigt (CDU/CSU/SPD 2025: 60). Im September 2025 forderte zudem die Oppositionsfraktion Bündnis 90/Die Grünen eine Sicherheitsoffensive gegen hybride Bedrohungen (Fraktionsvorstand Bündnis 90/Die Grünen im Deutschen Bundestag 2025).

Entsprechend der Nationalen Sicherheitsstrategie der Bundesregierung (2023) heißt integrierte Sicherheit, Digitalisierung menschenzentriert zu gestalten, also die Sicherheitsbedarfe der Menschen in den Blick zu nehmen (Die Bundesregierung 2023: 7). Ein Schlüsselaspekt der Prävention ist daher die Arbeit an den eigenen Schwachstellen und Einfallstoren für Dritte. Nach langer Verspätung hat der Bundestag 2025 höhere IT-Sicherheitsstandards für kritische Infrastrukturen im NIS2-Umsetzungsgesetz sowie 2026 eine entsprechende Erhöhung des physischen Schutzes kritischer Infrastrukturen im Rahmen des KRITIS-Dachgesetzes beschlossen. Je resilienter unsere eigenen Systeme gegen hybride Bedrohungen, etwa durch Cyberangriffe, Spionage, Sabotage oder Desinformation sind, desto schwieriger machen wir es externen Kräften, eine Angriffsfläche gegen uns zu finden.

Eine resiliente digitale Außenpolitik muss deshalb bei der digitalen Sicherheit im Inneren ansetzen. In der öffentlichen Debatte werden dafür erweiterte, flächendeckende Zugriffs- und Überwachungsmöglichkeiten für Strafverfolgungsbehörden diskutiert, etwa durch flächendeckende IP-Adressenspeicherung oder biometrische Überwachung. Diese Forderungen folgen jedoch einem Trugschluss: Sie sollen helfen, schnell zu reagieren, nachdem ein Angriff nicht verhindert werden konnte, weil entsprechende präventive Maßnahmen nicht ausgereicht haben.

Das Engagement digitaler Außenpolitik zeigt sich allerdings nicht nur im Inneren, sondern auch an ihrer Glaubwürdigkeit auf der internationalen Bühne. Dies erkennt auch die Nationale Sicherheitsstrategie an: „Im Rahmen unserer Cyberaußenpolitik werden wir daher bei der Regulierung des Cyberraums für die weltweite Einhaltung von menschenrechtlichen Standards eintreten, einschließlich des Schutzes der Privatsphäre, der Meinungsfreiheit und des Rechts auf Verschlüsselung“ (Die Bundesregierung 2023: 59). Menschliche Sicherheit muss sich an den Bedürfnissen der Menschen ausrichten; sie wollen sicher sein und sich sicher fühlen. Dafür müssen auch geschlechterspezifische und intersektionale Perspektiven in den Blick genommen werden. Wenn mit der Intention, das Sicherheitsgefühl von Bürger*innen zu stärken, Sicherheitslücken bewusst offen gehalten werden und damit Cybersicherheit geschwächt wird, ist dies nicht nur ein Widerspruch, sondern wirkt sich auch auf die Glaubwürdigkeit und Wahrnehmung Deutschlands in der Welt aus. Ein in sich stimmiger Ansatz richtet die Erwartungen für digitale Sicherheit gleichermaßen an vertrauensvolle internationale Partner, globale Wettbewerber und den eigenen Staat.

3 Instrumente digitaler Außenpolitik: Ein Maßnahmenpaket für mehr Schutz, Stärkung und Sicherheit nach innen und außen

Wenn Technologien Konflikte verändern, muss Deutschland dafür Sorge tragen, dass unsere Systeme und unsere Gesellschaft selbstbestimmt, sicher und widerstandsfähig bleiben. Dafür müssen die Souveränität der Cybersicherheitsstrukturen und kritische Infrastrukturen gegen Angriffe von außen gestärkt werden. Genauso essenziell ist es, demokratische Gesellschaften zu stärken und widerstandsfähig zu machen: gegen digitale Angriffe, die spalten und aufhetzen sollen.

3.1 Das Ökosystem digitaler Infrastruktur schützen

Zum Schutz vor digitalen Angriffen müssen im ersten Schritt Vulnerabilitäten in physischen wie digitalen Systemen erkannt und abgebaut werden. Dies beinhaltet die Sicherheit unserer Telekommunikationssysteme und Solaranlagen genauso wie unsere persönlichen Foto-Ordner in Cloudspeichern. Für den Ernstfall eines Angriffs müssen redundante Datenbotschaften mit extraterritorialen Back-ups, also Rechenzentren außerhalb des deutschen Territoriums, welche Kopien der wichtigsten Daten des Staates und von Bürger*innen speichern, die essenziellen digitalen Funktionen unseres Staates absichern. Eine widerstandsfähige demokratische Gesellschaft braucht funktionierende und neutrale digitale Räume. Deshalb müssen Plattformen, welche die digitale Öffentlichkeit organisieren, als kritische Infrastruktur anerkannt werden.

Interdependenzen als sicherheitspolitischen Machtfaktor erkennen

Europa muss neben Abhängigkeiten auch Interdependenzen systematisch in den Blick nehmen. In digitalen Wertschöpfungsketten sind diese ein sicherheitspolitischer Machtfaktor und müssen als solcher behandelt werden: Sie können zur Erpressung verwendet werden, wie es China mit seinen Exportkontrollen gegen die USA und Europa begonnen hat.

Interdependenzen können uns und unsere Partner jedoch auch schützen: Ohne Maschinen und Technologien von Upstream-Akteuren wie ASML, Zeiss und Trumpf lassen sich weltweit keine modernen Chips herstellen. Europa kontrolliert damit strategische Schlüsselpositionen in der globalen Halbleiterproduktion; Partner wie Taiwan verfügen über zentrale Fertigungskapazitäten. Diese verschränkte Interdependenz bietet keine Komfortzone, sie ist ein kooperativer Instrumentenkasten: Wer

erpressungsresistent sein will, braucht eine nüchterne „Leverage-Analyse“ der eigenen und fremden Engpässe, abgestimmte Maßnahmen mit Verbündeten (von Lieferzusagen über Redundanzen bis zu Exportkontroll- und Sanktionsoptionen) und klare Spielregeln, wie diese Hebel zum gemeinsamen Schutz der eigenen Handlungsfreiheit eingesetzt werden. Gerade weil Europas strukturelle Stärke häufig im vorgelagerten Bereich der Wertschöpfungskette, also weit Upstream, liegt, muss sie politisch übersetzt und koordiniert genutzt werden, sonst bleibt sie bestenfalls ökonomisch relevant, aber strategisch wirkungslos.

Sicherheit von Hardware-Komponenten in kritischer Infrastruktur

Die Sicherheit digitaler Infrastruktur hängt wesentlich von der eingesetzten Hardware ab. Wenn es um die Bauteile kritischer Infrastruktur geht, etwa um Telekommunikation und 5G-Infrastruktur oder um die für Solaranlagen erforderlichen Wechselrichter (Kessler 2025), wird schnell klar: Chinesische Komponenten sind aus vielen Wirtschaftssektoren nicht mehr wegzudenken, so verflochten und abhängig sind viele deutsche Industriezweige. Die Sicherheitsüberprüfung der Telekommunikationsinfrastrukturen der Bundesregierung 2024 hat gezeigt, dass besonders in den Kernnetzen dringend Handeln geboten ist: Bis Ende 2026 dürfen keine chinesischen Komponenten in den Kernnetzen mehr eingesetzt werden, da diese aus Sicht der Bundesregierung ein massives Sicherheitsrisiko bergen (Bundesministerium des Innern 2024). So unbequem es ist: Diese Auseinandersetzung muss auch auf andere kritische Infrastrukturen, auf deren Funktionsfähigkeit Deutschland dringend angewiesen ist, ausgeweitet werden. Insbesondere die Energie- und die Krankenhausversorgung müssen zügig daraufhin überprüft werden, ob kritische Komponenten im Ernstfall gezielt genutzt werden könnten, um diese Systeme abzuschalten oder zu zerstören. Der EU Cyber Resilience Act, der die Auflistung von Komponenten einer Software-Lösung vorschreibt (Software Bill of Materials, SBOM) (BSI o. D.), und der Verordnungsentwurf für den EU Cyber Security Act 2, der Hochrisikokomponenten aus kritischen Infrastrukturen verbannen soll, sind hierfür wichtige Schritte.

Exit-Option bei Cloudbeschaffung

Digitale Abhängigkeiten und potenzielle Vulnerabilität entstehen auch dort, wo Daten und Rechenleistung auf wenige, nicht europäische Cloudanbieter ausgelagert werden. Der europäische Data Act beinhaltet bereits weitreichende Vorschriften zur sogenannten Datenportabilität, die Cloudwechsel einfacher möglich machen und Lock-in-Effekte mildern sollen (Bensinger 2025). Diese Wechselmöglichkeiten sind wichtig, um Abhängigkeiten von Anbietern abzuschwächen und einen weiteren Vendor Lock-in zu verhindern. Ist ein schneller Wechsel garantiert, können Multi-Cloud-Strategien einfacher konzipiert werden, und Abhängigkeiten werden reduziert. Bei Cloudanbietern sollte in Ausschreibungen auf vertraglich vereinbarte und überprüfbare Wechselmöglichkeiten sowie Interoperabilitätsstandards geachtet werden.

Aufbau einer Datenbotschaft

Selbst bei umfassenden Präventionsmaßnahmen bleibt das Risiko bestehen, dass digitale Infrastrukturen im Ernstfall durch physische Angriffe, Sabotage oder Cyberangriffe beeinträchtigt werden oder vollständig ausfallen. Eine resiliente digitale Außen- und Sicherheitspolitik muss daher auch Vorsorge für genau diesen Fall treffen. Um staatliche Handlungsfähigkeit zu schützen, sollten essenzielle digitale Funktionen unabhängig vom nationalen Territorium aufrechterhalten werden können. Hier lohnt ein Blick in die europäische Nachbarschaft: In der Folge wachsender Sicherheitsbedenken in Estland, u. a. durch gravierende Cyberangriffe bereits 2007 und nach der russischen Annexion der Krim 2014 (De Pommereau 2017), beschloss Tallinn 2017 den Aufbau einer Datenbotschaft in Luxemburg. Für den Ernstfall werden dort Serverräume und Rechenzentren vorgehalten mit Redundanzen, d. h. „Sicherheitskopien" von besonders zu schützenden und relevanten Informationen, um die Funktionsfähigkeit des estnischen Staates auch im Krisenfall sicherzustellen (E-Estonia o. D.).

Angesichts der anhaltenden Bedrohung durch hybride Angriffe sollte auch Deutschland eine Datenbotschaft an einem digitalen Ausweichsitz an einem Standort außerhalb des Landes aufbauen. Dadurch können mehrere voneinander unabhängige IT-Infrastrukturen geschaffen werden, die digitale Souveränität und Redundanzen im Angriffsfall ermöglichen. Eine solche Datenbotschaft sollte völkerrechtlich abgesichert werden, also einen bilateral zugesicherten Status analog zu Botschaften erhalten, der sie unter deutsche Jurisdiktion stellt. Der hierfür erforderliche finanzielle Aufwand ist als Investition in unsere Sicherheitsinfrastruktur zu verstehen, für die z. B. ein Rückgriff auf das Sondervermögen Infrastruktur bestens geeignet wäre.

Transparenzpflichten für die digitale Öffentlichkeit

Soziale Plattformen sollten explizit als kritische Infrastrukturen definiert werden und damit unter deren Sicherheitsanforderungen fallen. Sie entscheiden maßgeblich darüber, welche Informationen verbreitet werden und wer sie wann und wie oft zu sehen bekommt, und prägen so die Meinungs- und Willensbildung. Deshalb muss unabhängig überprüfbar sein, wie diese Plattformen funktionieren. Um dies nachvollziehen zu können, schreibt der Digital Services Act (DSA) bereits erste Transparenzpflichten vor, die jedoch ausgeweitet werden sollten. Plattformen, die Teil der kritischen Infrastruktur sind, sollten ihre Algorithmen bestenfalls vollständig offenlegen müssen, zumindest jedoch Aufsichtsbehörden in Echtzeit Zugriff gewähren.

Dies gilt auch für die Trainingsdaten und Suchalgorithmen von generativen KI-Modellen beziehungsweise deren Interfaces, die immer mehr klassische Websuchen ersetzen und damit maßgeblich beeinflussen, welche Informationen bei den Menschen ankommen.

3.2 Souveräne digitale Infrastruktur fördern

Das zweite Maßnahmenfeld betrifft die Stärkung einer resilienten digitalen Infrastruktur. Der Staat ist dabei nicht nur Regulierer, sondern auch Marktakteur und Investor. Als maßgeblicher IT-Nachfrager und Kunde sollte er sich überlegen, inwiefern er beispielsweise auf Anbieter setzen will, bei denen Datensicherheit und Funktionssicherheit von digitaler Infrastruktur fraglich sind. Dies kann konkret durch lokale Gesetze wie beispielsweise den US-amerikanischen Cloud Act und das US-Gesetz zur Überwachung in der Auslandsaufklärung (FISA) gegeben sein (Kolain/Kipker 2026), durch geopolitische Entwicklungen und Interessen oder durch über Sanktionen erzwungene Einstellung des Services (sogenannter *legal Killswitch*) (FOTI 2026: 3). Solche Anbieter sollten ausgeschlossen oder ausgetauscht werden. Des Weiteren sollten auch Möglichkeiten der Aufsplittung von Leistungen und Redundanz sowie die Förderung von Open-Source-basierten Lösungen gestärkt werden.

Sovereign Tech Agency stärken

Open-Source-Basisinfrastruktur ist grundlegend für nahezu alle digitalen Systeme – wird jedoch bislang nicht ausreichend strukturell gefördert. Ein Erfolgsmodell ist die Sovereign Tech Agency. Sie ist eine Tochtergesellschaft der Bundesagentur für Sprunginnovation, kurz SPRIND, die seit 2022 strukturell in die Förderung von Open-Source-Lösungen und insbesondere Basiskomponenten investiert und von der Bundesregierung gefördert wird (Sovereign Tech Agency o. D.). Der dort verortete Sovereign Tech Fund ist eine der größten und wichtigsten Initiativen staatlicher Finanzierung für Open-Source-Basisinfrastruktur. Die Förderung der Sovereign Tech Agency sollte strukturell in die Haushaltsplanung des Bundes aufgenommen und Aufträge von europäischen Partnern sollten integriert werden.

Benchmarks für Open Source & europäische Anbieter

Die Nutzung von Open Source ist ein sicherheitspolitischer Vorteil. Sie erleichtert nicht nur, im Krisenfall den Anbieter zu wechseln, sie verschränkt auch die Sicherheitsinteressen aller Beteiligten: Wer ein System nutzt, will, dass es möglichst sicher ist. Selbst wenn es kurzfristig verlockend sein könnte, Sicherheitslücken anderer auszunutzen, bleibt das eigene Interesse bestehen, das System zu aktualisieren, zu patchen und abzusichern. Gerade diese gemeinsame Anreizstruktur macht das Gesamtsystem widerstandsfähiger.

Damit sich ein tragfähiges europäisches Ökosystem entwickeln kann, braucht es jedoch eine planbare Nachfrage. Die Bundesregierung, Länder und Kommunen sollten deshalb klare Ziele definieren, um Investitionsanreize zu bieten. Hier muss der Staat mit klarer Vision und Mut vorangehen: Er sollte anstreben, bis 2030 90 Prozent seiner neu abgeschlossenen Cloud-Verträge mit europäischen Anbietern abzuschließen, die bestenfalls auf Open Source setzen. Zudem sollten 50 Prozent seiner Software als

Open-Source-Lösung beschafft werden. Eine klare Richtungsweisung kann Sicherheit für das Ökosystem geben, um Investitionen in Hardwareinfrastruktur, in die Weiterentwicklung der Produkte und in den Aufbau des Supportsystems zu tätigen.

Aufbau eigener Alternativen: PCPs, Start- & Scale-up-Förderung

Wo es bisher keine Alternativen mit zufriedenstellender Funktionalität oder Sicherheitsanforderungen gibt, sollte Deutschland vermehrt auf vorkommerzielle Vergabeverfahren (*Precommercial Procurement*, PCPs) setzen. Bei diesen Vergabeverfahren, die in Deutschland bisher u. a. die Agentur für Innovation in der Cybersicherheit (kurz: Cyberagentur) einsetzt, vergibt der Staat seine Aufträge schrittweise: Zuerst werden Lösungen konzipiert und in späteren Stufen entwickelt und gebaut. Am Ende der PCPs könnten neben Prototypen bestenfalls auch ein oder mehrere staatliche Aufträge stehen. So nutzt der Staat die Innovationskraft der Wirtschaft und gibt Unternehmen die Grundlage, solche Lösungen überhaupt erst entwickeln zu können.

In ähnlicher Weise sollte der Staat zunehmend als Ankerkunde auftreten. Er sollte also selbst zum frühen Auftraggeber bzw. Käufer von europäischen Produkten werden, etwa mit der Deutschen Verwaltungscloud, die von IONOS und StackIt umgesetzt wird und damit vertrauenswürdige Unternehmen gezielt fördern.

Ergänzend dazu können Acceleratorprogramme und Wettbewerbe Innovation in strategisch wichtigen Bereichen anstoßen. Vielversprechende Unternehmen erhalten Investitionen in Form eines Convertible Loans, also zunächst als Darlehen, das später in eine nach unten und oben gedeckelte, ansonsten am Marktwert orientierte, im Falle einer staatlichen Investition bestenfalls stille Unternehmensbeteiligung umgewandelt werden kann. SPRIND arbeitet bereits mit ähnlichen Ansätzen. Dieses Modell sollte gezielt auf Bereiche ausgeweitet werden, in denen ein strategischer Bedarf an souveränen digitalen Lösungen besteht. Sollte ein letzter Schritt im Wettbewerb ein weiteres Investment bereitstellen, so sollte dieses an das Investmentkapital privater Investor*innen gekoppelt sein.

Strategische Diversifizierung in kritischen Lieferketten

Deutschland und die Europäische Union sollten Partner strategisch dabei unterstützen, die Lieferketten sowohl zur Rohstoffveredelung als auch zur Chipproduktion breiter und resilienter aufzustellen. Strategisch kluge Diversifizierung sorgt dafür, dass Projekte zu alternativen Bezugs-, Veredelungs- und Fertigungskapazitäten sowohl in Europa und in Partnerländern angesiedelt, diese darin unterstützt werden und sichergestellt wird, dass wirtschaftliche Entwicklung mit sozialen Standards, klimafreundlicher Industriepolitik und demokratischer Governance verbunden wird.

3.3 Digitale Sicherheit stärken

Der internationale Einsatz Deutschlands für menschliche Sicherheit muss sich auch darin zeigen, dass die eigenen Regeln und das eigene Handeln im Einklang stehen und keinen Widerspruch darstellen. Für die Prävention ist es zentral, an den eigenen Lücken zu arbeiten, damit sie nicht zum Einfallstor für autoritäre Akteure werden. Mit jeder neuen digitalen Technologie entstehen neue Schwachstellen. Doch jeder Schritt für mehr Resilienz der eigenen Systeme erschwert die Arbeit derjenigen, die sie angreifen wollen. Dafür braucht es einen konsequenten Mindeststandard für Cybersicherheit, der alle Menschen und insbesondere auch marginalisierte Gruppen und FLINTA*-Personen gleichermaßen schützt.

Konsequentes Schließen von Schwachstellen

Bis heute bleiben bekannte Schwachstellen viel zu lange offen und machen damit etliche Organisationen zum leichten Ziel von Angriffen. Um diese Schwachstellen schnellstmöglich zu schließen, braucht es ein ganzheitliches Konzept gegen hybride Bedrohungen. So war die Verabschiedung des KRITIS-Dachgesetzes zum Schutz physischer kritischer Infrastruktur längst überfällig, welches schließlich 2026 in Kraft getreten ist. Hier braucht es jetzt konsequentes Engagement, um die Sicherheitsstandards auch in der Praxis zu etablieren (Locher/Campbell 2026). Ebenso notwendig ist es, digitale und physische Sicherheit systematisch zu verschränken.

Darüber hinaus braucht es ein wirksames Schwachstellenmanagement nach dem Prinzip *Responsible Disclosure*: Wer eine Sicherheitslücke findet, meldet sie zunächst vertraulich. Hierfür muss das BSI als unabhängige Behörde weiter gestärkt werden und die Funktion einer zentralen Anlaufstelle, einer One-Stop-Agency zur Meldung von Schwachstellen, übernehmen, um diese Meldungen an föderale Stellen verteilen zu können. Nötig ist außerdem das Bekenntnis, dass Schwachstellen schnellstmöglich geschlossen werden – von Unternehmen, Industrie und Behörden gleichermaßen.

Es geht aber nicht nur um versehentliche und noch nicht geschlossene Schwachstellen. Mindestens genauso angreifbar sind sogenannte Backdoors, also Schwachstellen, die absichtlich oder auf Anordnung für Strafverfolgungsbehörden offen gelassen werden, um für die Strafverfolgung Zugang zu Daten zu ermöglichen. Ein bekanntes Beispiel ist der Staatstrojaner. Der Konflikt der Backdoors wird auch bei der umstrittenen Chatkontrolle ausgetragen: Sie würde Messenger-Dienste zwingen, private Nachrichten vor ihrer Verschlüsselung automatisch zu durchleuchten (sogenanntes Client-Side-Scanning), was die Verschlüsselung de facto aushebeln würde. Staatlich angeordnete Schwachstellen müssen dringend geschlossen werden. Denn sie führen zu einer Vielzahl von Sicherheitslücken und haben sicherheitspolitische Auswirkungen nicht nur in Deutschland, sondern auch weltweit. Stattdessen sollten Strafverfolgungsbehörden darin befähigt werden, im konkreten, anlassbezogenen Verdachts- und Verfolgungsfall gezielte Maßnahmen ergreifen zu können.

Sichere Kommunikation nach innen und außen

Die Integrität von (staatlicher) Kommunikation ist Voraussetzung politischer Handlungsfähigkeit. Sicherheitsvorfälle haben gezeigt, wie leicht vertrauliche Kommunikation kompromittiert werden kann. So wurden etwa vertrauliche bis geheime Gespräche über deutsche Waffenlieferungen an die Ukraine über ein WLAN in Singapur mitgehört, mitgeschnitten und öffentlich gemacht. Dafür muss flächendeckend in die Sicherheit unserer digitalen Systeme investiert werden. *Security by Design* muss zum Standard werden, indem die Sicherheit bei der Entwicklung und Konzeption von Systemen von Beginn an eingebunden wird. Die Infrastrukturen der Bundesregierung und des Bundestages müssen flächendeckend verschlüsselte Kommunikation ohne Sicherheitslücken garantieren.

Recht auf Verschlüsselung

Es muss auf eine konsequente Verschlüsselung gesetzt werden. Die Ampelregierung hatte sich im Koalitionsvertrag das Ziel eines gesetzlich verankerten Rechts auf Verschlüsselung gesetzt, dies jedoch nicht umgesetzt. Angesichts der diversen Angriffe auf unsere Kommunikation, Privatsphäre, Logistik und die öffentliche Meinung ist Verschlüsselung die Grundlage dafür, weiterhin Kontrolle über die eigene Kommunikation zu behalten. Verschlüsselung ist nicht nur ein „nice to have“: Mit Blick auf künftige technologische Entwicklungen – insbesondere durch Quantencomputer – muss davon ausgegangen werden, dass damit ein Großteil unserer Passwörter leicht zu knacken ist. Quantensichere Verschlüsselung ist deshalb ein Beitrag für die digitale Sicherheit der Zukunft weltweit.

Schutz der Freiheitsrechte

Investitionen in die eigene digitale Sicherheit in Deutschland und der EU finden jedoch nicht im Glashaus statt. Es hat Signalwirkung auf die wahrgenommene menschliche Sicherheit im Inneren und im Außen, ob *Backdoors* eingebaut werden, ob es Überwachungskameras im öffentlichen Raum gibt, die biometrische Daten erfassen und speichern, ob es effektive Maßnahmen gegen geschlechterbasierte digitale Gewalt gibt (Klappheck 2024) und ob Hasskriminalität klare strafrechtliche Grenzen erfährt. Davon hängt ab, wer Onlineräume nutzt oder wer sich aus diesen zurückzieht.

Derlei Entscheidungen wirken sich auch auf die Glaubwürdigkeit und das Handeln Deutschlands aus und sind Voraussetzung der eigenen diplomatischen Integrität weltweit. Deutschland kann sich nur dann glaubhaft zu Menschenrechten im digitalen Raum bekennen und ihren Schutz in der eigenen Außenpolitik erkämpfen, wenn es diese auch im Inneren wahrt. Dafür muss die Bundesregierung weiterhin eine klare Absage der Chatkontrolle im Trilog-Verfahren mit Europäischem Parlament, Europäischer Kommission und Rat der EU aufrechterhalten. Sie sollte biometrische Überwachung endgültig ausschließen und statt neuer Vorstöße zu einer anlasslosen,

flächendeckenden IP-Adressenspeicherung auf Maßnahmen setzen, die zielgerichtet im Verdachtsfall funktionieren wie etwa das *Quick-Freeze*-Verfahren, bei dem Verkehrsdaten erst bei einem konkreten Tatverdacht und auf richterliche Anordnung zeitlich begrenzt „eingefroren“ und damit zugänglich gemacht werden.

Selbst vor die Lage kommen

Digitale Außenpolitik ganzheitlich zu gestalten heißt, anzuerkennen, dass geopolitische Auseinandersetzungen, ob mit Russland, China oder jüngst auch mit den USA, zunehmend im digitalen Raum stattfinden. Das beinhaltet auch die Erkenntnis, dass Entscheidungen nach innen und außen nicht isoliert vom globalen Kontext wirken: Schwachstellen in Deutschland können immer auch zu Einfallstoren bei unseren internationalen Partnern werden. Prävention ist deshalb sicher nicht der einzige, aber ein zentraler Pfeiler digitaler Außenpolitik. Deshalb muss Deutschland zuerst bei den eigenen Lücken ansetzen.

Einseitige Abhängigkeiten in kritischen Infrastrukturen, Lieferketten und digitalen Basisdiensten müssen abgebaut und die digitale Resilienz muss erhöht werden, damit Deutschland und Europa auch in geopolitisch angespannten Situationen handlungsfähig bleiben. Zudem sollten souveräne digitale Anbieter und Lösungen gezielt gestärkt werden, etwa durch Investitionen in Open Source, öffentliche Aufträge, vorkommerzielle Auftragsvergabe und eine gestärkte Sovereign Tech Agency. Dabei müssen digitale Sicherheit und Freiheitsrechte konsequent geschützt werden. Denn Verschlüsselung, geschlossene Sicherheitslücken und eine geschützte digitale Öffentlichkeit sind Grundvoraussetzungen für Sicherheit, Vertrauen und internationale Glaubwürdigkeit. Investition in die Vorsorge digitaler Systeme muss daher ein leitendes Prinzip digitaler Außenpolitik sein.

Literaturverzeichnis

Bensinger, Viola (2025): Cloud-Switching gemäß EU-Data Act: Auswirkungen für IaaS-, PaaS- und SaaS-Anbieter; in: gtlaw.com; 25.9.2025, https://www.gtlaw.com/de/insights/2025/9/cloud-switching-under-the-eu-data-act, Zugriff 2.6.2026

Beuth, Patrick (2021): Log4J Sicherheitslücke: Wie löscht man ein brennendes Internet?, in: Der Spiegel, 13.12.2021, https://www.spiegel.de/netzwelt/web/log4j-sicherheitsluecke-wie-loescht-man-ein-brennendes-internet-a-27729847-8e28-4187-b4a2-468a45137fb4, Zugriff 2.6.2026

Briegleb, Volker (2021): Log4j. Angriff auf Netz des belgischen Verteidigungsministeriums; in: heise online, 20.12.2021, https://www.heise.de/news/Log4j-Angriff-auf-Netz-des-belgischen-Verteidigungsministeriums-6300519.html, Zugriff 2.6.2026

BSI (2021): BSI-Cyber-Sicherheitswarnung: Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228); in: bsi.bund.de; 17.12.2021, https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=10, Zugriff 2.6.2026

BSI (2025): Zusammenfassung und Bewertung. BSI Lagebericht 2025; in: medien.bsi.bund.de; https://medien.bsi.bund.de/lagebericht/de/zusammenfassung-und-bewertung/, Zugriff 2.6.2026

BSI (o. D.): Cyber Resilience Act; in: bsi.bund.de; https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act.html, Zugriff 2.6.2026

Bundesministerium des Innern (2024): Kurzmeldung: Stärkung der Sicherheit und technologischen Souveränität der deutschen 5G-Mobilfunknetze: Bundesregierung schließt Verträge mit Telekommunikationsunternehmen; in: bmi.bund.de; 11.7.2024, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2024/07/5g.html, Zugriff 2.6.2026

CDU/CSU/SPD (2025): Koalitionsvertrag zwischen CDU, CSU und SPD – Verantwortung für Deutschland. 21. Legislaturperiode des Deutschen Bundestags, Berlin, https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag2025_bf.pdf, Zugriff 2.6.2025

De Pommereau, Isabelle (2017): World's first „data embassy"; in: dw.com; 6.8.2017, https://www.dw.com/en/estonia-buoys-cyber-security-with-worlds-first-data-embassy/a-39168011#:~:text=Now,%20against%20the%20backdrop%20of,confidential%20data%20will%20be%20stored, Zugriff 2.6.2026

Der Beauftragte der Bundesregierung für Informationstechnik/IT Planungsrat/IT Rat (2020): Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung. Eckpunkte – Ziel und Handlungsfelder; in: Bundesministerium für Inneres; 31.3.2020, https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-19_Entscheidungsniederschrift_Umlaufverfahren_Eckpunktepapier.pdf, Zugriff 2.6.2026

Die Bundesregierung (2023): Nationale Sicherheitsstrategie, in: Auswärtiges Amt (Hrsg.), https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf, Zugriff 2.6.2026

Digital Austria (2025). Europa unterzeichnet gemeinsame Erklärung zur Europäischen Digitalen Souveränität – Österreich setzt Impulse in Berlin; in: digitalaustria.gv.at; https://www.digitalaustria.gv.at/wissenswertes/news/news-77.html, Zugriff 1.3.2026

E-Estonia (o. D.): e-Governance; in: e-estonia.com; https://e-estonia.com/solutions/e-governance/data-embassy/#:~:text=Data%20Embassy, Zugriff 2.6.2026

Eisenegger, Mark (2021): Dritter, digitaler Strukturwandel der Öffentlichkeit als Folge der Plattformisierung; in: Eisenegger, Mark et al. (Hrsg.): Digitaler Strukturwandel der Öffentlichkeit, Mediensymposium, Springer VS, Wiesbaden, S. 17–39, https://doi.org/10.1007/978-3-658-32133-8_2, Zugriff 2.6.2026

Fokuhl, Josefine/Heide, Dana et al. (2025): Infrastruktur: Koalition verschärft Sicherheitsanforderungen an 5G-Netz; handelsblatt.com; 6.11.2025, https://www.handelsblatt.com/politik/deutschland/infrastruktur-koalition-verschaerft-sicherheitsanforderungen-an-5g-netz/100171972.html, Zugriff 2.6.2026

FOTI Future of Technology Institute (2026): Cloud Defence: An exposed European flank, 2026; in: futureinstitute.tech; https://futureinstitute.tech/assets/doc/FOTICloudDefenceReport26.pdf, Zugriff 2.6.2026

Fraktionsvorstand Bündnis 90/Die Grünen im Deutschen Bundestag (2025): Fraktionsvorstandsbeschluss: Sicherheitsoffensive gegen hybride Bedrohungen; in: Bundestagsfraktion Bündnis 90/Die Grünen; 2.9.2025, https://www.gruene-bundestag.de/unsere-politik/fachtexte/fraktionsvorstandsbeschluss-sicherheitsoffensive-gegen-hybride-bedrohungen/, Zugriff 2.6.2026

Frühwirth, Lea/Smirnova, Julia (2024): Fortsetzung folgt. Die prorussische Desinformationskampagne Doppelgänger in Deutschland; in: cemas.io; 19.11.2024, https://cemas.io/publikationen/fortsetzung-folgt-doppelgaenger/, Zugriff 2.6.2026

Hausding, Götz (2025): „Soziale Medien sind kritische Infrastruktur“; in: das-parlament.de; 16.1.2025, https://www.das-parlament.de/wirtschaft/digitales/soziale-medien-sind-kritische-infrastruktur, Zugriff 2.6.2026

Kessler, Manfred (2025): Sabotagegefahr bei Photovoltaik. Könnte China deutsche PV-Anlagen abschalten?; in: zdfheute.de; 8.2.2025, https://www.zdfheute.de/wirtschaft/photovoltaik-windkraft-china-internet-zugriff-blackout-100.html, Zugriff 2.6.2026

Klappheck, Katharina (2024): Was bedeutet feministische Cybersecurity?; in: gwi-boell.de; 30.8.2024, https://www.gwi-boell.de/de/2024/08/30/was-bedeutet-feministische-cybersecurity, Zugriff 2.6.2026

Knop, Dirk (2021): Webseite des Bundesfinanzhofs nach Log4j-Angriff offline; in: heise online, 17.12.2021, https://www.heise.de/news/Webseite-des-Bundesfinanzhof-nach-Log4j-Angriff-offline-6298217.html, Zugriff 2.6.2026

Kolain, Michael/Kipker, Dennis-Kenji (2026): Rechtliche Risiken bei Cloud-Computing-Nutzung, in: <kes> Informationssicherheit, 2026#1, 24.2.2026

Körömi, Csongor (2025): US curtails Ukraine access to satellite imagery; in: politico.eu; 7.3.2025, https://www.politico.eu/article/

us-satellite-company-maxar-cuts-off-ukraine-access-imagery-report-says/, Zugriff 2.6.2026

Locher, Nina/Campbell, Loyle (2026): Lehren aus dem Krieg im Nahen Osten; in: dgap.org, Erstveröffentlichung in: table.media; 13.4.2026, https://dgap.org/de/forschung/publikationen/lehren-aus-krieg-im-nahen-osten, Zugriff 2.6.2026

Münch, Holger (2024): „Wir brauchen eine Zeitenwende der inneren Sicherheit"; in: Der Spiegel; 20.12.2024, https://www.spiegel.de/panorama/justiz/bka-chef-holger-muench-wir-brauchen-eine-zeitenwende-der-inneren-sicherheit-a-82ec4d88-f773-473c-9aed-af7a1ce92903, Zugriff 1.6.2026

Paulus, Alexandra/Voelsen, Daniel (2025): Digitale Abhängigkeit: Welchen Einfluss die Technologie- und Cyberpolitik der USA auf Europa hat, in: swp.de, SWP-Podcast 2025/P 21, 4.9.2025, https://www.swp-berlin.org/publikation/digitale-abhaengigkeit-welchen-einfluss-die-technologie-und-cyberpolitik-der-usa-auf-europa-hat, Zugriff 10.6.2026

Poirier, Clémence (2025): Orbit of Dependence: Ukraine's Space Challenge; in: CSS Analyses in Security Policy, No. 361, https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse361-EN.pdf, Zugriff 2.6.2026

Reuter, Markus/Köver, Chris (2019): Gute Laune und Zensur, in: netzpolitik.org, 23.11.2019, https://netzpolitik.org/2019/gute-laune-und-zensur/, Zugriff 1.6.2026

Shalal, Andrea/Roulette, Joey (2025): Exclusive: US could cut Ukraine's access to Starlink internet services over minerals, say sources; in: Reuters; 23.2.2025, https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/, Zugriff 2.6.2026

Sovereign Tech Agency. (o. D.): Sovereign Tech Agency; https://www.sovereign.tech/de, Zugriff 2.6.2026

Die Autor*innen

Nina Locher ist Policy Fellow für Integrierte Sicherheit und Resilienz im Zentrum für Sicherheit & Verteidigung der Deutschen Gesellschaft für Auswärtige Politik (DGAP). Fokus ihrer Arbeit sind innere und äußere Sicherheit, gesellschaftliche Resilienz und Gesamtverteidigung. Zuvor leitete sie das Team Cybersicherheitspolitik bei der Gesellschaft für Informatik. Von 2022 bis 2025 war sie Büroleiterin eines Abgeordneten im Deutschen Bundestag und verantwortete den Auswärtigen, Digital- und EU-Ausschuss. Davor arbeitete sie in verschiedenen Positionen bei der Heinrich-Böll-Stiftung. Sie hat einen Doppelmaster in Public Administration und Public Policy von der LSE und Hertie School.

Tobias B. Bacherle ist Germany Senior Lead beim FOTI (Future of Technology Institute), einem europäischen Thinktank für digitale Märkte, offene Tech-Ökosysteme und digitale Souveränität. Der Politikwissenschaftler verbindet Expertise in Technologiepolitik, internationalen Beziehungen und europäischer Digitalregulierung. Er war Mitglied des 20. Deutschen Bundestags und arbeitete im Auswärtigen Ausschuss und im Ausschuss für Digitales an der Schnittstelle von Geo- und Digitalpolitik. Zuvor war er für ein Mitglied des Europäischen Parlaments und als freier Campaigner tätig.

Impressum

Herausgeberin: Heinrich-Böll-Stiftung, Schumannstraße 8, D-10117 Berlin

Fachkontakt: Sofie Stoffel, Referat Außen- und Sicherheitspolitik, stoffel@boell.de

Layout: Sebastian Langer, feinkost Design, www.feinkost-design.de

Erscheinungsort: www.boell.de

Erscheinungsdatum: Juni 2026

Covermotiv: IMAGO/alimdi

Weitere Publikationen zum Download unter: www.boell.de/publikationen