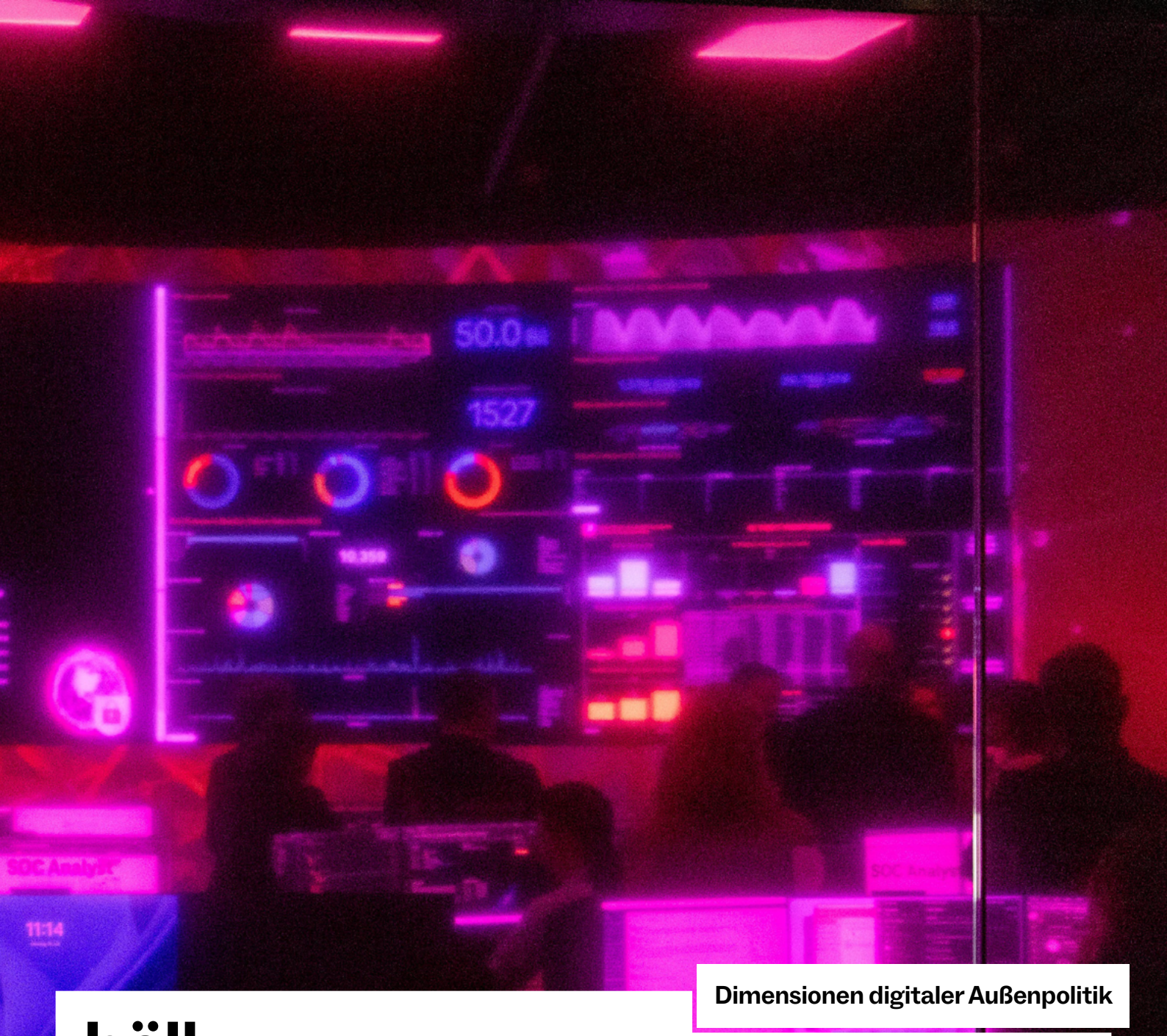


Dimensionen digitaler Außenpolitik

böllpaper

Teil 3: Digitale Außenpolitik international gestalten

Multilaterale Koalitionen für eine souveräne digitale Ordnung

Nina Locher und Tobias B. Bacherle

Teil 3:
Digitale Außenpolitik international gestalten

Multilaterale Koalitionen für eine souveräne digitale Ordnung

Ein Policy Paper von Nina Locher und Tobias B. Bacherle

HEINRICH BÖLL STIFTUNG

Inhalt

Zusammenfassung 4

1 Der globale Kontext digitaler Fragen 6

2 Das internationale Regelwerk für den digitalen Raum 8

3 Das internationale Regelwerk durch Engagement und Haltung stärken 10

3.1 Deutsches und europäisches Engagement für ein starkes Regelwerk der VN 10

3.2 Internationale Erklärungen konkret umsetzen 11

3.3 Content Credentials international standardisieren und das Engagement in Standardisierungsprozessen stärken 12

4 Kooperationen und Bündnisse für den digitalen Raum 13

5 Gemeinsam handeln und Koalitionen aufbauen 15

5.1 Internationaler Informationsaustausch: Frühwarnsysteme für hybride Bedrohungen 15

5.2 Infrastruktur: Ein multilaterales Bündnis für souveräne Satellitenkommunikation 16

5.3 Digitale Innovation: Internationale Datenmärkte und AI Coalition 17

5.4 Internationale Zusammenarbeit: Digitale Außenpolitik global gerecht gestalten 18

6 Fazit: Ein Maßnahmenpaket für eine global ausgerichtete digitale Außenpolitik 20

Literaturverzeichnis 21

Die Autor*innen 24

Impressum 24

Zusammenfassung

Digitale Außenpolitik umfasst nicht nur Prävention und Reaktion. Sie kann auch die zukünftigen Rahmenbedingungen der globalen digitalen Governance maßgeblich mitgestalten. In diesem dritten Policy Paper der Reihe „Dimensionen digitaler Außenpolitik“ arbeiten die Autor*innen heraus, in welchen Räumen dies entschieden wird. Eine zentrale Rolle spielen hier die Vereinten Nationen (VN): In ihren Gremien treffen geopolitische Interessen aufeinander. Zugleich werden dort die globalen Rahmenbedingungen für den digitalen Raum und insbesondere dessen Regulierung gesetzt und somit auch die Regeln, die für Staaten gelten. Dazu zählen sowohl verbindliche Konventionen als auch freiwillige Normen.

Staaten wie Russland und China haben lange vor Deutschland erkannt, dass sie die VN nutzen können, um die globale digitale Governance im eigenen Interesse zu prägen. Deutschland sollte deshalb die eigene Rolle auf VN-Ebene deutlich ausbauen und gemeinsam mit der EU das internationale Regelwerk durch aktives Engagement und eine klare Haltung stärken. Dabei könnte Deutschland als führender Akteur insbesondere folgende Vorhaben in VN-Prozessen vorantreiben: Erstens könnte Deutschland das VN-Regelwerk stärken, indem es die Umsetzung der VN-Cybercrime-Konvention kritisch begleitet und sich für ein völkerrechtlich bindendes Abkommen zur Begrenzung letaler Autonomer Waffensysteme (LAWS) einsetzt; zweitens könnte die Bundesregierung die konkrete Umsetzung internationaler Erklärungen anstoßen, etwa durch einen Umsetzungsplan gegen Internetsperren (Internet Shutdowns) im Rahmen der Erklärung zur Zukunft des Internets; und drittens könnte sie Content Credentials international beispielsweise im Rahmen der Internet Engineering Task Force (IETF) standardisieren sowie das deutsche und europäische Engagement in Standardisierungsprozessen stärken.

Auch über das VN-Regelwerk hinaus sind internationale Koalitionen und Partnerschaften entscheidend, um in Bündnissen digitale Innovationen anzustoßen, gemeinsame Abhängigkeiten zu verringern, Diversifizierung auszubauen und digitale Gefahren schneller zu erkennen. Hierfür sollte sich Deutschland für ein internationales Frühwarnsystem für Cybersicherheit und gegen Foreign Information Manipulation and Interference (FIMI) einsetzen, um durch einen schnellen Informationsaustausch die frühzeitige Erkennung digitaler Angriffe sowie Warnungen, Detektion und gemeinsame Reaktionen zu ermöglichen. So können Staaten und andere Akteure die verfügbaren Informationen nutzen, um rechtzeitig zu reagieren. Für ein multilaterales Bündnis zum Aufbau souveräner Satellitenkommunikation braucht es ein klares internationales Bekenntnis, konsequentes Engagement und den Mut, nationale wirtschaftliche Interessen auf deutscher wie europäischer Seite zurückzustellen.

Zudem sollte Deutschland mit weiteren Partnern eine Organisation für eine AI Coalition gründen, um einen verbindlichen, multilateralen Rahmen aufzubauen, der Rechenkapazitäten, Kompetenzen und Kapital bündelt und eine faire Teilhabe an der

Wertschöpfung sicherstellt. Entscheidend ist dabei eine gleichberechtigte Zusammenarbeit mit Ländern des Globalen Südens, die gemeinsame Potenziale nutzt, die Grenzen natürlicher Ressourcen respektiert und einen wertebasierten, demokratischen und gleichberechtigten internationalen Raum stärkt.

1 Der globale Kontext digitaler Fragen

Für die Gestaltung des digitalen Raums bleibt eine zentrale Prämisse: Der digitale Raum macht nicht an nationalen Grenzen halt. Ob technische Innovationen, Sicherheitslücken, die Verwaltung digitaler Debattenräume oder Entscheidungen global agierender Tech-Konzerne: Die Auswirkungen der digitalen Transformation betreffen Akteure in verschiedenen Ländern zwar unterschiedlich, sind aber global eng miteinander verflochten. Aus guten Gründen gibt es seit Jahren globale Multistakeholder-Ansätze wie das Internet Governance Forum (IGF) der VN oder die Internet Corporation for Assigned Names and Numbers (ICANN), die das Domain Name System (DNS) global verwaltet. Sie binden zahlreiche zivilgesellschaftliche, wirtschaftliche und politische Akteure ein. Auch wenn die Macht nicht immer ausgewogen verteilt ist, ist es ihr Ziel, einer Machtkonzentration vorzubeugen und verschiedene Interessen in Entscheidungs- und Diskussionsprozesse einzubeziehen.

Eine gut koordinierte und klare digitale Außenpolitik kann auf internationaler Ebene maßgeblich beeinflussen, wie die Rahmenbedingungen für die Entwicklung und das Zusammenleben im digitalen Raum aussehen. Schließlich werden in internationalen Gremien und Organisationen weitreichende, international geltende Regeln und Normen erlassen, einige davon verbindlich. Hier entsteht das globale Rahmenwerk, das sich anschließend in nationale Gesetze und die Governance des digitalen Raums übersetzt.

Autoritäre Regime haben erkannt, dass für ihre Heimatmärkte vorteilhafte Standards ihnen nicht nur wirtschaftlich nutzen, sondern diese auch dazu dienen können, politische Ziele durchzusetzen. Insbesondere digitale Normen und Regelwerke sind dabei immer wieder Angriffen des digitalen Autoritarismus ausgesetzt: In entsprechenden Verhandlungen versuchen autoritäre Kräfte strategisch, Unterdrückungstechniken zu legitimieren und geltendes internationales Recht sowie den Schutz der Menschenrechte aufzuweichen (Bacherle 2024).

Gemeinsame Interessen in der digitalen Außenpolitik können zugleich neue Allianzen ermöglichen. Ein Beispiel, das an Bündnisse in der internationalen Klimapolitik erinnert, ist die Freedom Online Coalition, die Akteure und Staaten zusammenbringt, die sich für Menschenrechte im digitalen Raum einsetzen. Dem Bündnis zur „Koordinierung diplomatischer und zivilgesellschaftlicher Bemühungen zum Schutz der Menschenrechte bei der Regulierung neuer Technologien“ (Niazi et al. 2026: 238) gehören neben zahlreichen europäischen Staaten unter anderem auch die Mongolei, Armenien, Kenia und die Malediven an. Abkommen über digitale Marktzugänge, Investitionen in digitale Infrastruktur, Kapazitätsaufbau sowie die Zusammenarbeit mit aufstrebenden Digitalwirtschaften können Partnerschaften zudem weiter stärken – auch Bündnisse, die in der konventionellen Diplomatie und Außenpolitik so nicht

möglich wären. Das heißt: Strategisch und zielführend gestaltet, kann digitale Außenpolitik den Handlungsspielraum der Diplomatie erweitern.

Digitale Außenpolitik ist somit ein unverzichtbarer Teil einer ganzheitlichen Außenpolitik. Sie ermöglicht es, gesellschaftliche, wirtschaftliche, rechtliche und politische Rahmenbedingungen auf internationaler Ebene mitzugestalten. Außenpolitik im 21. Jahrhundert kann die digitalen Räume nicht mehr ignorieren.

Eine aktive digitale Außenpolitik baut internationale Allianzen und vertritt europäische und deutsche Interessen sowie eine klare Position für einen menschzentrierten digitalen Raum – sowohl gegenüber anderen Staaten als auch anderen Akteuren wie großen Digitalkonzernen. Europa braucht hierfür klare Zuständigkeiten und eine gute Koordination, die außenpolitische und digitalpolitische Expertise zusammenführt (Barker 2020).

2 Das internationale Regelwerk für den digitalen Raum

Mit Blick auf die Anwendung des Völkerrechts im digitalen Raum stehen sich zwei konkurrierende Haltungen gegenüber: Während vermehrt autoritäre Staaten wie Russland vertreten, das Völkerrecht und seine Normen seien im digitalen Raum nicht einfach zu übernehmen und anwendbar (und können entsprechendes Verhalten daher nicht ahnden), setzen sich andere Staaten dafür ein, bestehende völkerrechtliche Normen auch für den digitalen Raum auszulegen und anzuwenden (Weber 2025: 2). Mit dem Multilateralismus-Antrag hat sich der Deutsche Bundestag hierzu im Jahr 2024 klar für die zweite Position ausgesprochen.

Aufgrund der rasanten technologischen Entwicklungen bestehen und entstehen dennoch weiterhin Lücken im multilateralen Regelwerk, die es zu schließen gilt – von Cybersicherheit über Plattformpolitik und Künstliche Intelligenz (KI) bis hin zu Standardisierung und Internet Governance. 2023 richteten die Vereinten Nationen etwa das Multistakeholder High-Level Advisory Body on AI ein, das mitunter mit dem Intergovernmental Panel on Climate Change (IPCC) der VN verglichen wurde. Ziel des Gremiums war es, globale Fragen der KI-Governance zu bearbeiten und am Global Digital Compact mitzuwirken, der globale und menschenrechtliche Fragen der Digitalisierung adressiert. Dieser wurde 2024 im Rahmen des Summit of the Future der VN beschlossen. Hieraus gingen unter anderem das internationale wissenschaftliche KI-Panel und ein globaler Dialog zur KI-Governance hervor, welche seit 2026 an ähnlichen Themen arbeiten wie zuvor der High-Level Adisory Body on AI (vgl. Kleinwächter 2026). Welche politische Wirkung sie entfalten und welche Rolle der Global Digital Compact spielen wird, ist jedoch noch offen. Auch abseits der VN-Ebene entstehen internationale Foren für die Zusammenarbeit im Bereich KI, wie der AI Impact Summit in Indien 2026 oder das Netzwerk der AI Safety Institute.

Aufgrund der globalen Bedeutung digitaler Fragen ist der digitale Raum ein Schauplatz des globalen Systemwettbewerbs und geopolitischer Dominanz geworden. Autoritäre Staaten haben dies früher als Deutschland und die EU für sich genutzt. So investieren etwa Russland und China viele Ressourcen in VN-Gremien zu digitalen Fragen. Hierbei geht es zum einen um das entsandte Personal zu wichtigen VN-Konferenzen. Von 2015 bis 2022 stellte China mit Houlin Zhao den Generalsekretär der International Telecommunication Union (ITU) (Klotz 2023: 561). Nach einer umfangreichen Kampagne bewarb sich 2022 ein russischer Kandidat auf den Posten des Generalsekretärs der ITU, einer völkerrechtlich verankerten Sonderorganisation der VN, die sich mit den technischen Aspekten von Funk und Telekommunikation befasst (Komaitis/Sherman 2022). Darüber hinaus bringt sich China gezielt mit Expertise, Wissenschaft und weiterem Personal mit geostrategischen Interessen in diversen Standardisierungsprozessen ein (Rühlig 2022: 13f.), während Deutschland und Europa sich lange auf den historisch gewachsenen, eigenen Einfluss in Standardisierungsgremien verlassen und erst

langsam die Notwendigkeit erkannt haben, den politisch und geopolitisch motivierten Aktivitäten insbesondere Chinas auf internationaler Bühne strategisch entgegenzutreten (Barker/Hagebölling 2022: 7).[1]

Zum anderen zeigt sich das gezielte Engagement autoritärer Staaten auch in VN-Gremien und Initiativen für eigene Resolutionen und völkerrechtlich bindende Verträge. Die 2024 von der VN-Generalversammlung verabschiedete Cybercrime-Konvention geht vor allem auf eine russische Initiative aus dem Jahr 2017 zurück – mit dem Ziel, auf Grundlage möglichst weit gefasster Definitionen von Cyberkriminalität die grenzüberschreitende Strafverfolgung unter anderem eigener Kritiker*innen zu ermöglichen (Bacherle 2024). Darüber hinaus investiert China im Rahmen seiner Seidenstraßen-Initiative gezielt in digitale Projekte, auch um chinesische Produkte und Standards zu verbreiten (Riedel 2023: 8).

1 2018 entsandte beispielsweise Deutschland den zuständigen Referatsleiter für das Policy Statement bei der ITU-Plenipotentiary Conference in Dubai, während für China ein Minister und für Russland ein stellvertretender Minister sprachen (ITU 2018).

3 Das internationale Regelwerk durch Engagement und Haltung stärken

Internationale Rahmenbedingungen geben der Politik für neue Technologien Orientierung und können Grenzen setzen. Deutschland sollte hier als führender Akteur eine aktive Rolle übernehmen und auf VN-Ebene die menschenrechtskonforme Umsetzung der Cybercrime-Konvention kritisch begleiten sowie ein völkerrechtlich bindendes Abkommen zur Begrenzung Letaler Autonomer Waffensysteme vorantreiben. Auch bei nichtverbindlichen Beschlüssen, etwa der Erklärung zur Zukunft des Internets, sollte Deutschland auf einen konkreten Umsetzungsplan, besonders zur Unterbindung von Internetsperren (Internet Shutdowns), hinwirken. In internationalen Standardisierungsprozessen sollte sich Deutschland dafür einsetzen, die in Artikel 50 des AI Acts geregelte Kennzeichnungspflicht mithilfe der in Teil 2 dieser Reihe beschriebenen Content Credentials zu einem globalen Standard zu entwickeln (Bacherle/Locher 2026: 12).

3.1 Deutsches und europäisches Engagement für ein starkes Regelwerk der VN

Die rasante technologische Entwicklung fordert die internationalen und multilateralen Normen heraus. Während völkerrechtliche Abkommen für die analoge Welt ein gemeinsames Rechtsverständnis geschaffen haben und dort Anwendung finden, muss ihre Anwendung im digitalen Raum und im Cyberraum erst noch erkämpft werden. Ebenso hat die Geschwindigkeit technologischer Innovation dazu geführt, dass multilaterale Bündnisse hinterherhinken: So war es bis heute nicht möglich, ein völkerrechtlich bindendes Abkommen zur Begrenzung von LAWS abzuschließen.

Deutschland und die EU sollten hier gemeinsam mit internationalen Partnern mit klarem Beispiel vorangehen und eine Führungsrolle übernehmen. Zum einen sollte sich die Bundesregierung weiter aktiv für die Weiterentwicklung und Gestaltung des VN-Regelwerks im digitalen Raum einsetzen. Deutschland könnte sich zum Beispiel in der Umsetzung der verabschiedeten VN-Cybercrime-Konvention aktiv einbringen, um die Konvention an klaren Menschenrechtskriterien auszurichten und der Überwachung Grenzen zu setzen. Trotz großer Widerstände – besonders seitens zivilgesellschaftlicher Organisationen – wurde 2024 die VN-Cybercrime-Konvention beschlossen. Das auf eine russische Initiative zurückgehende Abkommen bekämpft Cyberkriminalität jedoch nur auf den ersten Blick. Stattdessen läuft die Konvention aktuell Gefahr, ohne transparente Verfahren eine grenzüberschreitende Abfrage personenbezogener Daten zu ermöglichen, wodurch kritische Stimmen in autoritären Staaten einfacher verfolgt werden können (Bacherle 2024).

Zum anderen sollte sich Deutschland für ein international verbindliches Abkommen zu LAWS starkmachen. 2025 verabschiedeten die VN eine weitere Resolution, die die Dringlichkeit eines gemeinsamen Abkommens erneut betont. Der VN-Generalsekretär forderte, ein solches Abkommen 2026 zu erreichen (United Nations General Assembly 2025). Eine führende Rolle könnte Deutschland auf der siebten Überprüfungskonferenz der Convention on Certain Conventional Weapons (CCW) (vom 16. bis zum 20. November 2026 in Genf) übernehmen, indem es auf Grundlage des erarbeiteten Textentwurfs ein Verhandlungsmandat für ein rechtlich bindendes CCW-Zusatzprotokoll vorantreibt. Gegenüber skeptischen Staaten wie den USA, China und Indien sollte Deutschland als einflussreiches Land zugleich aktiv für mindestens eine politisch (wenn auch nicht rechtlich) bindende Regelung eintreten.

3.2 Internationale Erklärungen konkret umsetzen

Multilaterale Normen werden nicht nur durch die Prägung des VN-Regelwerks gestärkt, sondern auch durch Allianzen und Bündnisse gleichgesinnter Staaten. Sie dienen der Stärkung eines wertebasierten Umgangs mit dem digitalen Raum und dem Schutz digitaler Menschenrechte. Mehrere solcher Bündnisse wurden in den vergangenen Jahren geschlossen: Die Erklärung zur Zukunft des Internets (Declaration for the Future of the Internet) wurde seit 2022 von 70 Staaten unterzeichnet, und der Freedom Online Coalition (FOC) gehören mehr als 40 Regierungen an – ein Bündnis, das sich seit Jahren für digitale Menschenrechte und ein freies, offenes Internet einsetzt (European Commission 2022).

In einer Zeit, in der Multilateralismus zunehmend unter Druck gerät, sollte umso stärker darauf gesetzt werden, mit gemeinsamen Vereinbarungen ein wertebasiertes Vorgehen im digitalen Raum zu fördern und Menschen- und Frauenrechte wirksam zu schützen. Dies ist umso wichtiger, als die USA Anfang 2026 aus mehreren internationalen digitalpolitischen Abkommen ausgetreten sind – darunter der Freedom Online Coalition und dem Global Forum on Cyber Expertise (The White House 2026). Der sogenannte WSIS+20-Prozess, der im Jahr 2025 Umsetzung und Wirkung des World Summit on the Information Society (WSIS) der letzten 20 Jahre überprüft hat, ist dabei als Erfolg zu werten: Er hat das Mandat des Internet Governance Forums (IGF) verstetigt und den Multistakeholder-Ansatz bekräftigt. Deutschland hat mit der Ankündigung einer Finanzierung des IGF in New York in Höhe von einer Million Euro ein Zeichen gesetzt. Vision des WSIS ist eine menschzentrierte, inklusive und entwicklungsorientierte Informationsgesellschaft.

Deshalb sollte die Bundesregierung zusätzlich zur Stärkung von VN-Regelwerken Bündnisse und Koalitionen mit gleichgesinnten – sogenannten likeminded – Staaten wie Kanada, Kenia, Mexiko oder der Republik Korea ausbauen und pflegen. Dies gilt umso mehr, als angesichts der Machtverhältnisse in den Vereinten Nationen viele Beschlüsse faktisch blockiert sind.

Ein zentraler Ansatzpunkt wäre, bereits bestehende Beschlüsse wie die Erklärung zur Zukunft des Internets nun konkret in Handlungen zu übersetzen und umzusetzen. In der gemeinsamen Absichtserklärung werden gemeinsame Prinzipien vereinbart – darunter der Verzicht auf staatlich verordnete Internetsperren sowie auf vollständige oder teilweise Einschränkungen des Internetzugangs und das weltweite Eintreten für diese Prinzipien (European Commission 2022). Die Bundesregierung könnte hier eine leitende Rolle übernehmen und einen konkreten Umsetzungsplan zur Erklärung zur Zukunft des Internets anstoßen.

3.3 Content Credentials international standardisieren und das Engagement in Standardisierungsprozessen stärken

Mit der KI-Verordnung ist die Europäische Union bei der Regulierung von Künstlicher Intelligenz vorangegangen. Während Umfang und Logik der Regulierung Gegenstand von Debatten sind, gilt der AI Act mal mehr – wie in Brasilien – und mal weniger – wie in Südkorea – als Vorbild für andere Länder. Viel beachtet ist jedoch die im August 2026 in Kraft getretene Verpflichtung nach Artikel 50 der KI-Verordnung, KI-generierte Inhalte maschinenlesbar zu kennzeichnen. Wie bereits in Teil 2 dieser Reihe erläutert, braucht es hierfür einen einheitlichen Standard, der Informationen über die Entstehung von Content auch plattformübergreifend erhält: sogenannte Content Credentials (Bacherle/Locher 2026: 12f.). Dieser Standard sollte nicht nur in Europa durchgesetzt, sondern auch international etabliert werden. Einen solchen Prozess könnte die Internet Engineering Task Force (IETF) vorantreiben. Alternativ könnte die Coalition for Content Provenance and Authenticity (C2PA) als Standardisierungsgremium gestärkt werden oder ihren Standard in Prozesse der IETF oder der International Organization for Standardization (ISO) einbringen.

Deutschland und Europa sollten sich für den Erhalt und die Stärkung von globalen Standardisierungsgremien und -prozessen einsetzen. Zentral ist, die europäische Präsenz dort zu stärken, ohne die Prozesse weiter zu politisieren. Hierfür sollten Förderprogramme wie WIPANO (Wissens- und Technologietransfer durch Patente und Normen) ausgebaut werden. Dieses Programm unterstützt kleine und mittlere Unternehmen (KMU) dabei, sich in Standardisierungsgremien einzubringen (BMWE 2026). Aber auch in den Ausbildungen sollten Standardisierungskompetenzen stärker vermittelt werden (Rühlig 2023). Außerdem könnten nationale Pooling-Systeme geschaffen werden, über die KMU sich niedrigschwellig und ressourcenarm an laufenden Standardisierungsverfahren beteiligen, eigene Positionen einbringen und sich über den aktuellen Stand informieren können. Unabhängige Koordinator*innen, beispielsweise aus dem akademischen Bereich, könnten die Positionen der Unternehmen bündeln und an den Standardisierungsverfahren und Gremien teilnehmen, um die gesammelten Positionen dort einzubringen und zugleich Erkenntnisse zu den Standardisierungsverfahren zurückzuspiegeln.

4 Kooperationen und Bündnisse für den digitalen Raum

Der digitale Raum ermöglicht und erfordert internationale Kooperation: Informationen über Cybersicherheitslücken, Patches und Updates müssen schnell überall dorthin gelangen, wo die betreffende Software eingesetzt wird. Zugleich werden Internetinfrastrukturen gemeinsam genutzt und teilweise global verwaltet, während Standards und Protokolle weltweit einheitlich sein und koordiniert weiterentwickelt werden müssen. Dadurch sind die Sicherheitsinteressen im digitalen Raum eng miteinander verflochten (Policy Paper 1 der Reihe „Dimensionen digitaler Außenpolitik“, Locher/Bacherle 2026: 12). Aber auch der Zugang zu proprietärer Innovation kann durch Zusammenarbeit besser erschlossen werden. Hier können globale Partnerschaften den Aufbau von Kapazitäten und den Zugang zu Infrastruktur ermöglichen, oft Hand in Hand mit sicherheitspolitischem Koalitionsaufbau und dem Zugang zu europäischen Wertschöpfungsketten.

Gemeinsam genutzte digitale Infrastruktur, gerade bei Open-Source-Programmen und -Code, führt zu gemeinsamen Sicherheitsinteressen. Um diese zu wahren und Sicherheitslücken zu schließen, ist eine enge internationale Kooperation notwendig. Viele dieser Kooperationsformate sind bislang stark von den USA abhängig, die umfangreiche Informationen über Cybersicherheitsvorfälle und andere Bedrohungen beisteuern und in internationalen Gremien oder bilateralen Kooperationen anderen Nationen zur Verfügung stellen (Paulus 2025). Seit Beginn der zweiten Präsidentschaft Donald Trumps zeigt sich zunehmend, wie fragil Bündnisse mit den USA geworden sind. Der kanadische Premierminister Mark Carney hat diese Entwicklung in Davos im Januar 2026 eindrücklich beschrieben. Einseitige Abhängigkeiten von den USA werden dadurch zu einem Sicherheitsrisiko. Deutschland kann weder in multilateralen Foren noch in bilateraler Zusammenarbeit länger mit einem automatischen, privilegierten Sonderstatus aufgrund der transatlantischen Partnerschaft rechnen. Das bedeutet, dass sich Deutschland und Europa auch im Bereich der Cybersicherheit und weiteren digitalpolitischen Interessen verstärkt themenbezogene Koalitionen aufbauen sollten. Darin liegt zugleich eine Chance auf neue Partnerschaften. Europa erkennt erst seit Kurzem die Notwendigkeit, seine strategische Souveränität zu stärken und digitale Abhängigkeiten möglichst einzugrenzen – viele Mittel- und Kleinstaaten verfolgen dieses Ziel bereits wesentlich länger. Auf dieser Grundlage können und müssen nun neue Kooperationen und Frühwarnsysteme entstehen.

Digitale Infrastruktur ist fast immer eine geteilte Infrastruktur. Das gilt sowohl für Open-Source-Basiskomponenten, die in proprietärer Software genutzt werden, als auch für physische Infrastruktur. Oft wird diese Infrastruktur in irgendeiner Form gemeinsam verwaltet, etwa durch offene Multistakeholder-Ansätze oder – wie beim deutschen DE-CIX, dem Betreiber unter anderem des Frankfurter Internetknotens – durch eine Art industriell-kollektiver Governance durch den eco – den Verband der

Internetwirtschaft (Wagner/Mindus 2015: 2). Dem stehen die Infrastrukturen gegenüber, die sich in der jüngsten Vergangenheit herausgebildet haben: Insbesondere im Bereich der satellitengestützten Internetinfrastruktur ist Elon Musks Starlink als dominierender Akteur auf dem besten Weg, sein De-facto-Monopol zu festigen (Riedel 2023: 7f.). Für mehr Handlungsfreiheit sollte Europa unabhängiger von Starlink werden. Dabei können strategische Unabhängigkeit und Handlungsfähigkeit aus funktionierenden Märkten, Diversifizierung und mehr Wettbewerb entstehen. Es braucht also nicht zwingend einen Alleingang, um ein globales, konkurrenzfähiges Netzwerk aus Low-Orbit-Satelliten aufzubauen, das die einseitige Abhängigkeit von Starlink reduziert.

Je global vernetzter die Welt wird, desto wichtiger wird auch die digitale Entwicklungszusammenarbeit. Die Förderung menschzentrierter digitaler Infrastrukturen kann Allianzen, bilaterale Beziehungen und gemeinsame Interessen stärken. Entwicklungspolitik im digitalen Bereich – insbesondere die Förderung von Digital Literacy, also von Digitalkompetenz, und daran anknüpfend wirtschaftliche Kooperationen – sollte auch als Instrument der Softpower verstanden werden. China, aber auch Saudi-Arabien und teilweise die USA drängen hier bereits in den Markt. Europa sollte unbürokratischer und schneller aktiv werden, um nicht nur die Wertebasis der globalen Digitalisierung zu prägen, sondern auch wirtschaftliche sowie geopolitische Partnerschaften aufzubauen. In diesem Zusammenhang sollten auch die Marktzugänge zur europäischen Digitalwirtschaft neu organisiert und erleichtert werden. Ein leichterer Zugang kann digitale Wertschöpfungsketten breiter verteilen und Partnerländern neue Marktchancen eröffnen. Dies kann die Abwanderung von Fachkräften verringern und zugleich qualifizierte Arbeitskräfte dem europäischen Arbeitsmarkt zugänglich machen. Auf diese Weise kann Europa auch Innovation aus digitalen Ökosystemen anderer Länder als den USA und China einfacher nutzen und die genutzten digitalen Dienste zugleich diversifizieren.

Zwar existieren bereits Angemessenheitsbeschlüss der Datenschutz-Grundverordnung (DSGVO), die garantieren sollen, dass deren Schutzniveau auch bei der Verarbeitung personenbezogener Daten im nicht-europäischen Ausland eingehalten wird, doch weitreichendere Ansätze könnten die Verbindlichkeit und Wirkung erhöhen. Denkbar wäre beispielsweise eine Datenunion, die einen gemeinsamen Standard für die teilnehmenden Staaten definiert und grob als verbindlichere Weiterentwicklung des G7-Ansatzes „Data Free Flow with Trust“ (Voelsen 2022: 4) zusammengefasst werden kann, oder darauf aufbauend eine Koalition mittlerer Mächte für KI-Wettbewerbsfähigkeit, die Zugänge und die Verteilung der Wertschöpfung klar aufteilt und Investitionen und Kompetenzen bündelt und koordiniert.

5 Gemeinsam handeln und Koalitionen aufbauen

Da die USA für Europa kein uneingeschränkt verlässlicher Partner mehr sind, muss Europa neue Koalitionen aufbauen und sich dafür einsetzen, digitale Infrastrukturen und Standards weiterhin offen zu halten und zu teilen.

5.1 Internationaler Informationsaustausch: Frühwarnsysteme für hybride Bedrohungen

Wie in den vorherigen Policy Papern 1 und 2 ausgeführt, hängt Sicherheit wesentlich davon ab, Bedrohungen zuvorzukommen. Dazu müssen Angriffsmuster und -dynamiken frühzeitig erkannt werden. Frühwarnsysteme – ob für Cybersicherheit, den Informationsraum oder weitere hybride Bedrohungen – sind daher essenziell. Bislang fehlt jedoch ein umfassendes Lagebild, das aktuelle Gefahren für Kommunen, Länder und den Bund sowie für den öffentlichen und privaten Sektor zusammenträgt und dabei auch parallele Angriffsmuster jenseits der eigenen Grenzen im Blick behält. Zudem müssen Frühwarnsysteme zu Cyberbedrohungen und FIMI miteinander kombiniert werden, um breiter angelegte Kampagnen, die unterschiedliche hybride Angriffsformen systematisch miteinander kombinieren, erkennen zu können. Auf deutscher Ebene könnte das Nationale Cyberabwehrzentrum der Bundesregierung im Bereich Cybersicherheit diese Aufgabe perspektivisch übernehmen. Bislang verfügt es jedoch über zu geringe Durchsetzungskraft und zu wenige Kompetenzen, um sie wirksam zu erfüllen. In Deutschland prägt zudem weiterhin eine Kultur der Verschwiegenheit den Umgang mit Sicherheitslücken: Aus Sorge vor Imageschäden werden sie häufig nicht transparent und schnell kommuniziert.

Für eine funktionierende Vorausschau braucht es ein ganzheitliches, zentrales und laufend aktualisiertes Lagebild. Die schwarz-rote Koalition hat im Koalitionsvertrag den Aufbau eines Nationalen Lagezentrums angekündigt, bislang aber nicht umgesetzt. Auch der sogenannte Cyberdome des Bundesinnenministeriums soll zu einem Lagebild beitragen, lässt dabei jedoch die europäische und internationale Ebene außer Acht. Ebenso forderte die Fraktion Bündnis 90/Die Grünen im September 2025 die Einrichtung eines Zentrums für strategische Vorausschau, das ein Gesamtbild hybrider Bedrohungen schaffen soll. Ein solches Lagebild muss auf nationaler Ebene anfangen, darf dort aber nicht enden: Eine europäische und internationale Lagebilderfassung in multilateralen Bündnissen ist notwendig, um grenzüberschreitende regionale Bedrohungsdynamiken rechtzeitig zu erkennen und frühzeitig vor ihnen zu warnen. Dabei gilt: Niemand ist sicher, solange nicht alle sicher sind.

Ähnlich wie bei Cybersicherheitsvorfällen setzt auch das frühzeitige Erkennen von Desinformationskampagnen den Austausch vorhandener Erkenntnisse (Information

Sharing) voraus. Neben den in Teil 1 dieser Reihe beschriebenen Verpflichtungen zu Transparenz und Datenzugängen (Locher/Bacherle 2026: 7, 14) sollten Akteure Erkenntnisse und Daten möglichst offen, interdisziplinär und international teilen. So lässt sich ein internationales Frühwarnsystem für Desinformationskampagnen und Manipulation digitaler Informationsräume entwickeln, bei dem Anomalien in der Entwicklung oder Verbreitung von Narrativen frühzeitig entdeckt und entsprechende Warnungen weitergegeben werden können.

Deutschland hat mit der Zentralen Stelle zur Erkennung ausländischer Informationsmanipulation (ZEAM) einen ersten Schritt unternommen, um die Arbeit verschiedener Ministerien zu koordinieren. Eine wichtige Weiterentwicklung wäre, diese interministerielle Arbeitsgruppe zu einem europäischen Cluster auszubauen. Nach dem Vorbild des kanadischen Media Ecosystem Observatory könnte dieses Cluster digitale Informationsräume datenbasiert und plattformübergreifend beobachten, Anomalien identifizieren und die Ergebnisse unter Einbeziehung von Expertise zu europäischen Sprachen und regionalen soziokulturellen Entwicklungen und Besonderheiten öffentlich zugänglich aufbereiten (Pehlivan et al. 2025).

5.2 Infrastruktur: Ein multilaterales Bündnis für souveräne Satellitenkommunikation

Die Entwicklungen in der Ukraine zeigen unlängst, wie wichtig eine funktionierende und geopolitisch souveräne Satelliteninfrastruktur ist. Die Verteidigungsfähigkeit der Ukraine ist in hohem Maße auf Satellitenkommunikation und -infrastruktur der Streitkräfte angewiesen. Ein großflächiger Cyberangriff auf GEO-Satelliten-Breitbanddienste des US-Kommunikationsunternehmens Viasat kappte den Satelliten-Internetzugang und legte die Satellitenkommunikation der ukrainischen Streitkräfte lahm (Gehringer/Stegner 2025: 212). Die Ukraine bat daraufhin Elon Musk um die Unterstützung durch Starlink, der dies wiederum als geopolitischen Hebel nutzen konnte (ebd., Locher/Bacherle 2026). Beide Beispiele zeigen: Eine funktionierende, redundante und souveräne Satelliteninfrastruktur ist ein zentraler Bestandteil der eigenen Sicherheitsarchitektur.

Im europäischen Verbund sollte Deutschland deshalb auf den Aufbau europäischer Lösungen für die Satelliteninfrastruktur setzen. Erste Ansätze bestehen bereits: Der Tallinn-Mechanismus, dem auch Deutschland angehört, ist eine 2023 gegründete Initiative von zwölf Staaten zur systematischen Unterstützung der Ukraine im Bereich der Cybersicherheit (Tallinn Mechanism Platform o. D.). Der Tallinn-Mechanismus unterstützt die Ukraine unter anderem darin, Terminals für sichere Satellitenkommunikation aufzubauen (Auswärtiges Amt 2024). Darüber hinaus hat die EU Ende 2024 das europäische Satellitenprogramm IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite) für eine sichere europäische Konnektivität bis 2030 ins Leben gerufen (European Commission 2024). IRIS² hatte anfänglich Schwierigkeiten

(Locker/Kulbatzki 2025); inzwischen gewinnt das Projekt mit seiner geplanten Inbetriebnahme und der Satellitenkommunikation GOVSATCOM für die militärische Nutzung jedoch an Fahrt. Zu Beginn wurde an IRIS² vor allem kritisiert, dass es in erster Linie französischen Unternehmen zugutekomme und weniger ein gesamteuropäisches Projekt sei – eine Debatte, die auch an andere Auseinandersetzungen im Bereich von Sicherheit und Verteidigung erinnert (etwa bei dem deutsch-französischen Kampfjetvorhaben Future Combat Air System FCAS).

Um langfristig echte Alternativen zu Starlink aufzubauen, braucht Europa Mut für Investitionen, konsequentes Engagement und eine verbindliche Zusammenarbeit. Vorhaben für den Aufbau von Satelliteninfrastrukturen müssen strukturell verankert werden, während nationale Befindlichkeiten und Interessen zurückstehen sollten. Projekte wie IRIS² sowie weitere europäische Lösungen, etwa des britisch-französischen Unternehmens Eutelsat OneWeb, können mithilfe von Staaten als Ankerkunden für eine wachsende Abdeckung in Europa und gegebenenfalls Afrika sorgen, während diese Systeme bestenfalls untereinander kompatibel sind und mit weiteren interagieren können. Hierfür sind Investitionen in öffentliche Projekte wie IRIS² und private Projekte wie Eutelsat OneWeb sowie ein klares Bekenntnis zu offenen Standards und deren Einsatz notwendig. Souveräne Alternativen können nur dann konkurrenzfähig sein und realistische Erfolgschancen haben, wenn Systeme, die auf multilateraler Zusammenarbeit aufbauen, ihre Kapazitäten und Stärken bündeln, wie dies etwa die Satellitenhersteller Airbus, Leonardo und Thales jüngst mit der Fusion ihrer Raumfahrtsparten angekündigt haben.

5.3 Digitale Innovation: Internationale Datenmärkte und AI Coalition

Die schnelle und kostenintensive Entwicklung leistungsfähiger KI-Modelle verstärkt Europas Abhängigkeit von digitalen Diensten, insbesondere in der Cybersicherheit. Auch wenn die Europäische Union mit Initiativen wie dem Tech Sovereignty Package und der Initiative für KI-Gigafactories versucht, eigene Entwicklungen zu fördern, dürfte selbst eine Priorisierung von Follow-up-Modellen (insbesondere zu KI-Foundation-Modellen), die neueste Spitzenmodelle rasch nachbilden, im europäischen Alleingang kaum ausreichen. Auch aus ökologischer Sicht wäre es nicht ratsam, dem weitgehend ungesteuerten Ausbau von Rechenzentren wie in den USA zu folgen. Er fördert vielerorts den Ausbau fossiler Energieerzeugung und belastet lokale Ökosysteme durch einen immensen Wasserverbrauch. Rechenzentren sollten dort gebaut werden, wo erneuerbarer Strom verfügbar ist, Kühlung weniger notwendig ist bzw. Abwärme effizient genutzt werden kann. Hier können einige Staaten günstige Bedingungen anbieten. Für manche ist auch eine Diversifizierung des KI-Marktes und ein gesicherter Zugriff auf neuste Modelle interessant.

Deutschland und die Europäische Union sollten daher zusammen mit anderen Mittelmächten, die ihre Abhängigkeit von US-amerikanischen und chinesischen Unternehmen und deren KI-Modellen verringern wollen, eine Organisation für eine AI Coalition gründen. Diese könnte ein verbindliches multilaterales Bündnis bilden, um Rechenkapazitäten, Kompetenzen und Kapital zu bündeln und die daraus entstehende Wertschöpfung fair zu verteilen. Sozial-ökologische Nachhaltigkeitskriterien können dabei die Akzeptanz der KI-Modelle erhöhen. Sonderwirtschaftszonen können die Bildung von Exzellenzclustern fördern, in denen Forschungsinvestitionen zusammengeführt und Unternehmensgründungen erleichtert werden. Dynamische arbeitsrechtliche Regelungen, ein vereinfachtes Einwanderungsrecht insbesondere für hochbezahlte Fachkräfte sowie Steueranreize können hier zudem weitere Ansiedlungen begünstigen. Im Gegenzug werden die mittel- und langfristigen Steuereinnahmen an die an der Koalition beteiligten Länder unter Berücksichtigung von sozial-ökologischen Lasten verteilt.

Gleichzeitig könnte so ein dritter Weg der Datenverwaltung und Zugangsorganisation etabliert werden. Aktuell wird der für Big Data und KI-Entwicklung so wichtige Zugang zu großen Datenmengen am effektivsten im digitalen Autoritarismus und im Überwachungskapitalismus organisiert. Während im Überwachungskapitalismus monopolartige Konzerne Daten über ihre angebotenen Dienste sammeln und diese ohne weitere Zustimmung oder Beteiligung der datengenerierenden Menschen weiterverwenden, liegt im digitalen Autoritarismus dieses Monopol beim Staat, der mehr oder weniger direkt über Zugriffsverwaltung verfügen kann. Beide Formen erleichtern beispielsweise das Training großer KI-Modelle. Dabei werden Urheberrechte verletzt und sensible personenbezogene Daten genutzt. Doch in manchen Bereichen ist dieses Vorgehen bislang legal, und tragfähige Alternativen fehlen. Mit dem Data Act und weiteren Gesetzen hat die Europäische Union bereits versucht, einen regulatorischen Gegenentwurf zu schaffen, der den Nutzenden von digitalen Geräten mehr Mitbestimmung und eine Beteiligung an der datenbasierten Wertschöpfung ermöglichen soll. Diesen dritten Weg der individuellen Datensouveränität und ökonomischen Teilhabe an Datengeschäftsmodellen gilt es nun weiterzuentwickeln, zum Beispiel durch die rechtliche Stärkung von Datentreuhandmodellen, Datenzugriffs- und Nutzungsrechten für Nutzende sowie klare Rahmen- und Musterverträge zur Lizenzierung von Datennutzung.

5.4 Internationale Zusammenarbeit: Digitale Außenpolitik global gerecht gestalten

Technologische Entwicklungen und ihre Konsequenzen lassen sich nicht vom globalen Kontext trennen (Bacherle/Zorn 2023). Wie wir Digitalpolitik, Sicherheit und Außenpolitik gestalten, hat unmittelbare Auswirkungen auf den Globalen Süden – und umgekehrt. Die erste Strategie der Ampel-Bundesregierung für internationale Digitalpolitik aus 2024 nimmt die Bedeutung globaler Partnerschaften zwar in den Blick, setzt

hier jedoch keinen Schwerpunkt und leitet daraus keine konkreten Maßnahmen ab (Die Bundesregierung 2024). Große Teile der digitalen Transformation beruhen heute in erheblichem Maß auf der Ausbeutung von Clickworker*innen aus dem Globalen Süden, die unter prekärsten Bedingungen und hoher psychischer Belastung Algorithmen für KI-Modelle trainieren und die Contentmoderation[2] übernehmen. Gleichzeitig sind die Ausbeutung natürlicher Ressourcen für digitale Technologien und die Abhängigkeit von zentralen Vorprodukten wie Chips sowohl geopolitische als auch sicherheitspolitische Fragen.

Es ist deshalb essenziell, auf europäischer und nationaler Ebene eine gleichberechtigte Zusammenarbeit mit Ländern des Globalen Südens zu gestalten. Sie sollte gemeinsame Potenziale nutzen, die Grenzen natürlicher Ressourcen gleichermaßen respektieren und einen wertebasierten, demokratischen sowie gleichberechtigten internationalen Raum verankern. Digitale Außenpolitik muss den Menschen in den Mittelpunkt stellen: Denn der Zugang zu digitalen Technologien entscheidet immer noch maßgeblich über Chancen auf dem Arbeitsmarkt, die demokratische Teilhabe und auch die Gesundheit, besonders für Frauen und marginalisierte Gruppen (Bacherle/Zorn 2023). Ein aktives Engagement der Bundesregierung, etwa über das EU-Programm Global Gateway, kann die globale Zusammenarbeit im Digitalen stärken. Im Unterschied zu russischen und chinesischen Angeboten muss sie dabei die Handlungsfähigkeit der Partnerländer fördern, statt neue Abhängigkeiten zu schaffen. Die Bundesregierung wäre gut beraten, auch haushaltspolitisch auf eine nachhaltige Zusammenarbeit zu setzen, die globale Partnerschaften stärkt und dekoloniale Grundsätze endlich konsequent berücksichtigt.

2 Contentmoderation bezeichnet die Überprüfung von Inhalten, insbesondere solcher, die zuvor wegen eines mutmaßlichen Verstoßes gegen die Nutzungsbedingungen oder wegen vermuteter Illegalität gemeldet wurden.

6 Fazit: Ein Maßnahmenpaket für eine global ausgerichtete digitale Außenpolitik

Die Auswirkungen, Regeln und Rahmenbedingungen der digitalen Transformation werden maßgeblich auf internationaler Ebene entschieden. Deutschland sollte diesen Raum gemeinsam mit der EU nutzen, um digitale Technologien menschzentriert und fair zu gestalten. Erstens sollte sich Deutschland stärker in entscheidende Prozesse der VN einbringen, etwa indem die Bundesregierung eine verbindliche Regelung für LAWS vorantreibt, die VN-Cybercrime-Konvention kritisch begleitet, bereits bestehende Allianzen zur Bekämpfung von Internetsperren mobilisiert und einen globalen Standard für Content Credentials der IETF anstößt. Zweitens sollte Deutschland neue Bündnisse anstoßen, um ein internationales Frühwarnsystem für hybride Bedrohungen zu etablieren, ein multilaterales Bündnis zum Aufbau souveräner Satellitenkommunikation voranzutreiben und eine Organisation für eine AI Coalition zu gründen.

Literaturverzeichnis

Auswärtiges Amt (2024): Gemeinsame Erklärung des Tallinn-Mechanismus. Geber bringen 200 Millionen Euro für die Widerstandsfähigkeit der Ukraine im Cyberraum auf; in: auswaertiges-amt.de, https://www.auswaertiges-amt.de/de/newsroom/2691870-2691870, Zugriff 14.9.2026

Bacherle, Tobias (2024): Russia and China Cheer UN Cybercrime Convention; in: CEPA, 21.8.2024, https://cepa.org/article/russia-and-china-cheer-un-cybercrime-convention/, Zugriff 14.9.2026

Bacherle, Tobias/Locher, Nina (2026): Reaktionsfähigkeit stärken. Effektive Maßnahmen gegen hybride Bedrohungen; in: Dimensionen digitaler Außenpolitik, Teil 2, Heinrich-Böll-Stiftung, https://www.boell.de/de/2026/07/08/teil-2-reaktionsfaehigkeit-staerken, Zugriff 14.9.2026

Bacherle, Tobias/Zorn, Armand (2023): Internationale Digitalstrategie. Deutschland muss aktiv werden!; in: Tagesspiegel Background: Digitalisierung & KI, 25.7.2023, https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/internationale-digitalstrategie-deutschland-muss-aktiv-werden, Zugriff 14.9.2026

Barker, Tyson (2020): Die EU braucht eine digitale Außenpolitik; in: Tagesspiegel Background: Digitalisierung & KI, 13.11.2020, https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/die-eu-braucht-eine-digitale-aussenpolitik, Zugriff 14.9.2026

Barker, Tyson/Hagebölling, David (2022): A German Digital Grand Strategy. Integrating Digital Technology, Economic Competitiveness, and National Security in Times of Geopolitical Change, DGAP Report, Nr. 2022/7, German Council on Foreign Relations (DGAP), https://dgap.org/system/files/article_pdfs/DGAP-Report-2022-07-EN_0.pdf, Zugriff 14.9.2026

Bundesministerium für Wirtschaft und Energie (BMWE) (2026): 10 Jahre WIPANO. Innovationen durch Normung und Patente erfolgreich stärken; in: innovation-beratung-foerderung.de, https://www.innovation-beratung-foerderung.de/INNO/Redaktion/DE/Kurzmeldungen/Aktuelles/2026/260302-10-jahre-wipano.html, Zugriff 14.9.2026

Die Bundesregierung (2024): Strategie für die internationale Digitalpolitik; in: bundesregierung.de, https://www.bundesregierung.de/breg-de/aktuelles/internationale-digitalpolitik-2258116, Zugriff 14.9.2026

European Commission (2022): Erklärung zur Zukunft des Internets; in: Gestaltung der digitalen Zukunft Europas, https://digital-strategy.ec.europa.eu/de/library/declaration-future-internet, Zugriff 14.9.2026

European Commission (2024): IRIS² Secure Connectivity Programme; in: Defence Industry and Space, https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en, Zugriff 14.9.2026

Gehringer, Ferdinand/Stegner, Johannes (2025): Deutschland im Ernstfall. Was passiert, wenn wir angegriffen werden, Hoffmann und Campe, Hamburg

International Telecommunication Union (ITU) (2018): ITU-Plenipotentiary Conference in Dubai. Policy statements and speeches; in: itu.int, https://www.itu.int/web/pp-18/cn/policy-statement, Zugriff 14.9.2026

Kleinwächter, Wolfgang (2026): Entwicklungen im Internet Governance Umfeld Juli bis August 2026, in: DENIC Blog, 08.9.2026.

https://blog.denic.de/entwicklungen-im-internet-governance-umfeld-juli-bis-august-2026/ Zugriff 14.9.2026.

Klotz, Sebastian (2023): Who drives the international standardisation of telecommunication and digitalisation? Introducing a new data set; in: Global Policy 14(3), S. 558–568, https://doi.org/10.1111/1758-5899.13223, Zugriff 22.9.2026

Komaitis, Konstantinos/Sherman, Justin (2022): The ITU election pitted the United States and Russia against each other for the future of the internet; in: Tech at the leading edge, Atlantic Council, 29.9.2022, https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/the-itu-election-and-the-future-of-the-internet/, Zugriff 14.9.2026

Locher, Nina/Bacherle, Tobias (2026): Angriffsflächen vorbeugen. Prävention als Grundlage digitaler Außenpolitik; in: Dimensionen digitaler Außenpolitik, Teil 1, Heinrich-Böll-Stiftung, https://www.boell.de/de/2026/06/18/teil-1-angriffsflaechen-vorbeugen, Zugriff 14.9.2026

Locker, Theresa/Kulbatzki, Josefine (2025): iris2. Viele Fragezeichen bei Europas Starlink-Alternative; in: Tagesspiegel Background: Digitalisierung & KI, 7.8.2025, https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/iris2-viele-fragezeichen-bei-europas-starlink-alternative, Zugriff 14.9.2026

Niazi, Maral/Hassan, Oz/Smart, Sebastian (2026): Global AI Governance Framework: From Conceptualization to Implementation; in: Foundational Principles of AI Governance and Policy. Frontiers of Artificial Intelligence, Ethics and Multidisciplinary Applications. Springer, Cham. S. 227-243.

Paulus, Alexandra (2025): Europas Cybersicherheit hängt an den USA. Wie europäische Regierungen mehr Verantwortung übernehmen können; in: SWP-Aktuell 2025/A 48, S. 1–8, https://www.swp-berlin.org/publikation/europas-cybersicherheit-haengt-an-den-usa, Zugriff 14.9.2026

Pehlivan, Zeynep/Park, Saewon/Abrahams, Alexei Sisulu/Desblancs-Patel, Mika/Steel, Benjamin David/Bridgman, Aengus (2025): Building a Media Ecosystem Observatory from Scratch. A Data Infrastructure for Cross-Platform Analysis; in: arxiv.org, https://arxiv.org/pdf/2506.10942, Zugriff 14.9.2026

Riedel, Ann-Cathrin (2023): Digital policy in an age of global systemic rivalry. Challenges for liberal democracies, Friedrich-Naumann-Stiftung

Rühlig, Tim (2022): Chinas unsichtbare Macht technischer Standards. Eine Herausforderung für Deutschland und Europa, Friedrich-Naumann-Stiftung

Rühlig, Tim (2023): The New geopolitics of technical standardisation. A European perspective; in: Future Europe 3(1), S. 102–109, https://feu-journal.eu/issues/issue-3/the-new-geopolitics-of-technical-standardisation-a-european-perspective/, Zugriff 14.9.2026

Tallinn Mechanism Platform (o. D.): Tallinn Mechanism Platform. Enhancing Ukraine‘s long-term cyber resilience; in: platform-tm.com, https://platform-tm.com/, Zugriff 14.9.2026

The White House (2026): Withdrawing the United States from International Organizations, Conventions, and Treaties that Are Contrary to

the Interests of the United States; in: whitehouse.gov, 7.1.2026, https://www.whitehouse.gov/presidential-actions/2026/01/withdrawing-the-united-states-from-international-organizations-conventions-and-treaties-that-are-contrary-to-the-interests-of-the-united-states/, Zugriff 14.9.2026

United Nations General Assembly (2025): Lethal autonomous weapons systems. Resolution adopted by the General Assembly on 1 December 2025; in: docs.un.org, A/RES/80/57, https://docs.un.org/en/A/RES/80/57, Zugriff 14.9.2026

Voelsen, Daniel (2022): Deutschlands erste Strategie zur internationalen Digitalpolitik. Ein Vorschlag zur thematischen Ausrichtung, SWP-Aktuell 2022/A 79, S. 1–8, https://www.swp-berlin.org/10.18449/2022A79/, Zugriff 22.9.2026

Wagner, Ben/Mindus, Patricia (2015): Multistakeholder Governance and Nodal Authority. Understanding Internet Exchange Points; in: NoC Internet Governance Case Studies Series, https://cihr.eu/wp-content/uploads/2015/01/Wagner_Mindus_IXPs_NoC1.pdf, Zugriff 14.9.2026

Weber, Valentin (2025): A Lack of Action in UN Cyber Discussions Is Partly the Fault of the West. In: DGAP memo, No. 36, DGAP

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: November 2026

Covermotiv: IMAGO/Marc John

Lizenz: Creative Commons (CC BY-NC-ND 4.0)
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de

Die vorliegende Publikation spiegelt nicht notwendigerweise die Meinung der Heinrich-Böll-Stiftung wider.

Die Publikationen der Heinrich-Böll-Stiftung dürfen nicht zu Wahlkampfzwecken verwendet werden.

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