Dimensionen digitaler Außenpolitik

böllpaper

Der digitale Raum in geopolitisch angespannten Zeiten

Einführung in die dreiteilige Reihe

Tobias B. Bacherle und Nina Locher

Der digitale Raum in geopolitisch angespannten Zeiten

Einführung in die dreiteilige Reihe

Ein Policy Paper von Tobias B. Bacherle und Nina Locher

HEINRICH BÖLL STIFTUNG

Der digitale Raum als Austragungsort des Systemwettbewerbs

Digitalpolitik ist längst eine zentrale Dimension der Außen- und Sicherheitspolitik. Kämpfe um Macht und Einfluss zwischen Nationalstaaten, kriegerische Auseinandersetzungen, aber auch die Verteidigung der sowie die Angriffe auf Freiheits- und Menschenrechte haben sich zunehmend in den digitalen Raum verlagert. Im digitalen Raum wird immer öfter und vehementer der globale Systemwettbewerb ausgetragen.

Nach der russischen Vollinvasion in der Ukraine am 24. Februar 2022 läutete die Ampel-Regierung aus SPD, Bündnis 90/Die Grünen und FDP eine verteidigungspolitische Zeitenwende ein: Es wurde anerkannt und im Deutschen Bundestag entschieden, dass mehr in die Sicherheit und Verteidigung Deutschlands investiert werden muss, um Freiheit und Demokratie zu schützen (Deutscher Bundestag 2022). Die erste Nationale Sicherheitsstrategie überhaupt zielt auf integrierte Sicherheit und rückt die individuellen Sicherheitsbedürfnisse der Menschen ins Zentrum (vgl. Die Bundesregierung 2023: 7). Mehr als vier Jahre nach dem Beginn des russischen Angriffskriegs und mehr als ein Jahr nach Beginn der zweiten Präsidentschaft Donald Trumps ist die (Neu-)Gestaltung digitaler Außenpolitik im Kontext der Zeitenwende auf nationaler und internationaler Ebene drängender denn je. Denn gerade in Zeiten divergierender Sicherheitsinteressen und geopolitischer Spannungen muss das Paradigma der digitalen Außenpolitik lauten: Sicher sind wir nur, wenn alle sicher sind.

Digitale Außenpolitik hat den Anspruch, die zunehmend auch im digitalen Raum stattfindenden außenpolitischen Herausforderungen ganzheitlich zu denken und zu gestalten. Sie stellt sich damit der Tatsache, dass viele der gegenwärtigen geopolitischen Herausforderungen, sichtbar oder unsichtbar, zwar schon länger im Digitalen stattfinden, aber noch lange nicht systematisch gedacht und betrachtet werden. Wie etwa muss nationale oder auch europäische Digitalpolitik gestaltet werden, damit sie die Handlungsfähigkeit auf der außenpolitischen Bühne stärkt? Welche digital-außenpolitischen Instrumente braucht die Politik, um digitalen Bedrohungen auf nationaler und europäischer Ebene klar entgegenzutreten? Welche multilateralen Bündnisse und Maßnahmen sind erforderlich, um integrierte Sicherheit auch im digitalen Raum global für alle Menschen zu stärken?

Geopolitische Auseinandersetzungen im digitalen Raum

Wir sind strukturell abhängig: von Bürosoftware wie Microsoft Office über Mikrochips aus China mit Seltenen Erden aus Afrika bis hin zu den Cloudspeichern von Amazon. Dies kann im Ernstfall geopolitische und wirtschaftliche Handlungsspielräume, z. B. der EU und afrikanischer Staaten, massiv einschränken, ganz ähnlich, wie es durch die energiepolitischen Abhängigkeiten Deutschlands von Russland zum Beginn der

Vollinvasion in der Ukraine der Fall war. Gleichzeitig baut die digitale Transformation mit ihrer KI-Entwicklung und Content-Moderation zu großen Teilen auf der Ausbeutung von Rohstoffen und Datenarbeiter*innen aus dem Globalen Süden auf (Albert 2025). Des Weiteren ist es kein Geheimnis mehr, dass u. a. Russland und China auf internationaler Bühne darum kämpfen, wer die Vorherrschaft über Standardisierungen, also international festgelegte Rahmenbedingungen für digitale Infrastrukturen, erlangt. Diese können die Abhängigkeit von digitalen Infrastrukturen langfristig vorbestimmen. Gleichzeitig leben die Struktur und Verwaltung des Internets von seinem offenen, dezentralen Charakter; digitalen Diensten liegt oft Open-Source-Basisinfrastruktur zugrunde. Dieses offene, demokratische, globale Internet gilt es zu schützen.

Digitale Außenpolitik forciert aktives multilaterales Engagement und mutige Investitionen in die eigene strategische Souveränität, um zu einer vorausschauenden Außenpolitik zu führen. Je mehr sich unsere Wirtschaft, Gesellschaft und unser globales Handeln digitalisieren, desto stärker verlagert sich dieser geopolitische Aushandlungsprozess in den digitalen Raum selbst.

Angriffe auf Menschenrechte im Digitalen

Autoritäre Kräfte im Inneren, im Äußeren und im Digitalen greifen unsere Freiheit an. Der digitale Raum ist ein zentraler Austragungsort der Strategien autoritärer Regime wie Russland, China oder Iran. Um unliebsame Kritiker*innen mundtot zu machen, nutzen diese Regime diverse digitale Werkzeuge. Sie überwachen, lesen mit und doxxen, zensieren und schalten Unliebsames stumm. Sie schalten in ihrem Land einzelne Plattformen oder auch das gesamte Internet ab. Sie manipulieren die öffentliche Meinung und die digitalen Debattenräume, gezielt auch in anderen Staaten.

So beschneiden sie Menschenrechte, untergraben das Vertrauen in freie Gesellschaften oder schüren Unsicherheit. Dies führt zu Selbstzensur und zum Rückzug kritischer Stimmen, oft von Frauen, LSBTIQ* sowie marginalisierten Gruppen. Darunter leidet die demokratische Community weltweit.

Digitale Außenpolitik kann mit kluger und verzahnter Politik Freiheitsrechte weltweit stärken. Dabei müssen nationale oder europäische Vorstöße im Einklang mit der eigenen außen- und sicherheitspolitischen Verantwortung und Glaubwürdigkeit stehen. Ein feministischer Blick auf digitale Menschenrechte hinterfragt etwa kritisch, wer z. B. von Cybersicherheit geschützt wird und wer außen vor bleibt. Denn Freiheitsrechte, die im Inneren selbst beschnitten werden, werden im Handumdrehen zur Blaupause für autoritäre Kräfte in anderen Staaten.

Digitale Angriffe als Dimension hybrider Kriegsführung

Auch die Taktiken, sowohl bei konventionell als auch bei hybrid ausgetragenen Konflikten, verlagern sich zunehmend ins Digitale. So sind etwa Cyberangriffe oder Desinformationskampagnen längst zum Standard der hybriden Kriegsführung geworden. Moderne Konflikte sind heute ohne Cyberattacken, Angriffe auf die kritische Infrastruktur und auf Satellitensysteme, Internetabschaltungen und den Einsatz von KI und Desinformationskampagnen kaum mehr vorstellbar. Im Dezember 2025 erklärte die Bundesregierung, dass die hybride Kriegsführung Russlands konkret unsere Sicherheit gefährde – nicht nur durch den Angriffskrieg gegen die Ukraine, sondern auch durch konkrete Angriffe bei uns in Deutschland (Auswärtiges Amt 2025): Die Bundesregierung ordnete in diesem Zusammenhang Russland sowohl einen Cyberangriff auf die deutsche Flugsicherung als auch eine gezielte Desinformationskampagne während des Bundestagswahlkampfes 2025 zu. Diese digitalen Angriffe, die auf den Zusammenhalt und das Sicherheitsgefühl in unserer Gesellschaft zielen, verdeutlichen die Gefahr hybrider Kriegsführung.

Digitale Außenpolitik kann unsere Resilienz stärken, wenn wir anerkennen, dass innere und äußere Sicherheit nicht mehr getrennt voneinander betrachtet werden können. Wir müssen beides zusammen denken und Kohärenz zwischen nationalem Handeln und internationalem Einsatz und Anspruch schaffen. Denn in Zeiten hybrid ausgetragener Konflikte ist entscheidend, dass digitale Außenpolitik dort ansetzt, wo hybride Bedrohungen die Widerstandsfähigkeit unserer Gesellschaft im Inneren, genauso wie die Wehrhaftigkeit im Äußeren berühren und internationale Kooperationen mit Kredibilität aufgebaut und gepflegt werden können.

Die dreiteilige Policy-Paper-Reihe widmet sich je einer Dimension digitaler Außenpolitik. Wie kann digitale Außenpolitik mit guter Prävention zu mehr Schutz, Sicherheit und Souveränität führen? Welche Maßnahmen sind nötig, um frühzeitig, schnell und koordiniert auf digitale Gefährdungen reagieren zu können? Welche internationalen Bündnisse und Kooperationen sind erforderlich, um integrierte Sicherheit global zu stärken?

Denn gerade vor dem Hintergrund der Zeitenwende muss eine grundlegende Erkenntnis in Bezug auf den digitalen Raum in die deutsche und europäische Außen- und Sicherheitspolitik dringen: Wir sind nur sicher, wenn alle sicher sind.

Literaturverzeichnis

Albert, Paulina (2025): Wie funktioniert der digitale Kolonialismus; in: fluter.de; 8.12.2025, https://www.fluter.de/digitaler-kolonialismus-sven-hilbig, Zugriff 2.6.2026

Auswärtiges Amt (2025): Erklärungen des Auswärtigen Amts in der Regierungspressekonferenz vom 12.12.2025; in: auswaertiges-amt.de; 12.12.2025, https://www.auswaertiges-amt.de/de/newsroom/regierungspressekonferenz-2748168, Zugriff 2.6.2026

Deutscher Bundestag (2022): Regierungserklärung. Bundeskanzler Olaf Scholz: Wir erleben eine Zeitenwende; in: bundestag.de; 27.02.2022, https://www.bundestag.de/dokumente/textarchiv/2022/kw08-sondersitzung-882198, Zugriff 2.6.2026

Die Bundesregierung (2023): Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland. Nationale Sicherheitsstrategie, https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf, Zugriff 2.6.2026

Die Autor*innen

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.

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.

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: freepik (Bilder auf dem Laptop: IMAGO/alimdi/ Sylvio Dittrich/Marc John)

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