Dimensionen digitaler Außenpolitik

böllpaper

Teil 2: Reaktionsfähigkeit stärken

Effektive Maßnahmen gegen hybride Bedrohungen

Tobias B. Bacherle und Nina Locher

Teil 2:
Reaktionsfähigkeit stärken

Effektive Maßnahmen gegen hybride Bedrohungen

Ein Policy-Paper von Tobias B. Bacherle und Nina Locher

HEINRICH BÖLL STIFTUNG

Inhalt

Zusammenfassung

Hybride Bedrohungen sind zu einer dauerhaften sicherheitspolitischen Realität geworden. Cyberangriffe, Desinformationskampagnen und ausländische Informationsmanipulation und Einmischungen sowie andere solche Bedrohungen erfordern klare Antworten. Für Deutschland und Europa folgt daraus: Digitale Außenpolitik muss nicht nur die Resilienz präventiv stärken, sondern zugleich über glaubwürdige, schnelle und koordinierte Reaktionsmechanismen verfügen. Dabei müssen digitale Menschenrechtsstandards zwingend eingehalten werden, auch um den eigenen Anspruch und die eigene Glaubwürdigkeit auf dem internationalen Parkett zu festigen.

Zur Stärkung der Cybersicherheit braucht es eine starke und gut koordinierte Cyberabwehr, die auf defensive Fähigkeiten, schnelle Detektion von Bedrohungen sowie schnelle Wiederherstellung von Systemen und Krisenbewältigung setzt. *Hackbacks*, also das Ausschalten digitaler Angriffssysteme auf ausländischem Territorium, sind kein nachhaltiges oder rechtssicheres Konzept: Weil die Urheberschaft hybrider Angriffe kaum sicher und schnell genug geklärt werden kann und keine Zielgenauigkeit gegeben ist, besteht die Gefahr, dass die Situation eskaliert und im Zweifel Systeme bzw. Akteure getroffen werden, die die Angriffe selbst nicht verursacht haben oder selbst deren Opfer wurden. Falls politisch trotz dieser Risiken für notwendig erachtet, muss parlamentarische Kontrolle bei *Hackbacks* gewährleistet sein. Zudem könnte ein Cyberhilfswerk helfen, wenn Cyberangriffe großen Schaden anrichten, etwa um zivile Systeme schnell wiederherzustellen, die Versorgung zu garantieren und kritische Dienstleistungen zu unterstützen.

Darüber hinaus braucht es Maßnahmen als Antwort auf die zunehmend komplexen, für geopolitische Interessen genutzten Desinformationskampagnen. Notwendig ist ein verbindliches Content-Credential-Regime, um KI-generierte Medien auf allen Plattformen kennzeichnen zu können. Für sehr große Plattformen sind transparente Kontextualisierungsmechanismen nötig, um aus dem Kontext gerissene Inhalte einzuordnen. Es braucht außerdem einen klaren Rechtsrahmen gegen professionelle Distributionsmanipulation, um die technisch amplifizierte Verbreitung ausländischer Manipulation und Einmischung (*Foreign Information Manipulation and Interference*, FIMI) einzudämmen. Wer solche Manipulationsleistungen nutzt oder anbietet, muss rechtlich belangt und sanktioniert werden können. Zugleich braucht es klare Zuständigkeiten in Ministerien und öffentlich-rechtlichen Medien, um auf veröffentlichte Analysen zu Narrativen, Netzwerkaktivitäten und Reichweitenverzerrungen reagieren zu können.

Schließlich muss Europa seine diplomatische Antwortfähigkeit im Sinne einer Abschreckung in der digitalen Außenpolitik stärken. Hybride Bedrohungen dürfen nicht in Silos bearbeitet werden. Cyberangriffe, FIMI, Spionage und digitale Menschenrechtsverletzungen sind eng miteinander verflochten und erfordern institutionell kohärente Ansätze. Dafür braucht es klare Zuständigkeiten innerhalb der Bundesregierung und eine engere Verzahnung auf europäischer Ebene. Ergänzend sollte die EU

eine *Digital Human Rights Toolbox* erarbeiten, um auf digitale Repression wie Internet-Shutdowns wirksamer reagieren zu können.

1 Hybride Bedrohungen sind Vorboten von Krieg und Menschenrechtsverletzungen und flankieren diese

> „Hybride Bedrohungen können von Cyberangriffen auf kritische Informationssysteme über die Unterbrechung kritischer Dienste wie Energieversorgung oder Finanzdienstleistungen bis hin zur Untergrabung des öffentlichen Vertrauens in staatliche Institutionen oder zur Vertiefung sozialer Spaltungen reichen."
>
> *Auswärtiger Dienst der Europäischen Union 2018*

Seit der russischen Vollinvasion der Ukraine nimmt auch in Deutschland die Aufmerksamkeit für hybride Angriffe zu. Schließlich flankiert Russland seinen Kriegszug nicht nur mit Cyberangriffen auf die Ukraine. Auch die Bundesrepublik und andere europäische Länder geraten ins Visier der hybriden Kriegsführung Russlands, nicht zuletzt, um die Unterstützung für die überfallene Ukraine zu untergraben: Die prorussische Doppelgänger-Kampagne (Frühwirth/Smirnova 2024), bei der Homepages von vertrauenswürdigen Informationsquellen nachgebaut und mit irreführenden Inhalten gefüllt werden, zielt beispielsweise direkt auf den deutschen Informationsraum. Währenddessen wurde bei der dem russischen oder belarussischen staatsnahen Umfeld zugeschriebenen Ghostwriter-Kampagne, die Cyberattacken und Desinformationsoperationen kombiniert, vor allem versucht, europäische Abgeordnete zu hacken und anschließend zu diskreditieren (Beuth/Wiedemann-Schmidt 2021).

Eine weitere Desinformationskampagne sollte zusammen mit einer breit angelegten Sabotageaktion gezielt einen politischen Akteur diskreditieren, indem Letztere seinem Umfeld zugeschrieben werden sollte: Mehr als 270 mit Bauschaum verklebte Auspuffrohre waren mit Stickern von Kanzlerkandidat Robert Habeck und dem Slogan „Sei grüner!" versehen worden. Es sollte fälschlicherweise der Eindruck erweckt werden, die Klimabewegung und das Umfeld der Bündnisgrünen wären für die Sachbeschädigung verantwortlich. So wollte die russische Desinformations- und Sabotagekampagne im Umfeld der Bundestagswahl 2025 Stimmung gegen die Partei Bündnis 90/Die Grünen machen (Lehberger et al. 2025).

Auch Cyberattacken nehmen zu und werden zur direkten Unterstützung geopolitischer Konflikte eingesetzt. Bereits seit Jahren dienen beispielsweise „die Angriffe spezialisierter nordkoreanischer Cybereinheiten vornehmlich der Cyberspionage und dem finanziellen Diebstahl zum Zwecke des Regimeerhalts" (Harnisch/Zettl 2020: 105). Zudem flankiert Russland seit der Annexion der Krim seinen Krieg gegen die Ukraine

auch im Cyberraum. Angriffe auf die kritische Infrastruktur wie die Stromversorgung wurden durch *Distributed Denial of Service-Attacken* (DDoS Attacken), also Angriffe, die durch massenhaftes Fluten von Anfragen digitale Systeme überlasten und damit funktionsunfähig machen, auf Supporthotlines und Supporthomepages unterstützt, um maximale Verunsicherung zu streuen und auf diesem Weg das Vertrauen in die demokratischen und staatlichen Institutionen zu untergraben (Lee 2016).

All diese Vorfälle zeigen die Dringlichkeit, sich gegen solche Angriffe wehren zu können und klare Reaktionsfähigkeit zu gewinnen. Diese Bedrohungslage hat die Bundesregierung im Dezember 2025 auch formell hervorgehoben, als sie Russland offiziell eine Desinformationskampagne auf die Bundestagswahl 2025 und einen Cyberangriff auf die Deutsche Flugsicherung im August 2024 zugeordnet hat. In diesem Policy Paper konzentrieren wir uns auf Cyberangriffe und Desinformation als zwei zentrale Aspekte hybrider Bedrohungen und elementare Bestandteile einer reaktionsfähigen digitalen Außenpolitik.

Im aktuellen geopolitischen Spannungsfeld wird neben guter Prävention (siehe Teil 1 der Reihe „Dimensionen digitaler Außenpolitik“) eine klare und konsequente Reaktionsfähigkeit immer wichtiger. Europa muss hier Fähigkeiten aufbauen. Dies beinhaltet u. a. Klarheit, Kompetenzen und Fähigkeiten für die Reaktion auf erfolgte hybride Angriffe. Das ist auch wegen der Unzuverlässigkeit der USA als Partner unumgänglich. Bei der Stärkung europäischer Reaktions- und Handlungsfähigkeit müssen die eigenen Ansprüche an ein offenes Internet und freie Meinungsäußerung jedoch gewahrt bleiben.

2 Was es für effektive und ganzheitliche Reaktionsfähigkeit bei hybriden Angriffen braucht

Während digitale Außenpolitik mit kluger Prävention Schwachstellen für hybride Angriffe schließen kann (siehe Teil 1), kann in der Praxis keine 100-prozentige Sicherheit durch Vorsorge gewährleistet werden. In den Bereichen Cybersicherheit, FIMI und digitale Diplomatie wurden auf nationaler und europäischer Ebene konkrete Maßnahmen und Gesetzgebungen auf den Weg gebracht. Die konsequente Umsetzung wichtiger Präventionsmaßnahmen, etwa durch die verabschiedeten Gesetze NIS2 und KRITIS-Dachgesetz, wird jedoch noch Jahre dauern. Daher ist darüber hinaus ein klar umrissenes Feld an technischen, praktischen und diplomatischen Reaktionsmöglichkeiten nötig, um hybride Angriffe abzuwehren.

2.1 Koordinierte Cyberabwehr

Die zunehmende Bedeutung von Cybersicherheit und deren Stärkung für Innen und Außen, Digitales und Verteidigung hat in den vergangenen Jahrzehnten zu einer komplexen Architektur von Gesetzgebung und Zuständigkeiten für Cybersicherheit geführt (Herpig/Dutke 2023: 11). Dabei werden eine schnelle, koordinierte Detektion von und Reaktion auf Cyberbedrohungen notwendiger denn je: Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zufolge bleibt die Lage der Cybersicherheit in Deutschland weiterhin sehr angespannt (BSI 2025). Knapp drei von vier Unternehmen in Deutschland, 73 Prozent, nahmen von 2024 auf 2025 eine gestiegene Bedrohungslage im Cyberbereich wahr (Bundesamt für Verfassungsschutz 2025).

Neben verstärkter Prävention für mehr Cyberresilienz, die maßgeblich durch die EU-Gesetzgebung und deren nationale Umsetzung (u. a. EU NIS2-Richtlinie, EU Cyber Solidarity Act, KRITIS-Dachgesetz, EU Cyber Security Act 2) vorangetrieben wird, arbeitet Bundesinnenminister Alexander Dobrindt 2026 an einem neuen Maßnahmenpaket für mehr Cybersicherheit: dem Aufbau eines nationalen „Cyberdome“ (Bundesministerium des Innern 2025). Das Maßnahmenpaket, das nach der Prävention ansetzt und konkret zur Verbesserung der Detektion und Reaktion auf Cyberbedrohungen in Deutschland gedacht ist, setzt auf den Ausbau von Befugnissen zur aktiven Cyberabwehr und zu sogenannten *Hackbacks*, soll die zivil-militärische Zusammenarbeit vertiefen und eine (teil-)automatisierte Abwehr im Netz nach dem Vorbild Israels ermöglichen. Als aktive Cyberabwehr bezeichnet die Bundesregierung Maßnahmen mit dem Ziel, im Falle eines laufenden bzw. bevorstehenden Angriffs die dabei genutzten IT-Systeme zu manipulieren oder zu stören (Deutscher Bundestag 2023: 3). Zum aktuellen Zeitpunkt ist aktive Cyberabwehr rechtlich nicht erlaubt. Bereits während der Ampelregierung 2024 wurde eine entsprechende Änderung des Grundgesetzes

diskutiert. Das Bundesinnenministerium (BMI) sieht laut Kabinettsbeschluss vom Mai 2026 anstelle einer Grundgesetzänderung hierfür aktuell eine Reform des Bundespolizeigesetzes (BPolG) sowie des Bundeskriminalamtgesetzes (BKAG) vor (Bundesministerium des Innern 2026).

Das Gesetz gibt dem BSI zwar neue Möglichkeiten, Institutionen auf deren Ersuchen frühzeitig zu warnen, setzt den Schwerpunkt jedoch auf Offensivmaßnahmen. Diese werden aus mehreren Gründen von Fachleuten kritisch gesehen: Erstens drohen bei Offensivmaßnahmen Kollateralschäden an unbeteiligten und kritischen Systemen bis hin zum Versorgungsausfall (AG KRITIS 2026). Zweitens bleiben durch den Entwurf wesentliche Grunddefizite unangetastet, besonders im Bereich der Prävention, etwa durch fehlendes verbindliches Schwachstellenmanagement oder eine stärkere Unabhängigkeit des BSI. Drittens verlagert der Entwurf grenzüberschreitende aktive Eingriffe ins Polizeirecht, obwohl z. B. die Wissenschaftlichen Dienste des Bundestages (2018) festhalten, dass diese in Einklang mit Art. 26 Abs. 1 des Grundgesetzes stehen müssen. Dies erschwert die parlamentarische Kontrolle, die bei aktiver Abwehr auf ausländischem Territorium eigentlich nötig wäre.

Abwehr statt aktiver Gegenangriffe

Um schnell und zielgerichtet auf Cyberangriffe reagieren zu können, müssen die Kapazitäten und Möglichkeiten der defensiven Cyberabwehr vollständig ausgeschöpft werden. Ein zentraler Aspekt ist, hier schnell in die Koordination und ins Handeln zu kommen. Was dabei nicht nachhaltig hilft, ist aktive Cyberabwehr.

Was auf den ersten Blick attraktiv klingen mag, ist auf den zweiten sehr gefährlich: Aktiv in ein fremdes System einzudringen setzt das Wissen voraus, wer die Angreifenden sind. Diesen Ursprung zu verschleiern ist jedoch verglichen mit konventionellen Angriffen deutlich einfacher und oft fester Bestandteil von digitalen Angriffen, was sich viele Angreifer zunutze machen: So können etwa IP-Adressen aus anderen, dritten Ländern oder Botnet-Armeen über infiltrierte externe Geräte, etwa smarte Haushaltsgeräte, genutzt werden. Diese Praxis erhöht bei *Hackbacks* das Risiko von Kollateralschäden, indem statt des Angriffsherds infiltrierte Infrastrukturen getroffen werden. Typisch sind zudem Übersetzungsfehler oder andere Sprachhinweise, um vom Ursprung des Angriffs abzulenken und stattdessen andere Akteure zu belasten (Steffens 2017). Wer hinter einem Cyberangriff steckt, lässt sich nur schwer ermitteln, und eine genaue Attribution dauert oft Monate bis Jahre. Eine aktive Cyberabwehr als schnelles Reaktionswerkzeug riskiert, die Falschen zu treffen. Zudem ist es schwierig, Fähigkeiten zum Gegenangriff außerhalb akuter Cyberangriffe zu demonstrieren, was ihren Abschreckungseffekt stark einschränkt. Dazu kommt, dass das Ergebnis einer aktiven Cyberabwehr nicht unbedingt sichtbar auf Deutschland zurückgeführt werden kann, auch Bekenntnisse strittig gestellt werden können und somit Abschreckungslogiken weiter abgeschwächt werden.

Die Umsetzung dieses Ansatzes wirft weitere Probleme auf. Sollte dringlich aktiv in ausländische Systeme eingegriffen werden müssen, vollzieht sich eine solche Handlung im Ausland, ähnlich einem Bundeswehreinsatz. Deshalb sollte ein solches Vorgehen mindestens einem Parlamentsvorbehalt unterstehen, also eine Zustimmung durch den Deutschen Bundestag erfordern. Eine parlamentarische Kontrolle über aktive Abwehr würde Transparenz und eine breite demokratische Unterstützung der Aktivitäten stärken sowie signalisieren und zudem erfordern, dass vor einem aktiven Gegenangriff mildere Mittel ausgereizt werden.

Aufbau eines Cyberhilfswerks (CHW)

Reaktionsfähigkeit auf digitale Angriffe zu stärken muss bedeuten, im Falle eines großflächigen Cyberangriffs, einer sogenannten Cyber-Großschadenslage, schnell und koordiniert reagieren zu können. Hier hilft ein Blick in den zivilen Katastrophenschutz: Bei der Flutkatastrophe im Ahrtal oder dem tagelangen Stromausfall in Berlin im Januar 2026 haben zivile, in Teilen ehrenamtliche Einsatzkräfte wesentlich dazu beigetragen, die Versorgung der Bevölkerung sicherzustellen. Vergleichbare Unterstützungsstrukturen braucht es dringend auch im Cyberraum, etwa durch den Aufbau eines Cyber-Hilfswerks (CHW).

Ziel des CHW ist es, in einer Großschadenslage mit betroffenen kritischen Infrastrukturen durch einen Cyberangriff schnell zivile Helfende bereitzustellen. Sie könnten vor Ort und digital in der Bewältigung eines großen Schadens an IT-Infrastruktur bei der Versorgung der Zivilbevölkerung sowie der Unterstützung in der Wiederherstellung essenzieller kritischer Dienstleistungen wie z. B. Strom oder Geldflüsse tätig werden. Ein solches CHW wird seit mehreren Jahren von der AG KRITIS gefordert (AG KRITIS 2025). Bis Ende 2025 hat das BMI eine Machbarkeitsstudie zum Aufbau des Bereichs Cyberhilfe, angesiedelt beim THW, beauftragt (Bundesanstalt Technisches Hilfswerk o. D.). Ein Bericht liegt Stand Juli 2026 bisher nicht vor.

Die Bundesregierung sollte Geld in die Hand nehmen, um mit einem CHW Strukturen zu schaffen, die eine schnelle Reaktion auf Cyberangriffe gegen kritische Infrastrukturen unterstützen können und dabei die Zivilgesellschaft einbinden, um diese zu schützen und um ihre Expertise einzubinden. Diese Strukturen sollten vergleichbar mit dem THW institutionell angebunden sein, sie könnten aber durch kleine ehrenamtliche Task Forces starten. Niedrigschwellig könnte man auch damit beginnen, zunächst Interesse und Kapazitäten von Freiwilligen für ein Cyber-Hilfswerk abzufragen und zu bündeln, eine solche Übersicht gibt es aktuell nicht.

Nicht zuletzt hat sich die Bundesregierung im Rahmen der NATO dazu verpflichtet, 1,5 Prozent des BIP für zivile Verteidigung einzusetzen, und mit der Aushebelung der Schuldenbremse 2025 eine entsprechende Finanzierung ermöglicht.

2.2 Schutz des digitalen Informationsraums

Propaganda und Manipulation des gegnerischen Informationsraums begleiten Kriegsführung nach innen und nach außen. Das gilt auch in klassischen Systemkonflikten und Grauzonenkonflikten, d. h. Aggressionen unterhalb der Schwelle eines offenen, bewaffneten Konflikts, wie sie heute zwischen Demokratien und Autokratien herrschen (Keller 2023: 66ff.). So sollen die Stimmung und Moral im eigenen und gegenüberstehenden Lager beeinflusst werden. In Zeiten digitaler Öffentlichkeit und generativer KI-Tools stehen für FIMI und Desinformationskampagnen neue Möglichkeiten bereit, die mit Blick auf die Verbreitung ganz neue Ausmaße erreicht haben (Barela 2024: 4ff.).

Der Begriff Desinformation hat sich inzwischen auch in der öffentlichen Debatte etabliert und dort praktisch die Nachfolge der Bezeichnung Fake News angetreten. Beide Begriffe greifen jedoch im Kontext von FIMI eigentlich zu kurz, da sie eine Täuschungsintention voraussetzen (Jaursch/Sänderlaub 2020: 33f.). Der Auswärtige Dienst der EU definiert FIMI auf seiner Homepage EUvsDesinfo daher wie folgt:

> „FIMI stellt die Weiterentwicklung moderner Propaganda dar: eine koordinierte und technologisch gestützte Form ausländischer Einmischung, die auf die Grundfesten demokratischer Gesellschaften abzielt. Während sich Desinformation auf falsche Informationen an sich konzentriert, ermöglicht uns der Begriff FIMI den Blick auf die umfassendere Strategie: die Netzwerke, Absichten und Verhaltensweisen, die feindliche Einflusskampagnen antreiben."
>
> *EUvsDesinfo 2026*

Ein Bestandteil solcher Einmischung können Desinfo-Ops sein, also Operationen zur gezielten Verbreitung von falschen oder irreführenden Informationen. Sie setzen oftmals auf organische Verbreitung. Oft bauen sie auch auf wahrheitsgemäßen Berichten oder echtem Material auf und entkontextualisieren diese, sodass ein falscher Eindruck entsteht, oder sie amplifizieren tendenziöse, organisch erzeugte Berichte, sodass sowohl Reichweite als auch die Wahrnehmung der Reaktionen auf diese Berichte verzerrt werden (Barela 2024: 4ff.).

Insbesondere bei organischer Weiterverbreitung von Desinformationen verschwimmt die Grenze zur Fehlinformation (engl. *misinformation*), also falschen Informationen, die unwissentlich weiterverbreitet werden. Dies ist beispielsweise der Fall, wenn Menschen ein Sharepic mit einem erfundenen Zitat eines Politikers an andere Personen weitersenden, ohne sich der falschen Zuschreibung bewusst zu sein.

Genauso umfasst die öffentliche Debatte über Desinformation auch die künstliche Amplifizierung von organisch geposteten Inhalten durch *inauthentic behaviour*, beispielsweise wenn ein tendenziöser oder schlicht politischer Post einer echten Person durch das massenhafte Liken und Retweeten von Fakeaccounts an Reichweite und

positiver Wahrnehmung gewinnt (Obrenović/Turčilo 2020: 9f.). Neben der künstlichen Manipulation von außen durch dritte Akteure kann eine solche Verzerrung der Reichweite auch von innen, also durch die Plattformbetreibenden, stattfinden. Wenn solche unbegründeten Eingriffe zur Verringerung der Sichtbarkeit von bestimmten Posts stattfinden und insbesondere wenn sie den Nutzenden nicht mitgeteilt und begründet werden, sind sie als sogenannte *Shadowbans* unter dem EU Digital Services Act (DSA) nicht mehr erlaubt. Doch seit Berichten um den Super-Bowl-Tweet von Elon Musk, der weniger Aufmerksamkeit bekam als ein gleichlautender Tweet des US-Präsidenten Joe Biden, was den Tech-Oligarchen daraufhin veranlasst haben soll, seine Reichweite erhöhen zu lassen, sind solche Szenarien der algorithmischen Manipulation bzw. Manipulation von innen besonders ernst zu nehmen (Paul 2023). Denn dieser Reichweiten-Boost zusammen mit Musks Einmischungen in diverse europäische Wahlkämpfe verdeutlicht die geopolitische Bedeutung des digitalen Informationsraums und wie er für außenpolitische Zielsetzungen manipuliert werden kann.

Aus dieser Mischung von Des-, Fehl- und Malinformationen entsteht ein Spannungsfeld zwischen der für Demokratien systemimmanenten Meinungsfreiheit und sicherheitspolitischen Schutzinteressen sowie der für Meinungs- und Willensbildung wichtigen Neutralität verbreiteter Inhalte.

Daraus ergibt sich, dass neben der Löschung und Verfolgung von strafrechtlich relevanten Inhalten insbesondere die Distribution und die Manipulation des Informationsraums besser beobachtet werden müssen. Während kommerzielle Firmen bereits heute intensive datenbasierte Narrativanalysen durchführen und Staaten wie Kanada mit dem *Media Ecosystem Observatory* Programme hierfür unterhalten, werden entsprechende Tools im deutschen politischen Raum wenig eingesetzt und entsprechende Erkenntnisse wenig öffentlich geteilt. Es fehlen klare Strukturen in Ministerien, Kanzleramt und Staatskanzleien sowie im öffentlich-rechtlichen Rundfunk und in anderen Medien, um auf solche Analysen reagieren zu können. Strukturen und Ressourcen sind jedoch Voraussetzung, um Antworten entwickeln und verbreiten zu können, also Desinformationen *debunken* zu können bzw. bestenfalls der Verbreitung vorhergehendes *Prebunking* vornehmen zu können.

Verbindliche Content Credentials

Heutzutage können Deepfakes und vollständig KI-generierte Bilder, Videos und Tonaufnahmen einfach und massenhaft erzeugt werden. Die von Tech-Firmen 2024 unterschriebenen, auf Freiwilligkeit basierenden und unverbindlich formulierten *Tech Accord to Combat Deceptive Use of AI in 2024 Elections* sind wenig überraschend wirkungslos verpufft (Munich Security Conference 2024). Sie waren eine klassische Pseudo-Selbstverpflichtung, um den Regulationsdruck zu senken. Doch *AI-Slop* ist auf den Plattformen omnipräsent (Curtis 2025), und trotz der theoretischen Verpflichtung, solche künstlich generierten Inhalte zu kennzeichnen, geschieht dies oft nicht.

Dies hat weitreichende Konsequenzen für die demokratische Meinungsbildung im öffentlichen Raum: Künstlich und authentisch generierte Inhalte können teilweise kaum mehr voneinander unterschieden werden. Daher wird eine Kennzeichnungspflicht immer wichtiger, denn jüngst zeigte eine Studie des CISPA Helmholtz Center for Information Security: „Kennzeichnungen [… verändern] die Art und Weise menschlicher Informationsbewertung […]. Labels wirken wie mentale Abkürzungen: Sie lenken Aufmerksamkeit und beeinflussen Vertrauen, und zwar oft stärker als der Inhalt selbst." (Koltermann 2026) *Content Credentials*, die eine Art Beipackzettel mit Bearbeitungs- und Erstellungsinformationen in den Metadaten hinterlegen, können hier helfen. Es braucht entsprechende Verpflichtungen für Bild-, Ton- und Videobearbeitungssoftwares und generative KI-Tools, solche *Content Credentials* zu generieren und den erzeugten Daten anzuhängen. Plattformen dürfen diese nicht löschen, müssen Zero-click-Sichtbarkeit für entsprechende Labels gewährleisten und nachgewiesene Verstöße gegen Kennzeichnungspflichten als Verstoß gegen die Communityrichtlinien mit Strafen bis hin zu Accountsperren ahnden.

Kontextualisierungsmechanismen

Video- und Tonaufnahmen, aber auch Fotos und Textfragmente können durch Ausschnitte oder anderen fehlenden Kontext stark irreführend wirken. Solche Darstellungen lassen sich durch Kontexthinweise korrigieren. Ein Beispiel dafür sind die *Community Notes* (dt. Gemeinschaftsnotizen) von X (vormals Twitter). Dabei können Nutzende pseudonymisiert entsprechenden Kontext hinzufügen. Dieser wird von anderen Nutzenden pseudonymisiert auf Notwendigkeit und Qualität bewertet. Erreicht ein Hinweis ausreichend qualifizierte Zustimmung durch die Bewertungen, wird diese Notiz unter dem Ursprungspost angezeigt, und die Reichweite des Beitrags wird eingeschränkt (Slaughter et al. 2025). So lassen sich verfälschte Darstellungen debunken, also als falsch oder irreführend kenntlich machen. Solche Kontexthinweise können auch von *Trusted Flaggers* stammen, also externer Expertise, die bisher Plattformen auf Inhalte mit Verdacht auf Rechtwidrigkeit hinweisen. Derartige Mechanismen (möglichst offen und transparent gestaltet) und inklusive passender Benachrichtigungsfunktion für Nutzende, die bereits mit markierten Posts interagiert haben, sollten für sehr große Plattformen (*Very Large Online Platforms*, VLOPs, unter dem DSA) verpflichtend werden.

Klarer Rechtsrahmen gegen Distributionsmanipulation

Bereits heute gilt in Deutschland in der Rechtsprechung: Der Kauf von Likes, Kommentaren oder anderen Interaktionen, die Reichweite künstlich erhöhen und Popularität vortäuschen, kann als unlautere geschäftliche Handlung gelten. Auch die Nutzungsbedingungen vieler Plattformen verbieten den Erwerb unechter Follower und Interaktionen. Nach dem DSA sind Plattformbetreiber zudem verpflichtet, ihre Regeln wirksam durchzusetzen und gegen missbräuchliche Praktiken vorzugehen. Auch ein solches

inauthentic behaviour, also die koordinierte Manipulation von Algorithmen und Contentdistribution durch Fake Accounts oder Bots, muss nach Art. 34 Abs. 2 von den VLOPs in ihre Risikobewertungen einbezogen werden, nach Art. 35 DSA sind sie zu entsprechender Risikominderung verpflichtet.

Bei all diesen Ansätzen stehen jedoch bislang vor allem die manipulative Handlung der Käufer*innen und die Pflichten der Plattformen im Mittelpunkt. Gerade aufgrund von internationaler Einmischung und sich daraus ergebender Notwendigkeit zu Rechtshilfeersuchen und diplomatischer Reaktionsfähigkeit sollte sich der Fokus ändern. Er sollte auch stärker auf diejenigen gerichtet werden, die solche Manipulationsleistungen kommerziell anbieten und damit ein eigenes Geschäftsmodell der Desinformation und Einflussnahme betreiben. Sie sollten je nach Schwere mit Gegenmaßnahmen wie Strafverfolgung, Sanktionen oder Einreiseverboten rechnen. Dafür braucht es eine klare gesetzliche Grundlage, die das Anbieten und Vermarkten von Distributionsmanipulation als eigenständige, sanktionierbare Handlung erfasst.

2.3 Abschreckung durch diplomatische Reaktionsfähigkeit

Während konkrete Antworten auf digitale Angriffe notwendig sind, ist drittens auch eine stärkere und koordinierte diplomatische Handlungsfähigkeit gefordert. Dazu gehören mehr europäische Kohärenz und Konsequenz in der digitalen Außenpolitik, digitale Angriffe müssen zudem stärker sanktioniert werden. Ebenso wichtig ist es, auf hybride Bedrohungen nicht mehr isoliert voneinander zu reagieren, sondern Maßnahmen aufeinander abzustimmen und stärker zu verzahnen. Um digitalen Angriffen auf Menschenrechte klar entgegenzutreten, sollte die EU eine *Digital Human Rights Toolbox* als europäischen Reaktionsmechanismus z. B. auf Internet-Shutdowns aufbauen.

Stand der digitalen Diplomatie der EU

Mit dem Strategischen Kompass hat der Rat der Europäischen Union 2022 gemeinsame Leitlinien zur Stärkung europäischer Sicherheit und Verteidigung bis 2030, darunter koordinierte Antworten auf hybride Bedrohungen, beschlossen (Europäischer Rat/Rat der Europäischen Union o. D. a). Ausgangspunkt dieser gemeinsamen Erklärung ist der Umstand, dass die Abwehr hybrider Bedrohungen im Kompetenzbereich der nationalen Mitgliedstaaten selbst liegt. In der Folge hat die EU in einer *EU Hybrid Toolbox* u. a. den Aufbau von *Rapid Response Teams* beschlossen, um koordiniert auf hybride Bedrohungen reagieren und betroffene Mitgliedstaaten unterstützen zu können (Europäischer Rat/Rat der Europäischen Union o. D. b). Während die *EU Hybrid Toolbox* als übergreifender Rahmen dienen soll, schreiben die *EU Cyber Diplomacy Toolbox* in ihrer ersten Version 2017 (Council of the European Union 2023) sowie die *EU FIMI Toolbox* 2022 (Council of the European Union 2022) spezifische Instrumentarien für

koordinierte Reaktionen gegen Cyberbedrohungen und FIMI fest. Diese Maßnahmen zeigen die Erkenntnis der EU, dass hybride Bedrohungen mehr und mehr verschränkt stattfinden und nicht mehr losgelöst voneinander betrachtet werden können und deshalb kohärent und koordiniert angegangen werden müssen.

Mit Blick auf den Cyberraum hat sich die EU in ihren außenpolitischen Prioritäten der Vision eines „globalen, offenen, freien, stabilen und sicheren Cyberspace" verschrieben (Council of the European Union 2023). In einer ersten Erklärung auf Grundlage dieser Zielsetzung hat die EU die *Cyber Diplomacy Toolbox* erstmals im Jahr 2017 auf den Weg gebracht. Die Leitlinien zur Umsetzung der *Cyber Diplomacy Toolbox* wurden 2023 vom Rat grundlegend überarbeitet (Council of the European Union 2023: 2ff.). Hintergrund des Vorstoßes war u. a. die Erkenntnis, dass gestiegenen Cyberbedrohungen, insbesondere seit den russischen Aggressionen gegen die Ukraine, kohärente, sich gegenseitig verstärkende diplomatische Antworten im Bereich Cyber- und Digitalpolitik entgegengesetzt werden müssen.

Beim Aufbau einer *EU FIMI Toolbox* zielt das Instrumentarium besonders auf vier Aspekte ab: Lageerkennung, Resilienz und Kapazitätsaufbau, regulatorische sowie diplomatische Antworten (European Union External Action Service 2026). Auf diplomatischer Ebene haben sich Mitgliedstaaten und EU-Institutionen beispielsweise zu mehr Austausch und Koordination von Maßnahmen in der Detektion von FIMI, in der Sanktionierung von FIMI-Akteuren sowie der politischen Attribution, also der Zuweisung der Urheberschaft von Angriffen, bekannt.

Europäische Kohärenz in der Attribution und Sanktionierung von digitalen Angriffen

Die EU ist in den vergangenen Jahren wichtige Schritte gegangen, um diplomatische „Werkzeugkästen" zu schaffen und diese mit konkreten Maßnahmen gegen hybride Bedrohungen, Desinformation und Cyberangriffe zu füllen. Diese Maßnahmen sind wichtig. Gleichzeitig entscheiden die europäische Einigkeit, Kohärenz und Koordination einer Attribution maßgeblich über den Erfolg und die Glaubwürdigkeit ihres Signalling-Effektes. In einer Analyse legte die Stiftung Wissenschaft und Politik (SWP) anschaulich dar, wie in der Vergangenheit diplomatische Attributionen in ihrer Wirksamkeit begrenzt waren: Dies lag an verzögerten, monate- bis jahrelangen europäischen Attributionsprozessen und der fehlenden Einigkeit in der politischen Attribution europäischer Mitgliedstaaten, mangelnder Kommunikation (Bendiek/Schulze 2021: 37ff.). Angesichts der angespannten sicherheitspolitischen Lage müssen die EU und ihre Mitgliedstaaten ihre Handlungsfähigkeiten stärken: Mitgliedstaaten müssen ihre Erkenntnisse transparenter machen und die Attribuierung nach einem digitalen Angriff deutlich schneller europaweit koordinieren und gemeinsam öffentlich erklären. Attributionsprozesse sollten auf europäischer Ebene stattfinden, anstatt parallele, oft redundante nationale Prozesse nebeneinander laufen zu lassen (ebd.). Für Sanktionen

auf digitale Angriffe braucht es eine klare Sprache – diese muss gemeinsam von den Mitgliedstaaten getragen werden.

Kohärente Governance, um hybride Bedrohungen integriert anzugehen

Cyberangriffe, Desinformationskampagnen, Sabotage von digitalen Infrastrukturen oder Spionage finden nicht isoliert voneinander statt. Im Vergleich zu konventionellen Angriffen verbindet sie, dass die Urheberschaft von Angriffen, die Motivlage und Verletzung von territorialer Souveränität viel schwieriger anzuzeigen sind.

Gleichzeitig findet die Governance unterschiedlicher hybrider Bedrohungselemente in der Außenpolitik oft getrennt statt: Im Auswärtigen Amt etwa findet ein Austausch zwar teamübergreifend statt, die zuständigen Referate zu Cybersicherheit und strategischer Kommunikation sind aber in unterschiedlichen Abteilungen angesiedelt. Die strukturelle Zusammenführung dieser Expertise wird mit der Reform des Hauses unter Außenminister Johann Wadephul eher ab- als ausgebaut. Ein kohärenter Ansatz für die Analyse und Reaktion auf hybride Bedrohungen innerhalb der gesamten Bundesregierung wird nun mit dem Nationalen Sicherheitsrat versucht.

Für einen ganzheitlichen Blick braucht das Auswärtige Amt eine kohärente Governance, die durch integrierte Kompetenzen in einer Abteilung für hybride Bedrohungen entstehen könnte. Mit Blick auf die gesamte Bundesregierung müsste die Arbeitsgruppe Hybride Bedrohungen sowie das neu im Juni 2026 eingerichtete Gemeinsame Zentrum zur Abwehr Hybrider Bedrohungen (GAZ) für Behörden zu einer Gesamtkoordination mit nationaler Risikoanalyse ausgebaut werden, einschließlich einer Bund-Länder-Koordinierung.

Für die Nutzung von Lagebildern auf europäischer Ebene etwa infolge eines Cyberangriffs sollte explizit auch das ganzheitliche hybride Bedrohungsbild, z. B. vorgelagerte Desinformationskampagnen, in den Blick genommen werden. Während die *EU Hybrid Toolbox* hybride Bedrohungen insgesamt adressiert, sind die bisher konkret festgehaltenen Attributionsprozesse für Cyberangriffe und Desinformation weiterhin strukturell getrennt. Diese Verschränkung muss deutlich gestärkt werden.

Aufbau einer *Digital Human Rights Toolbox*

Auf Menschenrechtsverbrechen, die ihren Ursprung im digitalen Raum nehmen und die auch über digitale Gewalt hinausgehen, muss klar und schnell reagiert werden können. Angriffe auf die Persönlichkeitsrechte, die informationelle Selbstbestimmung und die Sicherheit von Menschen werden inzwischen systematisch von autoritären Regimen eingesetzt. Das betrifft die demokratische Community weltweit, auch und gerade dann, wenn bedrohte Menschen Zuflucht suchen (vgl. Neumann 2026). Während für Cyberangriffe die *Cyber Diplomacy Toolbox* bereits Abläufe und Reaktionen vorgibt, sollte diese um Maßnahmen auf Menschenrechtsverletzungen im digitalen Raum erweitert werden. Eine *Digital Human Rights Toolbox* sollte neben

diplomatischen Reaktionen und möglichen Sanktionen gegen Cyberattacken auf Dissidenten, Oppositionelle und die Grundrechtsverletzung marginalisierter und vulnerabler Gruppen auch strukturelle Einschränkungen wie beispielsweise Internet-Shutdowns klar angehen. Entziehen Staaten ihrer Bevölkerung das Grundrecht auf informationelle Selbstbestimmung, z. B. durch Internet Shutdowns oder digitale Massenüberwachung, so werden die Grundrechte auf Meinungs- und Informationsfreiheit eingeschränkt (Klimke 2020). Ein solches internationales Engagement setzt voraus, dass diese digitalen Grundrechte in Deutschland ebenfalls geachtet werden (vgl. Teil 1 der Dimensionen digitaler Außenpolitik, Bacherle/Locher 2026).

Countering FIMI Framework

Neben der klaren rechtlichen Regelung zur gewerblichen oder transaktionalen Distributionsmanipulation braucht es in der FIMI-Toolbox zudem EU-weit klare Antworten auf solche Einmischungen in den Informationsraum. Betreibende, Finanziers und Auftraggebende von Bot- und Fake-Account-Farmen sollen mit Sanktionen und öffentlichen Gegenmaßnahmen rechnen müssen. So kann das Geschäftsmodell zerstört und als Betätigungsfeld unattraktiver werden. Bisher haben die Betreibenden meist keinerlei Konsequenzen zu befürchten. Um das zu ändern, müssen Informationen über Betreibende und Auftraggebende strukturiert gesammelt und anschließend gezielt eingesetzt werden (Miller 2024). Um dies zu gewährleisten, braucht es eine gut aufgestellte, zentrale Stelle, die ihre Erkenntnisse nicht nur dem Auswärtigen Amt und dem EU External Action Service, sondern auch der Öffentlichkeit zur Verfügung stellt. Es muss unbedingt vermieden werden, dass solche Ansätze durch föderale oder ministerielle Einzelgänge oder Befindlichkeiten unkoordiniert bleiben.

3 Fazit: Klare und schnelle Handlungs- und Reaktionsfähigkeit in der digitalen Außenpolitik

Hybride Bedrohungen erfordern eine digitale Außenpolitik, die digitale Menschenrechte konsequent wahrt und klare Strukturen für glaubwürdige, schnelle und koordinierte Reaktionen vorhält. Statt *Hackbacks* braucht es eine defensive, kooperativ eingebettete Cyberabwehr aus schneller Detektion, Wiederherstellung und Krisenbewältigung sowie effektive parlamentarische Kontrolle, falls dies dennoch politisch notwendig sein sollte, ergänzt um ein Cyberhilfswerk für zivile Großschadenslagen. Zur Eindämmung von Desinformation sind ein Maßnahmenpaket aus verbindlichen *Content Credentials* für KI-generierte Inhalte, Mechanismen zur Transparenz und Kontextualisierung auf Plattformen, Sanktionen gegen professionelle Distributionsmanipulation sowie klare Zuständigkeiten für schnelle Reaktionen notwendig. Schließlich müssen Kompetenzen und Koordination auf europäischer Ebene ausgebaut werden. Dies ist nötig, um die ganzheitliche diplomatische Reaktionsfähigkeit auf hybride Bedrohungen, über einzelne Reaktionen auf Cyberangriffe, Einmischungen und Menschenrechtsverletzungen hinaus, zu stärken und klar reagieren zu können. Zusätzlich sollte Deutschland für eine kohärente, gesamtstaatliche Governance für hybride Bedrohungen sorgen und die EU eine *Digital Human Rights Toolbox* etablieren, um gegen digitale Repressionen wie Internet-Shutdowns effektiv handeln zu können. So können Deutschland und Europa klare und schnelle Handlungs- und Reaktionsfähigkeit in der digitalen Außenpolitik erreichen.

Literaturverzeichnis

AG KRITIS (2025): Das Cyber-Hilfswerk. Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen; in: ag.kritis.info, 23.3.2025, https://ag.kritis.info/wp-content/uploads/2025/03/chw-konzept_v1.2_final.pdf, Zugriff 9.6.2026

AG KRITIS (2026): Stellungnahme zum Ref-E des Bundesministeriums des Innern (BMI) für ein Gesetz zur Stärkung der Cybersicherheit; in: ag.kritis.info, 12.3.2026, https://ag.kritis.info/wp-content/uploads/2026/03/20260311-AG_KRITIS_Stellungnahme_Cyberabwehr_-_final.pdf, Zugriff 9.6.2026

Barela, Steven J. (2024): Digital Disinformation Operations: Part I. Synthetic Forces vs. Humans and Human Rights; in: The Geneva Academy, https://archives.geneva-academy.ch/joomlatools-files/docman-files/Digital%20disinformation%20operations%20Part%20I%20(1).pdf, Zugriff 23.6.2026

Bendiek, Annegret/Schulze, Matthias (2021): Attribution als Herausforderung für EU-Cybersanktionen. Eine Analyse von WannaCry, NotPetya, Cloud Hopper, Bundestag-Hack, OVCW; in: Stiftung Wissenschaft und Politik SWP-Studie 17 vom Oktober 2021, S. 1-47, https://www.swp-berlin.org/publications/products/studien/2021S17_AttributionCyberangriffe.pdf, Zugriff 9.6.2026

Beuth, Patrick/Wiedmann-Schmidt, Wolf (2021): »Ghostwriter«-Kampagne: Steckt Belarus hinter Hackingversuch gegen deutsche Abgeordnete?; in: DER SPIEGEL, 16.11.2021, https://www.spiegel.de/netzwelt/netzpolitik/belarus-steckt-minsk-hinter-hackingversuch-gegen-deutsche-abgeordnete-a-a2316269-a930-4250-aaa3-209127631f6b, Zugriff 9.6.2026

BSI (2025): Zusammenfassung und Bewertung. BSI Lagebericht 2025; in: medien.bsi.bund.de, https://medien.bsi.bund.de/lagebericht/de/zusammenfassung-und-bewertung/, Zugriff 9.6.2026

Bundesamt für Verfassungsschutz (2025): Vorstellung der Bitkom-Studie „Wirtschaftsschutz 2025“; in: https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2025/2025-09-18-studie-bitkom.html, Zugriff 9.6.2026

Bundesanstalt Technisches Hilfswerk (o. D.): Cyberhilfe-MaSt; in: https://www.thw.de/SharedDocs/Downloads/DE/Forschung/cyberhilfe_mst_steckbrief.pdf?__blob=publicationFile&v=3, Zugriff 23.6.2026

Bundesministerium des Innern (2025): Pressemitteilung. Stärkung der Cybersicherheit – Kabinett beschließt Eckpunkte zur Erhöhung der Cybersicherheit; in: bmi.bund.de, 27.8.2025, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2025/08/beschluss-staerkung-cs.html, Zugriff 9.6.2026

Bundesministerium des Innern (2026): Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Stärkung der Cybersicherheit; in: bmi.bund.de, 21.5.2026, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/cyberabwehr-regierungsentwurf.pdf?__blob=publicationFile&v=1, Zugriff 31.5.2026

Council of the European Union (2022): Council conclusions on Foreign Information Manipulation and Interference (FIMI); 11429/22; in: data.

consilium.europa.eu, 18.7.2022, https://data.consilium.europa.eu/doc/document/ST-11429-2022-INIT/en/pdf, Zugriff 9.6.2026

Council of the European Union (2023): Revised Implementing Guidelines of the Cyber Diplomacy Toolbox; 10289/23; in: data.consilium.europa.eu, 8.6.2023, https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf, Zugriff 9.6.2026

Curtis, Liam (2025): AI Slop Report: The Global Rise of Low-Quality AI Videos; in: Kapwing Company Blog, 28.11.2025, https://www.kapwing.com/blog/ai-slop-report-the-global-rise-of-low-quality-ai-videos/, Zugriff 9.6.2026

Deutscher Bundestag (2023): Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU – Drucksache 20/5070 – Verteidigung im Cyberraum – EU-Kooperation und aktive Cyberverteidigung; Drucksache 20/5597; in: bundestag.de, 9.2.2023, https://dserver.bundestag.de/btd/20/055/2005597.pdf#:~:text=Eine%20–%20aktive%20–%20Maßnahme%20der%20Cyberabwehr%2C,umfasst%20die%20in%20der%20Bundeswehr%20für%20die, Zugriff 9.6.2026

Europäischer Rat/Rat der Europäischen Union (o. D. a): Ein Strategischer Kompass für Sicherheit und Verteidigung; in: consilium.europa.de, https://www.consilium.europa.eu/de/policies/strategic-compass/, Zugriff 9.6.2026

Europäischer Rat/Rat der Europäischen Union (o. D. b): Hybride Bedrohungen; in: consilium.europa.de, https://www.consilium.europa.eu/de/policies/hybrid-threats/, Zugriff 9.6.2026

European Union External Action Service (2018): A Europe that Protects: Countering Hybrid Threats; in: EEAS,13.6.2018, https://www.eeas.europa.eu/node/46393_en, Zugriff 9.6.2026

European Union External Action Service (2026): Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI); in: eeas.europa.eu, 27.1.2026, https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en, Zugriff 9.6.2026

EUvsDesinfo/EU External Action Service (2026): Ausländische Informationsmanipulation und Einmischung (FIMI) erklärt; in: euvsdisinfo.eu, 15.3.2026, https://euvsdisinfo.eu/de/auslaendische-informationsmanipulation-und-einmischung-fimi-erklaert/, Zugriff 12.4.2026

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 9.6.2026

Harnisch, Sebastian/Zettl, Kerstin (2020): Blame Game im Cyberspace. Informationstechnik als Waffe?; in: Ruperto Carola 16 (2020): S. 96–105

Herpig, Sven/Dutke, Frederic (2023): Deutschlands staatliche Cybersicherheitsarchitektur; 11. Aufl., Stiftung Neue Verantwortung, https://www.interface-eu.org/storage/archive/files/cybersicherheitsarchitektur_elfteauflage1123.pdf, Zugriff 9.6.2026

Jaursch, Julian/Sängerlaub, Alexander (2020): Desinformation als Arbeitsfeld der Medeinaufsicht; in: Was ist Desinformation? Betrachtungen aus sechs wissenschaftlichen Perspektiven, Landesanstalt für Medien NRW, 6.3.2020, https://www.medienanstalt-nrw.de/fileadmin/

user_upload/NeueWebsite_0120/Themen/Desinformation/WasIstDesinformation_Paper_LFMNRW.pdf, Zugriff 9.6.2026

Keller, Patrick (2023): Abschreckung in der Grauzone; in: Internationale Politik, 26.6.2023, https://internationalepolitik.de/de/abschreckung-der-grauzone, Zugriff 9.6.2026

Klimke, Romy (2020): Menschenrecht auf einen Internetzugang?; in: Verfassungsblog, 26.7.2020, https://verfassungsblog.de/menschenrecht-auf-einen-internetzugang/, Zugriff 9.6.2026

Koltermann, Felix (2026): Transparenz ist nicht gleich Wahrheit: Was Plattformen bei der Kennzeichnung von KI-Bildern beachten müssen; in: Idw Informationsdienst Wissenschaft e. V. Nachrichten aus der Wissenschaft, 1.6.2026, https://nachrichten.idw-online.de/2026/06/01/transparenz-ist-nicht-gleich-wahrheit-was-plattformen-bei-der-kennzeichnung-von-ki-bildern-beachten-muessen, Zugriff 9.6.2026

Lee, Robert M. (2016): Wie lief der Angriff auf das Stromnetz der Ukraine?; in: Security-Insider, 1.2.2016, https://www.security-insider.de/wie-lief-der-angriff-auf-das-stromnetz-der-ukraine-a-519686/, Zugriff 9.6.2026

Lehberger, Roman/Röbel, Sven/Wiedmann-Schmidt, Wolf (2025): Hunderte Autos beschädigt: Deutschlandweite Sabotageserie offenbar von Russland gesteuert; in: DER SPIEGEL, 5.2.2025, https://www.spiegel.de/panorama/justiz/hunderte-autos-beschaedigt-deutschlandweite-sabotageserie-offenbar-aus-russland-gesteuert-a-7625e908-2f28-4ef8-bb69-35e5bacd6125, Zugriff: 9.6.2026

Miller, Carl (2024): Directing Responses Against Illicit Influence Operations (D-RAIL); in: EU DisinfoLab, 19.8.2024, https://www.disinfo.eu/publications/directing-responses-against-illicit-influence-operations-d-rail/, Zugriff 9.6.2026

Munich Security Conference (2024): AI Elections Accord; in: securityconference.org, https://securityconference.org/en/aielectionsaccord/, Zugriff 9.6.2026

Neumann, Hannah (2026): Transnationale Repression: Die unterschätzte Bedrohung für Europas Sicherheit; in: Table.Forum: Neue Sicherheits-Strategien, 20.3.2026, https://table.media/forum/tableforum-neue-sicherheits-strategie/transnationale-repression-die-unterschaetzte-bedrohung-fuer-europas-sicherheit, Zugriff 9.6.2026

Obrenović, Mladen/Turčilo, Lejla (2020): Fehlinformationen, Desinformationen, Malinformationen: Ursachen, Entwicklungen und ihr Einfluss auf die Demokratie; in: boell.de, https://www.boell.de/sites/default/files/2020-08/200825_E-Paper3_DE.pdf, Zugriff 23.6.2026

Paul, Kari (2023): Elon Musk reportedly forced Twitter algorithm to boost his tweets after Super Bowl flop; in: The Guardian, 15.2.2023, https://www.theguardian.com/technology/2023/feb/15/elon-musk-changes-twitter-algorithm-super-bowl-slump-report, Zugriff 9.6.2026

Slaughter, Isaac/Peytavin, Axel/Ugander, Johan/Saveski, Martin (2025): Community notes reduce engagement with and diffusion of false information online; in: Proceedings Of The National Academy Of Sciences, Bd. 122, Nr. 38, 18.9.2025, https://www.pnas.org/doi/epub/10.1073/pnas.2503413122, Zugriff 23.6.2026

Steffens, Timo (2017): Hacker-Jagd im Cyberspace; in: heise magazine c't 14/17, S. 122, https://www.heise.de/select/ct/2017/14/1499030213570537, Zugriff 9.6.2026

Wissenschaftliche Dienste des Deutschen Bundestages (2018): Ausarbeitung. Verfassungsmäßigkeit von sog. „Hackbacks" im Ausland, WD 3 – 3000 – 159/18; in: Deutscher Bundestag, 8.6.2018, https://www.bundestag.de/resource/blob/560900/baf0bfb8f00a6814e125c8fce5e89009/wd-3-159-18-pdf-data.pdf, Zugriff 9.6.2026

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: Juli 2026

Covermotiv: IMAGO/alimdi

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