Deutsche Gesellschaft für Auswärtige Politik

DGAP BERICHT

Aktionsplan Resilienz und Demokratie

Wie Deutschland Angriffe auf Demokratie und Gesellschaft abwehren kann

Prof. Dr. Christian Calliess, LL.M. Eur.
Lehrstuhl für Öffentliches Recht und Europarecht, Freie Universität Berlin

Seit mehreren Jahren stehen die westlichen Demokratien in Europa ebenso wie in Amerika verstärkt unter „digitalem Beschuss". Inländische und ausländische Akteure versuchen mittels hybrider Methoden wie Cyberattacken die öffentliche Meinungsbildung zu ihren Gunsten zu beeinflussen und die Institutionen zu schwächen, um der Demokratie nachhaltig Schaden zuzufügen. Vor allem die Presse gerät aufgrund der Online-Angebote großer digitaler Anbieter immer mehr unter Druck und kann daher ihrem klassischen Auftrag immer weniger gerecht werden. Zugleich ist in einigen Teilen der Bevölkerung ein Vertrauensverlust in Bezug auf die traditionellen Medien und eine Zuwendung zu alternativen, onlinebasierten Medienangeboten (zum Beispiel Facebook, YouTube, Influencer) zu verzeichnen.

Die US-Präsidentschaftswahl 2016 und das Brexit-Referendum haben als Schlüsselereignisse der letzten Jahre die Verwundbarkeit demokratischer Gesellschaften gegenüber gezielten Desinformations- und Propagandakampagnen offengelegt. Die genannten Phänomene stellen sich dabei als Bedrohung für den Prozess der demokratischen Willensbildung sowie für die Integrität von Wahlen und Abstimmungen dar.

Die massive Welle an Falschinformationen und Verschwörungstheorien während der Corona-Pandemie hat gezeigt, dass Krisenzeiten mit unsicherer Informationslage ebenfalls bewusst ausgenutzt werden können, um Unsicherheit in der Bevölkerung zu verbreiten, die gesellschaftliche Spaltung voranzutreiben sowie das Vertrauen in staatliche Maßnahmen zur Krisenbewältigung zu untergraben. Neben dem Schutzgut Demokratie sind somit auch die innere und äußere Sicherheit der Bundesrepublik betroffen.

Seit Jahren kommt es schließlich immer wieder zu Hackerangriffen auf staatliche Institutionen (insbesondere den Deutschen Bundestag), die deren Funktions- und Handlungsfähigkeit und damit die Demokratie selbst gefährden.

HERAUSFORDERUNGEN

Gelingt es nicht, zeitnah eine Antwort auf die neuen Bedrohungen zu finden, droht die Demokratie irreversiblen Schaden zu nehmen. Ziel der Bemühungen muss es sein, die digitale und demokratische Resilienz innerhalb Deutschlands und der EU zu stärken und die Gesellschaften Europas gegen Angriffe aus dem In- und Ausland zu immunisieren.

Als besondere Herausforderung stellen sich die Komplexität und Vielschichtigkeit der neuen Bedrohungslandschaft dar, die ein Zusammenwirken verschiedenster Akteure auf mehreren Ebenen erfordert und eine Vielzahl möglicher Handlungs- und Aktionsfelder eröffnet. Demokratie ist im demokratischen Verfassungsstaat eine gemeinsame Verantwortung von Politik und Gesellschaft, EU und Mitgliedstaaten, Unternehmen und Verbrauchern, wobei kein Akteur imstande ist, die Probleme allein zu lösen.

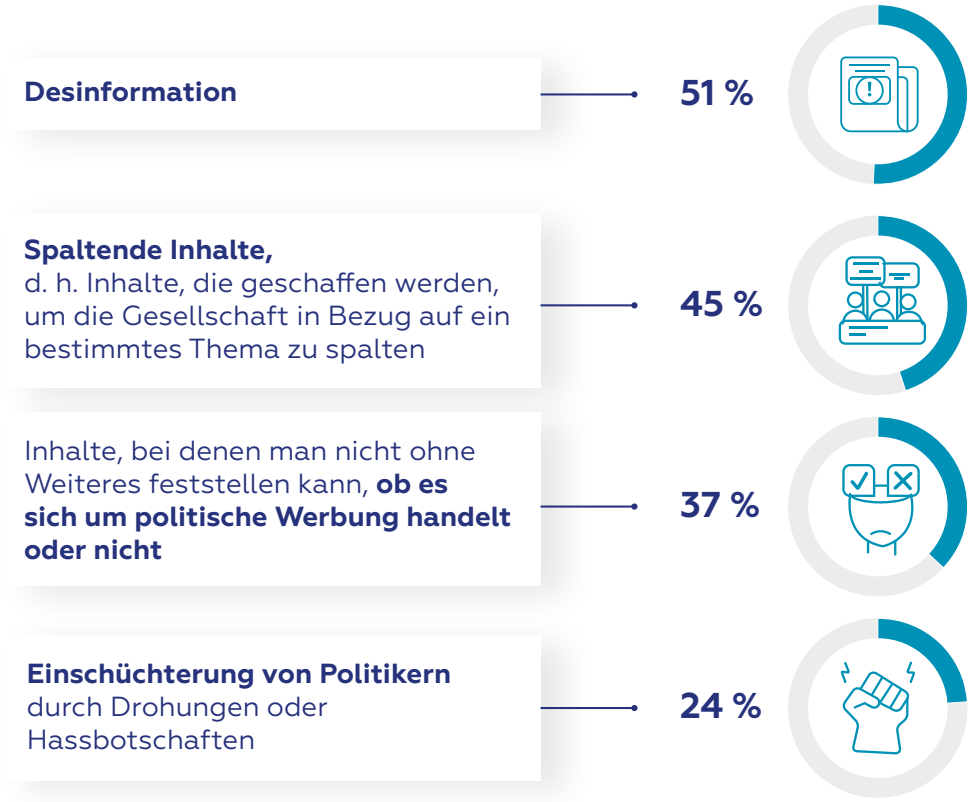
Der Themenkomplex Desinformation und Propaganda betrifft zudem eine Grauzone der für die Demokratie unabdingbaren Informations- und Meinungsfreiheit. Zur Vermeidung ungerechtfertigter Eingriffe in diese Freiheitsrechte sowie des Vorwurfs staatlicher Zensur ist daher ein differenziertes und abgestuftes Vorgehen erforderlich. Gezielte staatliche Maßnahmen gegen einzelne Inhalte kommen daher – wenn überhaupt – nur als Ultima Ratio in Betracht.

Inzwischen bezieht deutlich mehr als ein Drittel der Bürger politische Informationen aus sozialen Netzwerken. Seit bekannt wurde, dass Drittstaaten oder von ihnen bezahlte private Akteure diese Plattformen zielgerichtet nutzen, um das Vertrauen der Bürger in die Demokratie durch Desinformation und Propaganda zu erschüttern, sind diese Netzwerke allerdings zunehmend in den Fokus der Kritik geraten.

Die Zahl alternativer Online-Medien, über die gezielt Falschinformationen und Propaganda oder zumindest stark ideologisch eingefärbte Inhalte verbreitet werden, wächst. Gesunkene Produktionskosten und verbesserte technische Möglichkeiten lassen diese Formate professionell erscheinen, wodurch es den Bürgern erschwert wird, sie von seriösen Nachrichten zu unterscheiden. Zugleich ist die Medienkompetenz vieler Nutzer bislang eher gering. Hinzu kommen Nachrichtenangebote wie Russia Today (RT) oder Sputnik, die von ausländischen Akteuren gesteuert und ebenfalls als Mittel zur Verbreitung von Propaganda eingesetzt werden.

Europäerinnen und Europäer kommen häufig mit schädlichen oder illegalen Online-Praktiken in Berührung

EU-weit gaben befragte Internetnutzerinnen und Internetnutzerinnen an, dass sie schädlichen illegalen Praktiken in der Online-Umgebung ausgesetzt waren oder Zeugen davon geworden sind.



Quelle: Special Eurobarometer 507, https://t1p.de/n4f29

Empfehlungen

Schaffung einer resilienten Öffentlichkeit

Weder Desinformation noch Propaganda oder politische Werbung sind gänzlich neue Phänomene des digitalen Zeitalters. Um den durch das Internet bedingten Veränderungen der Informationsvermittlung und -wahrnehmung entgegenzuwirken, sollte in die Schaffung und Aufrechterhaltung einer resilienten Öffentlichkeit investiert werden. Konkret sollte es darum gehen, den Zugang zu vertrauenswürdigen, gut recherchierten Inhalten zu erleichtern, die Medienkompetenz der Bürgerinnen und Bürger zu stärken sowie ein Informationsökosystem zu schaffen, in dem Desinformation und Propaganda leichter als solche identifiziert werden können.

1. Presse und Rundfunk stärken

Vor dem Hintergrund einer für den Einzelnen nicht mehr zu bewältigenden Fülle an Nachrichten, die heutzutage über das Internet verfügbar sind, sind Menschen mehr denn je auf die Auswahl und Aufbereitung von Informationen durch die Institutionen der Presse und des Rundfunks angewiesen. Dabei kommt vor allem dem öffentlich-rechtlichen Rundfunk die Schlüsselrolle zu, die Grundversorgung der Bürger mit vertrauenswür-

digen und faktengeprüften Inhalten zu gewährleisten. Um künftig die Versorgung mit qualitativ hochwertigen Nachrichten sicherzustellen, bedarf es einer Stärkung der freien Presse. Auch ein regulatorisches Eingreifen mit dem Ziel, ein „level playing field" zwischen Internetkonzernen und Medienanbietern zu schaffen, kann sinnvoll sein. Dies kann vor allem durch die Ausweitung des neuen Medienstaatsvertrages auf die Betreiber von sozialen Netzwerken geschehen, die auf diese Weise vergleichbare Verantwortlichkeiten und Pflichten hinsichtlich der Berichterstattung übernehmen müssen.

Anders als in der rein privat ausgestalteten US-Medienlandschaft, deren Polarisierung einen erheblichen Beitrag zur gesellschaftlichen Spaltung der Vereinigten Staaten leistet, existiert in Deutschland mit dem öffentlich-rechtlichen Rundfunk eine Institution, deren Handeln auf gesellschaftliche Integration angelegt ist. In Hinblick auf den öffentlich-rechtlichen Rundfunk kommt dessen Verpflichtung auf die Grundsätze der Objektivität und Unparteilichkeit der Berichterstattung eine besondere Bedeutung zu. Diesem Auftrag kann der öffentlich-rechtliche Rundfunk langfristig jedoch nur durch eine strikte Beachtung seiner politischen Neutralität gerecht werden.

- Vor dem Hintergrund einer sich stark wandelnden Medienlandschaft muss über eine Neuausrichtung des verfassungsrechtlichen Auftrags des Rundfunks zur medialen Grundversorgung der Bürger nachgedacht werden, wobei künftig ein noch stärkerer Fokus auf der Bereitstellung faktengeprüfter Inhalte liegen sollte.

- In Ergänzung des deutschen öffentlich-rechtlichen Rundfunks sollte zudem über einen Europäischen Öffentlichen Rundfunk nachgedacht werden, der die Politiken der EU und die Entscheidungsprozesse in Brüssel, Straßburg und Luxemburg transparenter und verständlicher macht.

- Ferner könnte eine nicht-staatliche Rating-Agentur geschaffen werden, die ausgerichtet an Kriterien wie etwa der „Faktentreue der Berichterstattung" eine Bewertung der Medienangebote vornimmt. Eine solche Agentur müsste freilich staatsfern und unabhängig ausgestaltet sein und der Kontrolle durch Gerichte unterliegen, um den Eindruck eines „Wahrheitsministeriums" zu vermeiden.

2. Plattformregulierung

Große Online-Plattformen spielen als Gatekeeper heute eine zentrale Rolle bei der Informationsvermittlung. Damit das Vertrauen der Bürger in die Demokratie nicht durch Desinformation und Propaganda erschüttert wird, bedarf es einer Plattformregulierung, die neue – der Rolle als Gatekeeper entsprechende – Verantwortlichkeiten schafft und die Plattformen insgesamt stärker in die Pflicht nimmt.

Die EU-Kommission hat mit ihrem Vorschlag für ein Gesetz über digitale Dienste (DSA) einen ersten wichtigen Schritt in Richtung einer solchen Regulierung unternommen, deren Ziel es ist – ähnlich wie bei der Datenschutz-Grundverordnung – Standards für die sozialen Medien und die Datenerhebung durch Plattformen zu setzen. Darüber hinaus hat die EU angekündigt, Gesetzgebungsvorhaben zur Regulierung der künstlichen Intelligenz sowie zur Transparenz gesponserter politischer Inhalte im Internet auf den Weg zu bringen. Die künftige Bundesregierung sollte sich an diesen Vorhaben – vermittelt über den Rat der EU – aktiv beteiligen und mit eigenen Initiativen einbringen.

- Ein Kernanliegen sollte die Herstellung von mehr Transparenz im Online-Kontext bilden. Die Öffentlichkeit soll wissen können, wer der Auftraggeber einer Anzeige ist und mit wem oder was die Bürger über soziale Medien agieren. Es sollte erkennbar sein, was ein Bot ist und was nicht, und ob eine „Nachricht" aufgrund einer Interaktion mit dem Bot nicht mehr „real" ist.

- Ferner sollte bei Nachrichten mit politischem Inhalt für die Nutzer ersichtlich sein, ob es sich um bezahlte Werbung oder journalistische Inhalte handelt.

- Ebenso sollte die Verantwortung von Plattformen hinsichtlich des Einsatzes von Algorithmen vergrößert und die Kriterien der algorithmischen Nachrichtenauswahl und -präsentation transparenter gemacht werden.

- Auch die bislang selbstverständliche Anonymität im Internet wird zunehmend zu einer Herausforderung. Je mehr sich der Cyberraum zu einer zweiten (virtuellen) Lebenswelt der Menschen entwickelt, desto mehr sollte über Möglichkeiten nachgedacht werden, Identitätsfeststellungen analog der klassischen (realen) Lebenswelt zu ermöglichen. Vorstellbar wäre, dass anonyme „Cyber-Identitäten" (vermittelt über Internet-Avatare) in der analogen Lebenswelt zugeordnet werden können und auf diesem Wege unter bestimmten Voraussetzungen für ihr Handeln zur Verantwortung gezogen werden können.

3. Öffentlichkeitsarbeit

Obgleich die Bundesregierung nicht direkt in den Prozess der öffentlichen Meinungsbildung eingreifen darf, ist es ihr unbenommen, Informations- und Öffentlichkeitsarbeit zu betreiben und die Bevölkerung über das Regierungshandeln zu informieren. Die Bundesregierung sollte in Zukunft verstärkt die Möglichkeiten und die Reichweite der sozialen Netzwerke nutzen, um die Bürger mit vertrauenswürdigen Inhalten zu versorgen. Als Vorbild kann die Kampagne „Zusammen gegen Corona" des Bundesgesundheitsministeriums auf Instagram dienen, in der mittels kurzer, einfach verständlicher Videoclips über die neuesten Erkenntnisse in der Pandemiebekämpfung sowie die Empfehlungen des RKI informiert wird. Auf Gegenpropaganda im eigentlichen Sinne sollte jedoch verzichtetet werden, da Gegendarstellungen aus psychologischer Sicht den Effekt haben können, Menschen erst recht in ihren Vorstellungen zu bestärken.

4. Medienkompetenz stärken

Zwar nimmt die Nutzung sozialer Medien immer mehr zu, die Medien- und Technikkompetenz vieler Nutzer ist bislang jedoch gering ausgeprägt. So weiß etwa die Hälfte der Europäer nicht, was ein Algorithmus ist, geschweige denn wie er funktioniert oder welchen Einfluss Algorithmen auf die Auswahl und Darstellung von Informationen haben. Mittelfristig muss es darum gehen, die Medienkompetenz der Bürger, insbesondere der Jugend im Rahmen der Schulbildung, zu erhöhen und sie für die Mechanismen und Gefahren von Desinformation und Propaganda im Internet zu sensibilisieren.

Hier könnte erneut die Idee einer unabhängigen Rating-Agentur fruchtbar gemacht werden. Denkbar wäre ein Zertifizierungsverfahren, durch das sich Anbieter von Online-Nachrichten die Einhaltung und Beachtung journalistischer Standards nach dem Pressekodex bestätigen lassen könnten. Wie bereits bei Online-Shops üblich, wären Betreiber von Online-Nachrichtendiensten nach erfolgter Prüfung durch die Agentur berechtigt, eine Art Gütesiegel auf ihrer Homepage zu platzieren.

Wenn es um Cybersicherheit geht, gehört das „menschliche Element" nachweisbar zu den größten Sicherheitsrisiken. So wurde der bisher größte Cyberangriff auf den Bundestag im Jahr 2015 erst durch das unbedachte Öffnen von Phishing E-Mails ermöglicht. Dem Ausbau der Medienkompetenz der Bürgerinnen und Bürger kommt daher auch in diesem Bereich erhebliche Bedeutung zu.

Bedrohungen antizipieren, frühzeitig erkennen und reagieren

Ein wichtiger Schlüssel zur Abwehr der neuen Bedrohungen besteht darin, sie frühzeitig zu erkennen, um dann rechtzeitig auf sie reagieren zu können. Die bisherige Erfahrung mit Desinformationskampagnen und Cyberattacken hat gezeigt, dass ein beachtlicher Teil dieser Angriffe orchestriert und anlassbezogen erfolgt und daher unter Umständen antizipiert werden kann.

- Kurzfristig sollten Detektions- und Frühwarnsysteme geschaffen werden, die eine frühzeitige Erkennung und Abwehr solcher Angriffe erlauben. Die Lagezentren der zuständigen Sicherheitsbehörden könnten mit speziell geschulten Mitarbeitern verstärkt werden.

- Mit dem nationalen Cyberabwehrzentrum besteht bereits eine Kooperationsplattform der zuständigen Sicherheitsbehörden zur Identifikation und Abwehr von Cyberangriffen. Deren bislang auf Cyberangriffe im engeren Sinne (IT-Systeme) beschränktes Portfolio könnte um den Aspekt der Desinformationsbekämpfung erweitert werden.

- Es könnte ebenfalls erwogen werden, eine der EU-East StratCom vergleichbare Struktur in Deutschland zu schaffen, die ausschließlich mit der Aufdeckung und Bekämpfung ausländischer Desinformation und Propaganda befasst wäre.

- Auf europäischer Ebene könnte die EU-Agentur für Netz-und Informationssicherheit (ENISA) sodann ein Forum bilden, um den Austausch von Erfahrungen mit politischem Hacking und Desinformation im Kontext von Wahlen und Krisensituationen zwischen der EU und ihren Mitgliedstaaten zu erleichtern und zu koordinieren. Auf dem Erfahrungsaustausch basierend könnten Leitlinien und Regelbücher für den Umgang mit diesen Herausforderungen formuliert werden. Die Bundesregierung sollte auf eine enge Einbindung der deutschen Sicherheitsbehörden in solche kooperativen Strukturen hinwirken.

- Als Konsequenz aus den Erfahrungen der Corona-Pandemie sollte der Themenkomplex Desinformation und Propaganda in Zukunft fester Bestandteil deutscher Krisenreaktionspolitik werden.

- Es zeichnet sich bereits jetzt ab, dass sich Desinformationskampagnen und Cyberattacken zu einem dauerhaften Problem entwickeln, zu dessen Lösung es fester Strukturen bedarf, die einen engen

Austausch zwischen Politik, Sicherheitsbehörden, Wissenschaft und Wirtschaft ermöglichen. Es ist notwendig, die Bekämpfung hybrider Bedrohungen weiter zu institutionalisieren. Insbesondere die Arbeit des nationalen Cybersicherheitsrats sowie der daran angeschlossenen Arbeitsgruppen sollten auf jeden Fall fortgesetzt und vertieft werden.

- Um künftigen Cyberangriffen auf staatliche Institutionen besser vorzubeugen und deren jederzeitige Handlungsfähigkeit sicherzustellen, sollte in die IT-Sicherheit kritischer Infrastrukturen, insbesondere der Verfassungsorgane von Bund und Ländern, investiert werden.

Forschung fördern

Neue hybride Bedrohungen wie Desinformation und Cyberattacken weisen die Besonderheit auf, dass sie maßgeblich von der verstärkenden Wirkung bestimmter Technologien (Algorithmen, Malicious Social Bots, etc.) profitieren oder sogar deren Produkt sind (KI-generierte Deepfakes). Die Bekämpfung dieser Phänomene setzt daher ein genaues Verständnis ihrer Funktionsweise sowie der technologischen Zusammenhänge voraus. Hinzu kommt, dass aufgrund des rasanten technologischen Fortschritts jederzeit neue Bedrohungen entstehen können und die Gegenmaßnahmen deshalb kontinuierlich angepasst werden müssen. Staatliche Stellen sind darauf angewiesen, stets ein aktuelles Bild der Bedrohungslandschaft zu haben.

- Um mit künftigen Entwicklungen im Bereich Desinformation Schritt halten zu können, sollte die Bundesregierung weiterhin interdisziplinäre Forschungsprojekte fördern. Mit dem vom BMBF unterstützen Projekt DORIAN (Desinformation aufdecken und bekämpfen) existiert bereits eine vielversprechende interdisziplinäre Plattform, die als Ausgangspunkt für weitere Arbeiten dienen kann.

- Mit größter Aufmerksamkeit sollten dabei neue und noch gefährlicherer Formen von Desinformation, insbesondere die sogenannten Deepfakes, in den Blick genommen werden. Dabei handelt es sich um Fotos oder Videos, die mittels KI derart manipuliert werden können, dass sie nicht mehr ohne Weiteres als „Fakes" zu identifizieren sind. Experten befürchten, dass der absehbare großflächige Einsatz von Deepfakes in naher Zukunft das ohnehin schon angeschlagene Vertrauen der Öffentlichkeit in Politik und Medien weiter erodieren lassen könnte. Umso wichtiger ist es daher, die Regulierung des Einsatzes von künstlicher Intelligenz voranzutreiben.

- Zur wissenschaftlichen Erschließung des Phänomens Desinformation sind Forscher auf Daten angewiesen, die einen genauen Einblick in die Dynamiken der Verbreitung von Falschnachrichten in sozialen Netzwerken liefern können. Zurzeit besteht jedoch ein Informationsgefälle zugunsten der großen Online-Plattformen, die über die relevanten Daten verfügen, sich jedoch häufig weigern, diese der Wissenschaft zu Forschungszwecken zugänglich zu machen. Im Zuge der anstehenden Plattformregulierung auf EU-Ebene sollte daher auch über eine Verpflichtung der Online-Anbieter nachgedacht werden, Wissenschaftlern datenschutzkonformen Zugriff auf diese Daten zu gewähren.

Transatlantische Wirtschafts- und Wertegemeinschaft

- Als Mitgliedstaat ist Deutschland Teil des europäischen Staaten- und Verfassungsverbundes der EU. Deutsches Handeln darf daher nicht isoliert, sondern muss stets im Verbund, also kooperativ-arbeitsteilig gedacht werden. Dies gilt insbesondere bei Herausforderungen wie den hier relevanten hybriden Bedrohungen, die alle Mitgliedstaaten und die EU gleichermaßen betreffen und ein geschlossenes Vorgehen erfordern. Die Bundesregierung sollte auf die Definition einer gemeinsamen Strategie von EU und Mitgliedstaaten hinwirken.

- Zugleich sollten sich Deutschland und die EU auf der anderen Seite des Atlantiks (USA, Kanada) und in anderen Teilen der Welt (insbesondere der EU-Nachbarschaft sowie Australien und Neuseeland) nach Partnern umsehen, die sich den Bemühungen um die Sicherung der Demokratie und der Stärkung der digitalen Resilienz anschließen wollen. Ein gemeinsames Forum zum Austausch von Praktiken und neuen Anliegen könnte als Teil einer „Transatlantischen Wirtschafts- und Wertegemeinschaft (TWW)" bei der OECD, der NATO oder einer neuen „Allianz für digitale Demokratie" verankert werden.

ERGEBNIS

Verschiedene Schlüsselereignisse der letzten Jahre haben die Verwundbarkeit westlicher Gesellschaften gegenüber Desinformation, Propaganda und gezielter Wahlbeeinflussung offengelegt und Handlungsbedarf erkennen lassen. Angesichts dieser neuartigen Bedrohungen für die Demokratie ist die deutsche Politik aufgerufen, aktiv Maßnahmen zu ihrem Schutz zu ergreifen und ihre demokratische und digitale Resilienz zu stärken. Insoweit erfordert die Komplexität der neuen Bedrohungslandschaft ein geschlossenes Vorgehen der demokratischen Verfassungsstaaten Europas unter Einbeziehung von Unternehmen und Akteuren der Zivilgesellschaft sowie der Partner jenseits des Atlantiks. In diesem Rahmen sollte sich Deutschland im Verbund mit der EU für die Entwicklung einer gemeinsamen Strategie einsetzen, die auf den Leitprinzipien der Transparenz, Glaubwürdigkeit, Medienkompetenz und geteilten Verantwortung basiert.

DGAP
Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin

Tel. +49 30 254231-0

info@dgap.org
www.dgap.org
@dgapev

Die Deutsche Gesellschaft für Auswärtige Politik e.V. (DGAP) forscht und berät zu aktuellen Themen der deutschen und europäischen Außenpolitik. Dieser Text spiegelt die Meinung der Autorinnen und Autoren wider, nicht die der DGAP.

Herausgeber
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 1866-9182

Redaktion Bettina Vestring

Layout & Grafik
Carl-Friedrich Richter
Studio Friedrichter

Design Konzept:
WeDo

Fotos Autorinnen und Autoren

Seite 19 (oben)	Unsplash, Massimo Virgilio
Seite 27 (oben)	IMAGO, Poolfoto
Seite 27 (unten)	Malene Lauritsen
Seite 39 (oben)	Unsplash, Andrew Coop
Seite 47 (oben)	REUTERS, Aly Song
Seite 57 (oben)	Unsplash, Alexandre Debieve
Seite 67 (oben)	Unsplash, Camilo Jimenez
Seite 75 (oben)	Unsplash, Gustavo Quepon
Seite 75 (unten)	John Cairns
Seite 83 (oben)	Unsplash, Mikhail Serdyukov
Seite 89 (oben)	IMAGO, Jochen Tack
Seite 89 (unten)	Francesco Scarpa
Seite 97 (oben)	IMAGO, Xinhua
Seite 97 (unten)	Francesco Scarpa