Demokratie unter Beschuss: die EU muss Resilienz nach innen und außen zeigen

Calliess, Christian

Veröffentlichungsversion / Published Version
Stellungnahme / comment

Nr. 5
August 2021

DGAP POLICY BRIEF

Demokratie unter Beschuss

Die EU muss Resilienz nach innen und außen zeigen.*

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

Verschiedene Schlüsselereignisse der letzten Jahre haben die Verwundbarkeit westlicher Gesellschaften gegenüber Desinformation, Propaganda und gezielter Wahlbeeinflussung offengelegt und Handlungsbedarf erkennen lassen. Angesichts dieser neuartigen hybriden Bedrohungen für die Demokratie sind die EU und ihre Mitgliedstaaten dazu aufgerufen, aktiv Maßnahmen zu ihrem Schutz zu ergreifen und ihre demokratische und digitale Resilienz zu stärken.

– **Desinformation, gezielte politische Online-Werbung und Cyberattacken stellen eine Gefahr für den Prozess der öffentlichen Meinungsbildung, die Integrität der Wahlen sowie die Handlungsfähigkeit des Staates dar.**

– **Die Komplexität der neuen Bedrohungslandschaft erfordert ein geschlossenes Vorgehen der demokratischen Verfassungsstaaten Europas unter Einbeziehung der Unternehmen und Akteure der Zivilgesellschaft sowie der Partner jenseits des Atlantiks.**

– **Deutschland und die EU sollten sich bei der Entwicklung einer gemeinsamen Strategie von den Prinzipien der Transparenz, Glaubwürdigkeit, Medienkompetenz und geteilten Verantwortung leiten lassen.**

* Das vorliegende Policy Paper beruht in Teilen auf Arbeiten, mit denen ich während meiner Tätigkeit als Rechtsberater des beim Präsidenten der Europäischen Kommission angesiedelten Strategieteams (EPSC) und Leiter von dessen Institutionellem Team von 2015-2018 befasst war.

EINLEITUNG

Demokratie unter Beschuss

Seit einigen Jahren stehen die westlichen Demokratien in Europa (und den USA) verstärkt unter „digitalem Beschuss". Inländische sowie ausländische Akteure versuchen, mittels gezielter Desinformationskampagnen, politscher Online-Werbung und Cyberattacken den öffentlichen Meinungsbildungsprozess zu ihren Gunsten zu beeinflussen und demokratische Institutionen zu schwächen, um der Demokratie nachhaltig Schaden zuzufügen.

Zahlreiche Beispiele sind dokumentiert. Diese reichen von der Einflussnahme auf den US-Wahlkampf 2016 unter Mitwirkung des Datenanalyse-Unternehmens Cambridge Analytica über die inzwischen belegte Beeinflussung des Brexit-Referendums durch gezielte Desinformation[1] bis hin zur aktuellen Corona-Pandemie, welche laut WHO mit einer regelrechten „Infodemie"[2] einhergeht.

Dabei kommt Social-Media-Plattformen wie Facebook, Twitter und YouTube eine Schlüsselrolle zu. Diese stehen zunehmend im Fokus der Kritik seit bekannt wurde, dass staatliche Geheimdienste ebenso wie (mitunter von ihnen unterstütze) europäische und amerikanische Akteure sie nutzen, um Desinformation und „Leaks" von politischen Hackern zu verbreiten oder illegal an große Mengen privater Nutzerdaten zu gelangen. Insoweit geht es nicht mehr um die von der Informations- und Meinungsfreiheit geschützte Aktivität der Nutzerinnen und Nutzer von werbefinanzierten Social-Media-Plattformen, sondern um Drittstaaten oder von ihnen bezahlte private Akteure, die die Plattformen zielgerichtet nutzen (missbrauchen), um das Vertrauen der Bürgerinnen und Bürger in die Demokratie der EU durch Lüge und Hetze sowie illegal erlangte Informationen zu erschüttern.

Handeln, bevor es zu spät ist

Anders als die USA, sind die EU und ihre Mitgliedstaaten, darunter Deutschland, von den negativen Folgen der genannten Phänomene bislang weitestgehend verschont geblieben. Daraus darf aber nicht geschlossen werden, dass dies auch in Zukunft so bleibt. Ebenso wenig sollte blind in die natürliche Resilienz der demokratischen Gesellschaften innerhalb der EU vertraut werden. Die Vorkommnisse der letzten Jahre in den USA sowie dem Vereinigten Königreich sollten als mahnende Beispiele dafür verstanden werden, wie selbst in Ländern mit langer demokratischer Tradition die Demokratie innerhalb kurzer Zeit nachhaltigen Schaden nehmen kann, wenn nicht rechtzeitig Gegenmaßnahmen ergriffen werden. Dies gilt umso mehr, als Deutschland und die EU bereits jetzt nachweislich Ziel gezielter Desinformationskampagnen und Hackerangriffe (vor allem aus Russland) sind.[3]

Es sollte nicht blind in die natürliche Resilienz demokratischer Gesellschaften in der EU vertraut werden.

Mit Blick auf das hohe Schutzgut der Demokratie und der für ihre Vertrauenswürdigkeit und ihren Fortbestand bedeutsamen Institutionen, können die demokratischen Verfassungsstaaten der EU ebenso wenig wie die EU selbst tatenlos zusehen, wie sich ihre Grundlagen von innen heraus auflösen. Empirische Belege, die eine hinreichende Wahrscheinlichkeit im Sinne der Gefahrenabwehr begründen, erlauben und erfordern ein Handeln der verantwortlichen staatlichen Stellen zum Schutz der Demokratie. Wehrhafte Demokratie bedeutet, dass die Politik und Gesellschaft in demokratischen Verfassungsstaaten insoweit sensibel sind und nicht erst reagieren, wenn es zu spät ist.

Auch wenn der Begriff „Demokratie" aus rechtlicher Perspektive nicht ganz einfach zu fassen ist (sowohl Art. 20 GG als auch Art. 2 i.V.m. Art. 9 bis 12 AEUV definieren lediglich Elemente der Demokratie), lassen sich drei Aspekte identifizieren, die in diesem Zusammenhang von Bedeutung sind: Erstens der Prozess der öffentlichen Meinungsbildung, zweitens das unmittelbare zeitliche Vorfeld der Wahlen sowie die Integrität des Wahlvorgangs als solchem und drittens die Funktionsfähigkeit demokratischer Institutionen.

1 Vgl. Disinformation and "fake news": Final report, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf, vom 18. Februar 2019.

2 WHO, Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation, https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation, vom 23. September 2020.

3 Der East StratCom Taskforce des EAD zufolge, ist Deutschland der am stärksten von Desinformation betroffene Mitgliedstaat der EU und das Hauptziel russischer Desinformationskampagnen, EU vs Disinfo, Vilifying Germany; Wooing Germany, https://euvsdisinfo.eu/villifying-germany-wooing-germany/, vom 9. März 2021.

BEDROHUNGSSZENARIEN

Die Verlagerung vieler, für die Demokratie relevanter Prozesse in den Online-Kontext sowie die Digitalisierung hat zu einer neuen Bedrohungslandschaft geführt, die neue Gefahren für den demokratischen Verfassungsstaat schafft. Obwohl das genaue Ausmaß der Herausforderungen bislang noch nicht gänzlich bekannt ist, lassen sich dennoch zwei für das Schutzgut Demokratie relevante Bedrohungsszenarien benennen, welche im Folgenden näher dargestellt werden sollen. Erstens die Bedrohung für den Prozess der öffentlichen Meinungsbildung und zweitens Cyberangriffe.

Es reichen mitunter schon einige 10.000 Wählerstimmen aus, um ein anderes Ergebnis herbeizuführen.

Erstes Bedrohungsszenario

Das erste Bedrohungsszenario betrifft das Schutzgut Demokratie durch **Desinformation, politische Werbung und technologische Verstärker.**

Bedrohung durch Desinformation

Desinformationen stellen insoweit eine Gefahr für die Demokratie dar, als sie den Meinungsbildungsprozess verzerren und ihm die Grundlage entziehen. Die Verbreitung von Desinformationen ist – zumindest nach deutschem verfassungsrechtlichem Verständnis – daher auch nicht von der Meinungsfreiheit (Art. 5 Abs. 1 S. 1 GG) gedeckt.[4][5] Anders verhält es sich mit Tatsachenbehauptungen, deren Unwahrheit nicht dem Vorsatz, sondern der Unwissenheit oder Fahrlässigkeit des Äußernden geschuldet ist[6] (Fehlinformation). Die Abgrenzung zwischen diesen beiden Formen der Falschinformationen dürfte sich in der Praxis indes als schwierig erweisen.

Somit entsteht eine Grauzone zur für die Demokratie unabdingbaren Informations- und Meinungsfreiheit, welche ein differenziertes Vorgehen erfordert. Gezielte, sich gegen bestimmte Inhalte richtende staatliche Maßnahmen kommen daher – wenn überhaupt – nur als Ultima Ratio in Betracht. Vielversprechender scheint es, die Medienkompetenz der Bürgerinnen und Bürger zu stärken, den Zugang zu vertrauenswürdigen Inhalten zu erleichtern und ein Informationsumfeld zu schaffen, in dem Desinformationen leichter identifiziert werden können (s.u.).

Bedrohung durch politische Werbung

War Wahlkampf in analogen Zeiten noch ein aufwendiges Unterfangen, hat die Akkumulation großer Datenmengen durch private Unternehmen („Big Data“) und das dadurch ermöglichte Profiling von Nutzerinnen und Nutzern dazu geführt, dass politische Werbung heute um ein Vielfaches gezielter geschaltet werden kann als noch vor wenigen Jahren. Dabei wird auf die eigentlich zum Zwecke gezielter Werbung entwickelte Technik des sogenannten Microtargeting zurückgegriffen, welche es dem Werbetreibenden erlaubt, einzelnen Nutzerinnen und Nutzern – meist ohne ihre Kenntnis - auf sie zugeschnittene Inhalte zu präsentieren.

Das Risiko gezielter politischer Online-Werbung liegt dabei weniger in den vermittelten Inhalten (sofern es sich dabei nicht um Desinformation handelt) als in der damit verbundenen Manipulationsgefahr begründet: Sie kann unter anderem dazu eingesetzt werden, auf eine geringere Wahlbeteiligung hinzuwirken oder aber unentschiedene Wählergruppen gezielt in die eine oder andere Richtung zu beeinflussen. Bedenkt man den sehr knappen Ausgang des Brexit-Referendums oder der US-Wahl 2020, reichen mitunter schon einige 10.000 Wählerstimmen aus, um ein anderes Ergebnis herbeizuführen.

Noch problematischer wird es, wenn zum Zwecke der politischen Online-Werbung auf Daten zurückgegriffen wird, die – wie im Falle von Cambridge Analytica – ohne Einwilligung der betroffenen Nutzerinnen und Nutzer erlangt wurden. Angesichts der mit politischer Online-Werbung verbundenen finanziellen Anreize für Unternehmen steht zu befürchten, dass in Europa ein Markt für politisches Microtargeting entstehen könnte.

Bedrohung durch technologische Verstärker

Fast alle großen Internetkonzerne betreiben heutzutage ein werbebasiertes Geschäftsmodell. Um die von ihnen (vermeintlich) kostenlos angebotenen Dienste rentabel zu machen, sammeln die Unternehmen massenhaft Verhaltensdaten, die die Nutzerinnen und

4 Zu dieser Frage: Steinbach, JZ 2017, 653 ff.

5 BVerfGE 90, 241 (247) (Auschwitzlüge).

6 *Grabenwarter*, in: Maunz/Dürig Grundgesetz, Art. 5, Rn. 49.

Nutzer beim Besuch der Plattformen hinterlassen. Aus diesen Daten werden dann Profile erstellt, aus denen sich auf die Präferenzen einzelner Nutzer(gruppen) schließen lässt. Diese Profile bilden sodann die Grundlage für das Schalten von gezielter Online-Werbung durch werbetreibende Dritte, welche zu diesem Zweck in Echtzeit Werbeflächen von den Internetkonzernen erwerben.

Um aus der unglaublichen Masse der auf den Plattformen vorhandenen Informationen die für Nutzerinnen und Nutzer relevanten Inhalte herauszufiltern, setzen die Unternehmen sogenannte Empfehlungsalgorithmen ein.[7] Diese Algorithmen sind am oben beschriebenen Geschäftsmodell der Plattformen ausgerichtet. Dies führt dazu, dass die Algorithmen vor allem solche Inhalte bevorzugen, die beim Nutzer Gefühle wie Sensationslust, Angst oder Wut auslösen. Dazu gehören vor allem Desinformationen, Lügen und Hassnachrichten, die sich ungehindert auf den Plattformen ausbreiten können.

Die von den Algorithmen bewirkte personalisierte Informationsauswahl kann zudem dazu führen, dass sich Nutzerinnen und Nutzer in „Filterblasen“ oder „Echokammern“ wiederfinden, in denen sie nur noch mit Inhalten konfrontiert werden, die ihren schon bestehenden Anschauungen entsprechen. Dem demokratischen Diskurs wird somit die gemeinsame Diskussionsgrundlage entzogen.

Ein weiterer Faktor, der zur Verzerrung des Prozesses der öffentlichen Meinungsbildung beiträgt, ist der Einsatz sogenannter Social Bots.[8] Dies sind automatisierte, künstliche Accounts, die unter Ausnutzung der vorherrschenden (und oftmals vehement verteidigten) Anonymität im Internet dazu eingesetzt werden, Trends zu erzeugen und Mehrheiten zu fingieren.

Seit Jahren kommt es immer wieder zu Hackerangriffen auf staatliche Institutionen.

Zweites Bedrohungsszenario

Das zweite Bedrohungsszenario betrifft das Schutzgut Demokratie durch Cyberangriffe in Hinblick auf die Integrität der Wahlen sowie die Funktionsfähigkeit staatlicher Institutionen.

Bedrohung durch Cyberangriffe

Cyberangriffe können zum einen den Zugang zu elektronischen Wahlmaschinen oder digital verwalteten Wahlergebnissen ermöglichen und diese, ohne Spuren zu hinterlassen, manipulieren. In Deutschland gibt es zwar ähnlich wie in fast allen Mitgliedstaaten der EU[9] bislang nicht die Möglichkeit einer elektronischen Stimmabgabe.[10] Der Ruf nach neuen Möglichkeiten der elektronischen Stimmenabgabe ist aufgrund der Corona-Pandemie zuletzt jedoch wieder lauter geworden. Dabei erscheint der Zugang zu den Systemen der Stimmauszählung, mit denen Wahlbeamte die Wahlergebnisse der 70.000 Stimmbezirke verschicken, schon jetzt nicht sicher.[11] Für den flächendeckenden Einsatz von Wahlcomputern bei Bundestags- und Europawahlen fehlt es an verbindlichen Sicherheitsvorgaben für Hersteller und Lieferanten und einer daran anknüpfenden europaweit gültigen Zertifizierung, durch die ausgeschlossen werden kann, dass in die Maschinen beispielsweise Malware oder Sleeper-Befehle eingebettet werden.

Zum anderen kommt es seit Jahren immer wieder zu Hackerangriffen auf staatliche Institutionen, insbesondere den deutschen Bundestag, die deren Funktionsfähigkeit gefährden.

MASSNAHMEN ZUR STÄRKUNG DER DEMOKRATISCHEN RESILIENZ

Die EU sollte die Mitgliedstaaten, Unternehmen und Akteure der Zivilgesellschaft zum Schutz der europäischen Demokratie mobilisieren („Multi-Stakeholder Forum“). Zugleich sollte sie sich auf der anderen Seite des Atlantiks (USA, Kanada) und in anderen Teilen der Welt nach Partnern umsehen, die sich den Bemühungen um Sicherung der Demokratie und der Stärkung der digitalen Resilienz anschließen. Diese Bemühungen könnten in der OECD oder einer neuen „Allianz für digitale Demokratie“ verankert werden und zu einem Forum werden, in dem Praktiken und neue Anliegen

7 Dazu u.a. Schemmel, Der Staat (57), 2018, 501 (506).
8 Dazu grundlegend Milker, ZUM 2017, 216 ff.
9 https://www.euractiv.de/section/europawahlen/news/vor-den-wahlen-eu-testet-cybersicherheitssysteme/ (zuletzt abgerufen am 13.3.2021).
10 BVerfGE 123, 39 ff. (Wahlcomputer).
11 https://www.zeit.de/digital/datenschutz/2017-09/bundestagswahl-wahlsoftware-hackerangriff-sicherheit-bsi-bundeswahlleiter (zuletzt abgerufen am 13.3.2021).

ausgetauscht werden. Deutschland und die EU sollten sich bei all ihren Maßnahmen auf die folgenden Leitprinzipien stützen.

Leitprinzipien

Transparenz

Die Öffentlichkeit soll wissen können, wer die Quelle einer Anzeige ist und mit wem oder was die Bürgerinnen und Bürger über soziale Medien agieren. Es sollte erkennbar sein, was ein Bot ist und was nicht. 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.

Glaubwürdigkeit

Ohne feststellbare Identitäten wird das Vertrauen der Bürgerinnen und Bürger in Social-Media-Plattformen und in die digitale demokratische Konversation mit der Zeit schwinden. Die Medien sollten versuchen, ihre eigene Glaubwürdigkeit und Integrität zu wahren, vielleicht sogar eine nichtstaatliche **Rating-Agentur** schaffen.

Medienkompetenz

Mittelfristig geht es darum, die Medienkompetenz der Menschen, insbesondere der Jugend im Rahmen der **Schulbildung**, zu erhöhen und zugleich sicherzustellen, dass journalistische Qualitätsprodukte in den Ergebnissen von Suchmaschinen besser dargestellt werden.

Die bislang selbstverständliche Anonymität im Internet wird zunehmend zu einer Herausforderung.

Geteilte Verantwortung

Demokratie ist im demokratischen Verfassungsstaat eine gemeinsame Verantwortung von Politik und Gesellschaft, EU und Mitgliedstaaten, Unternehmen und Verbrauchern. Vor diesem Hintergrund sollte die EU über ihre im Rahmen der Wettbewerbspolitik angestrengten individuellen Maßnahmen hinaus **Standards für die sozialen Medien und die Datenerhebung durch Plattformen** formulieren.

Maßnahmen mit Blick auf Bedrohungsszenario 1

Mit Blick auf Bedrohungsszenario 1 könnte die EU eine Gesetzgebung auf den Weg bringen, mit der (über das NetzDG hinaus) die Verantwortung für Inhalte in den sozialen Medien geregelt wird. Der Vorschlag der Kommission für ein Gesetz über digitale Dienste[12] stellt einen ersten Schritt in diese Richtung dar.

Ergänzend könnte der Rat Empfehlungen formulieren, wie die nationalen Wahlgesetze und -regeln in der EU zu aktualisieren sind, um intransparente politische Werbung und unverhältnismäßige Einflussnahme zu begrenzen.

Überdies könnte der öffentlich-rechtliche Rundfunk in den Mitgliedstaaten gestärkt und – wo nicht existent – mit einem dem Demokratieprinzip verpflichteten **Informationsauftrag zur Grundversorgung** aufgebaut werden. Eine solche öffentlich-rechtliche Grundversorgung sollte der strikten Kontrolle durch politisch unabhängige Gremien sowie Verfassungsgerichte unterworfen sein. Auf entsprechender Grundlage sollte auch über einen **Europäischen Öffentlichen Rundfunk** nachgedacht werden, der die Politiken der EU und die Entscheidungsprozesse in Brüssel, Straßburg und Luxemburg transparenter und verständlicher macht. Dabei müsste der Auftrag an einen solchen „Europafunk“ so definiert werden, dass er im Zuge seiner Begrenzung auf die europäische Grundversorgung nicht nur eine sinnvolle Koexistenz mit privaten Medien eingeht, sondern privaten Qualitätsmedien vielleicht sogar neue Einnahmequellen erschließt, indem er (statt Google) auch als Plattform für bereits vorhandene journalistische Inhalte fungiert.

Ebenso sollte die Zusammenarbeit mit Technologieunternehmen gesucht werden, um deren soziale Verantwortung auf Plattformen und bei Algorithmen zu erhöhen. Insoweit könnten **Grundsätze für die digitale Verwaltung** durch Technologieunternehmen geschaffen werden, die die Identifizierung gefälschter Online-Nachrichten gewährleisten.

Maßnahmen mit Blick auf Bedrohungsszenario 2

Die Erfahrung hat gezeigt, dass politisches Hacking und andere Cyberangriffe gegen einen Mitgliedsstaat oft über Server in anderen Mitgliedsstaaten initiiert werden. Allerdings fehlt in der EU ein gesetzli-

12 Kommission, DSA proposal, COM (2020) 825 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en.

cher Rahmen, der es den angegriffenen Mitgliedsstaaten erlaubt, schnell mit Strafverfolgungsbehörden und Internetanbietern außerhalb ihrer eigenen Grenzen zu interagieren und den Angriff abzuschalten.

Auch fehlt der EU ein wirksamer **Krisenreaktionsmechanismus**, der sofort auf gegen die EU gerichtete Angriffe reagieren kann und die Ressourcen der EU insgesamt, vor allem aber auch der zuständigen Generaldirektionen der Europäischen Kommission wirksam koordinieren kann. In einem ersten Schritt könnte beim Präsidenten der Europäischen Kommission eine Task Force etabliert werden, die alle Akteure innerhalb der Kommission zusammenführt. Zugleich könnte das EU-Koordinierungszentrum für Notfallmaßnahmen dem Generalsekretariat der Kommission unterstellt werden.

Ein zweiter Schritt wäre die Einrichtung einer **EU-Plattform**, die ENISA, die bestehenden Einrichtungen des Europäischen Auswärtigen Dienstes (EAD), also INTCEN, StratCom, Hybrid-Fusionszelle etc., sowie Europol und Vertreter der Mitgliedstaaten zusammenbringt. Einen interessanten Vorstoß, der auch mit Blick auf den Schutz der Demokratie als Vorbild dienen könnte, hat jüngst die Europäische Zentralbank (EZB) mit ihrer **Allianz zur Bekämpfung von Cyberrisiken** unternommen. Diese EU-Plattform könnte als Vorläufer einer vollwertigen Europäischen Agentur für Cybersicherheit wirken, die die Expertise der bereits vorhandenen, aber fragmentierten Akteure unter Respektierung ihrer institutionellen Eigenheiten unter einem Dach koordiniert. Mit ihrer Expertise könnte eine solche Plattform (mittelfristig Agentur) auch als Schnellreaktionskapazität herangezogen werden, um massiven Desinformationskampagnen mit allen zur Verfügung stehenden Instrumenten entgegenzuwirken (einschließlich einer Stand-by-Option für nationale Wahlen). Diese Europäische Agentur für Cybersicherheit wäre zugleich eine geeignete Schnittstelle, um – angesichts der beim Thema Cybersicherheit verschmelzenden Grenzen zwischen innerer und äußerer Sicherheit – eine wirksame Zusammenarbeit mit Akteuren der europäischen Sicherheits- und Verteidigungspolitik (etwa einer Europäischen Cyberbrigade) und den korrespondierenden Einheiten der NATO zu gewährleisten.

Darüber hinaus sollten nationale Wahlen als Schutzgut und Wahltechnologie als **„kritische Infrastruktur" in die Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie)** aufgenommen werden. Das im Vorfeld der Wahlen zum Europäischen Parlament von der NIS Cooperation Group erstellte „Compendium on Cyber Security of Election Technology" ist mangels Verbindlichkeit nicht hinreichend und kann nur ein erster Schritt sein. Erforderlich sind verbindliche Sicherheitsvorgaben für Hersteller und Lieferanten und einer daran anknüpfenden europaweit gültigen Zertifizierung.

Schaffung neuer institutioneller Strukturen

Abseits der oben geschilderten Maßnahmen sollte auf EU-Ebene zudem über institutionelle Strukturen nachgedacht werden, die ein „Ownership" im Hinblick auf den Schutz der Demokratie in Europa gewährleisten:

Der Präsidentin/Dem Präsidenten der Europäischen Kommission sollte eine Struktur für das Krisenmanagement zur Verfügung stehen, die es ihm und seinen Kommissaren ermöglicht, koordiniert auf hybride Bedrohungen (wozu Desinformation und politisches Hacking gezählt werden) zu reagieren. In diesem Zusammenhang sollten die Kapazitäten von EU-StratCom genutzt und gestärkt werden. Die Abteilung für strategische Kommunikation im EAD hat drei Teams mit geografischem Schwerpunkt: South mit vier Mitarbeitern, Western Balkans mit zwei Mitarbeitern und East Stratcom mit 14 Mitarbeitern. Nur East Stratcom hat ein spezielles Mandat des Europäischen Rates. EU-StratCom benötigt ein eigenes Budget, mit dem die Einheit in die Lage versetzt wird, Arbeiten auszulagern und in ihren Bereichen Forschung und Projekte in Auftrag zu geben.

Überdies sollten die Mitgliedstaaten Anreize erhalten, um nationale Expertinnen und Experten längerfristig abzuordnen und solchermaßen ein arbeitsteiliges Zusammenwirken zwischen EU und Mitgliedstaaten zu gewährleisten. Indem sie Digital-Ingenieurinnen und -Ingenieure aus Technologieunternehmen einsetzt und sie mit langjährigen Expertinnen und Experten der Kommission in Verbindung bringt, könnte die EU eine natürliche Gemeinschaft für die Diskussion von Werten in der Technologie innerhalb „der Blase" schaffen.

Schließlich könnte die ENISA ein Forum bilden, um den Austausch von Erfahrungen mit politischem Hacking und Desinformation im Kontext von Wahlen zwischen EU und Mitgliedstaaten zu erleichtern und zu koordinieren.

Der vorliegende DGAP-Policy Brief entstand im Rahmen des von der Stiftung Mercator geförderten Projekts „Ideenwerkstatt Deutsche Außenpolitik". Dessen Ziel ist es, deutsche Außenpolitik auf den Prüfstand zu stellen und mittels Analysen und Debatten zur Stärkung der deutschen und europäischen außenpolitischen Handlungsfähigkeit beizutragen.

DGAP
Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin

Tel. +49 (0)30 25 42 31 -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 2198-5936

Redaktion Jana Idris

Layout/Satz Mark McQuay

Design Konzept: WeDo