Bendiek, Annegret; Schulze, Matthias

Research Report

Desinformation und die Wahlen zum Europäischen Parlament

SWP-Aktuell, No. 10/2019

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Bendiek, Annegret; Schulze, Matthias (2019) : Desinformation und die Wahlen zum Europäischen Parlament, SWP-Aktuell, No. 10/2019, Stiftung Wissenschaft und Politik (SWP), Berlin, https://doi.org/10.18449/2019A10

This Version is available at:
https://hdl.handle.net/10419/255587

SWP-Aktuell
NR. 10 FEBRUAR 2019

Desinformation und die Wahlen zum Europäischen Parlament

Annegret Bendiek/Matthias Schulze

Im Mai 2019 finden Wahlen zum Europäischen Parlament (EP) statt. Politik und Experten fürchten, dass der Wahlprozess mit Desinformationskampagnen und Cyberangriffen empfindlich gestört wird. Die Europäische Kommission hat im Dezember 2018 einen Aktionsplan gegen Desinformation vorgelegt und will 5 Millionen Euro zur Verfügung stellen, um Wähler und Verantwortliche in der Politik für Manipulationen zu sensibilisieren. Es geht auch darum, die Cybersicherheit von Wahlsystemen und -prozessen zu erhöhen. Kurzfristige Selbstregulierungsansätze der Internetkonzerne reichen dazu bei weitem nicht aus. Um mittelfristig die Integrität von Wahlen zu schützen, gilt es, unabhängige Forschung als Basis für technische, rechtliche und marktregulierende Reformen zu stärken. Ziel muss sein, die Funktionsfähigkeit von Demokratien und Wahlen in der Digitalisierung zu bewahren.

Vom 23. bis 26. Mai 2019 findet in den Mitgliedstaaten der Europäischen Union die nächste Europawahl statt. Weil rechtsnationalistische und europaskeptische Strömungen erstarkt sind, wird bereits von einer »Schicksalswahl« gesprochen, welche die künftige Ausrichtung der EU maßgeblich prägen könnte. Schon jetzt vereinigen europaskeptische Parteien knapp ein Drittel der Abgeordneten im Parlament auf sich, ein Anteil, der mit der Wahl steigen könnte.

Bisher galten die EP-Wahlen als »Wahlen zweiter Ordnung« und daher als gute Gelegenheit für einen Denkzettel an die Regierung des jeweiligen Mitgliedstaats. Diese Sichtweise verkennt das Mobilisierungspotential der aktuellen Debatte über Pro und Contra der europäischen Integration, über den Einfluss von Dritten und über die gewachsene Bedeutung des EP. Für die strategische Ausrichtung europäischer Integration sind die Wahlen äußerst wichtig. Ein Erfolg der EU-Gegner könnte die Union an den Rand ihrer Handlungsfähigkeit drängen, etwa durch weitere Ausstiegsforderungen nach britischem Muster oder eine Blockade des komplexen Entscheidungsprozesses. Die Wahlen entscheiden nicht nur über die Neubesetzung des EP, sondern auch über den Amtsantritt der neuen EU-Kommission für die Wahlperiode 2019—2024. Das EP beeinflusst die Ernennung der Kommissare und kann mit Zweidrittelmehrheit die gesamte Kommission zum Rücktritt zwingen sowie den Mehrjährigen Finanzrahmen finanzpolitisch neu ausrichten.

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Herausforderungen

Struktur und Funktionen der EU sind nicht leicht zu verstehen. Europäische Themen sind vielen unbekannt, und es ist recht einfach, falsche Informationen über die EU zu verbreiten. Mit Blick auf die Europawahl ermahnte der EU-Kommissar für die Sicherheitsunion, Julian King, die Mitgliedstaaten, »die Bedrohung der demokratischen Prozesse und Institutionen durch Cyberangriffe und Desinformationen« ernst zu nehmen und »nationale Pläne zur Vorbeugung« aufzustellen. Es gelte zu verhindern, »dass staatliche und nichtstaatliche Akteure unsere demokratischen Systeme untergraben und als Waffe gegen uns einsetzen«. Dazu gehören vor allem Desinformationskampagnen sowie Cyberangriffe auf die elektronische Wahlinfrastruktur, die Vertraulichkeit, Verfügbarkeit und Integrität des Wahlprozesses beeinträchtigen können.

Offenbar habe Desinformation bereits Wirkung in Europa gezeigt: Forscher der Universität Edinburgh identifizierten in sozialen Netzwerken über 400 falsche Accounts, mit denen von St. Petersburg aus bezahlte Störenfriede (Trolls) im Vorlauf des Brexit-Referendums agitierten. Aus sicherheits- und verteidigungspolitischer Sicht werden Desinformation und Cyberangriffe als Elemente hybrider Bedrohungen definiert, also Handlungen Dritter, mit denen Europa oder das EU-System destabilisiert werden soll. Mit dem Begriff hybride Bedrohungen ist gewöhnlich eine Form der Kriegsführung gemeint, die unterhalb der Schwelle des Einsatzes militärischer Gewalt bleibt und so einen militärischen Gegenschlag auf Basis internationaler Konventionen erschwert.

Desinformationskampagnen

Desinformation ist kein neues Phänomen. In der Sicherheitsforschung gilt sie als »schwarze« Propaganda, da sie aus dem Verborgenen die öffentliche Meinung zu beeinflussen sucht. Dazu bedient sie sich derselben Mittel wie etwa moderne Public Relations (PR) und Werbekampagnen.

Im Gegensatz zu PR aber will Desinformation die Stützpfeiler der Demokratie ins Wanken bringen, indem sie Parteien, gewählte Politiker oder die EU als politisches System angreift. Dabei bedeutet Desinformation nicht notwendig Falschinformation, da auch wahre, aus dem Kontext gerissene Aussagen für suggestive Schlussfolgerungen missbraucht werden können. Desinformationskampagnen können kurzfristig angelegt sein, beispielsweise um Einfluss auf ein Wahlergebnis zu nehmen, oder langfristig, etwa um das Vertrauen in die EU zu untergraben. So wird versucht, einzelne Politiker zu diskreditieren, um ihre Wiederwahl zu verhindern. Im Zuge eines »negative campaigning« werden zum Beispiel angebliche Skandale aufgedeckt oder Korruptionsvorwürfe erhoben. Während des letzten Wahlkampfs um die Präsidentschaft in den USA verbreiteten vermutlich russische Twitter-Bots, also automatisierte Computerprogramme, überwiegend negative Berichte über Hillary Clinton und eher positive über Donald Trump. Mittelfristig sollen die gesellschaftliche Spaltung und die Polarisierung des öffentlichen Diskurses vorangetrieben werden.

Die Aushandlung politischer Interessen in gesellschaftlichen Diskursen ist Kernelement, aber auch Achillesferse von Demokratien. Mit Taktiken wie der Streuung zweifelhafter Behauptungen (»muddying the waters«) oder massenhaften, stetig wiederholten Falschinformationen oder Verschwörungstheorien (»firehose of falsehood«) sollen politische Gewissheiten ausgehöhlt und ein gesellschaftlich geteiltes Konzept von Wahrheit aufgelöst werden. Ein Beispiel dafür waren Reaktionen auf den Abschuss eines malaysischen Passagierflugzeugs im Juli 2014: In sozialen Netzwerken wurde versucht, den Untersuchungsbericht zu diskreditieren, dem zufolge russische Streitkräfte die Katastrophe herbeigeführt hatten.

IT-gestützte Desinformation

Zu unterscheiden ist zwischen digitaler und IT-gestützter Desinformation: Digitale Des-

information umfasst die gesamte Bandbreite digitaler Mechanismen zum Verbreiten von Informationen. IT-unterstützte Desinformation dagegen beinhaltet Hacking-Vorfälle oder Cyberangriffe, die Schutzziele von IT-Sicherheit, also Vertraulichkeit, Verfügbarkeit und Integrität, beeinträchtigen. Der technische Hack ist dabei nur eines von vielen Mitteln, mit denen die Vertraulichkeit von Informationen verletzt wird, etwa indem sensible Informationen aus den Accounts von Politikern, Parteien oder Amtsträgern gestohlen und dann mit schädigender Absicht veröffentlicht werden (Doxing). Bekannte Beispiele sind die Veröffentlichung der E-Mails des Wahlkomitees der US-Demokraten (DNC) auf der Enthüllungsplattform Wikileaks 2016 und des Wahlkampfteams von Emmanuel Macron 2017.

Immer häufiger wird in autoritär regierten Ländern die Verfügbarkeit technischer Systeme eingeschränkt, um Desinformation zu betreiben. Webseiten von Politikern, Parteien und Services wie Twitter und Facebook werden zielgerichtet kurz vor Wahlen durch Distributed-Denial-of-Service-Angriffe lahmgelegt, also absichtliche Überlastung des betreffenden Servers. Auf ähnliche Weise lässt sich die digitale Wahlinfrastruktur mit ihren Wahlcomputern und Auszählungssystemen stören und manipulieren.

Digitale Desinformation

Digitale Desinformation hat den Vorteil geringer Kosten bei großer Wirkung: Ohne viel Ressourcenaufwand lässt sich mit maßgeschneiderten Desinformationen ein globales Publikum erreichen. Digitale Desinformation bedient sich legitimer Mittel der Werbeindustrie, um Nutzer mit ihren individuellen Verhaltensprofilen gezielt anzusprechen (was als »targeted ads« und »microtargeting« bezeichnet wird).

Die sozialen Netzwerke wie Facebook sind nicht zum Zwecke demokratischer Diskurse entwickelt worden, sondern um Interessen und Verhalten ihrer Nutzer zu analysieren, zu kategorisieren und diese Informationen an Dritte für Werbezwecke zu verkaufen. Gemäß ihren Verhaltensmustern werden Nutzern Inhalte angezeigt, die andere Nutzer der gleichen Kategorie oder mit ähnlichem Verhaltensprofil ebenfalls bevorzugen. Algorithmen bewirken also, dass Nutzern mehr des Gleichen gezeigt wird, um ihre Aufmerksamkeit zu binden und sie so lange wie möglich auf den Plattformen zu halten. Diese sogenannten Filterblasen entstehen direkt aus dem Geschäftsmodell von Online-Plattformen, Werbung an möglichst viele Nutzer zu bringen. Werden gleiche Meinungen gruppiert und zugleich unterschiedliche Ansichten ausgeblendet, kann eine selbstreferentielle Echokammer entstehen. In Online-Foren, die nur gleichgesinnte Nutzer zusammenbringen, werden diese sich tendenziell lediglich in ihren Wahrnehmungen bestärken, weil sie keine Gegenrede erfahren.

Besonders polarisierend wirkt Desinformation bei bereits politisierten Gruppierungen mit starken ideologischen Ausrichtungen. Jenen Gruppen kann man gezielt Verschwörungstheorien anbieten, die zu ihrem Weltbild passen. Ein Beispiel dafür sind Kampagnen gegen angebliche Vergewaltigung durch Asylsuchende wie im berühmten Fall Lisa 2016. Aus dem US-Wahlkampf 2016 sind Fälle bekannt, in denen Anhänger der rechtsgerichteten Bewegung Alternative Right und linksgerichtete Gruppen separat über Facebook aufgefordert wurden, an derselben Demonstration teilzunehmen. Damit sollte eine gewaltsame Eskalation provoziert werden.

Über soziale Netzwerke können Verschwörungstheorien und Desinformation schnell weltweit geteilt werden. Basieren kann dies auf einem Mix automatisierter Accounts (»social bots«), hybrider Accounts (teils menschlich, teils automatisiert) und sogenannter Troll- oder 50-Cent-Armeen. Solche »Armeen« bestehen aus staatlich oder privat organisierten Kommentatoren, die in sozialen Medien oder auf Nachrichtenseiten systematisch bestimmte Narrative verbreiten. Häufig sind es auch Freiwillige, die unwissentlich Desinformation streuen (»unwitting agents«). Im US-Wahlkampf 2016 verbreiteten US-Bürger Kremlpropaganda, ohne die Urheberschaft zu kennen.

Aber auch die traditionelle Medienberichterstattung bleibt relevant, da sie immer häufiger Themen von sozialen Netzwerken aufgreift. Handelt es sich dabei um Desinformation und tragen die Medien diese unreflektiert weiter, verfestigen sie auf diese Weise die darin enthaltenen Narrative oder Falschmeldungen. Desinformation wirkt kumulativ über längere Zeiträume hinweg.

Gegenstrategien der EU

Die Abhaltung der EP-Wahl liegt in der Verantwortung der Mitgliedstaaten. Diese unternehmen einiges, um die Integrität von Wahlen zu schützen. Bis jetzt handelt es sich aber eher um einen Flickenteppich von Maßnahmen. Es steht zu befürchten, dass die EP-Wahlen von Europagegnern manipuliert, gestört oder unrechtmäßig beeinflusst werden, sei es während des Wahlkampfs, des Wahlakts oder der Stimmauszählung. Einer Eurobarometer-Umfrage zufolge sorgen sich 83 Prozent der Europäer wegen gezielter Desinformation im Netz. Die EU geht davon aus, dass gezielte Desinformationskampagnen im Wahlkampf zu beobachten sein werden.

Desinformationsbekämpfung

Seit 2015 versucht die Europäische Kommission, mit außen- und innenpolitischen Maßnahmen gegen Desinformation und technisch bedingte Beeinflussungen vorzugehen. Zu diesem Zweck hat sie unter anderem die Europäische Agentur für Netz- und Informationssicherheit (ENISA) personell und finanziell aufgestockt sowie eine East StratCom Task Force im Europäischen Auswärtigen Dienst (EAD) gegründet. Die Taskforce dokumentiert Desinformationskampagnen in den nordöstlichen Mitgliedsländern und informiert regelmäßig darüber. 2016 folgten eine Gemeinsame Mitteilung und ein Gemeinsamer Rahmen der EU für die Bekämpfung hybrider Bedrohungen. Die Kommission und der EAD sind sich darin einig, dass solche Bedrohungen der EU immer stärker zu schaffen machen.

Unter hybrider Bedrohung versteht die EU »eine Vermischung militärischer und ziviler Kriegsführung durch staatliche und nichtstaatliche Akteure wie verdeckte Militäroperationen, intensive Propaganda und wirtschaftliche Drangsalierung«. Diese Aggressionen würden nicht nur unmittelbaren Schaden anrichten und Verwundbarkeiten ausnutzen, sondern Gesellschaften destabilisieren und »durch Verschleierungstaktik« die Spaltung der EU befördern. Innere und äußere Sicherheit müssten deshalb noch stärker ineinandergreifen.

Kommissionspräsident Jean-Claude Juncker schlug in seiner Rede zur Lage der Union 2018 eine Reihe konkreter Maßnahmen vor, damit die Wahlen im Mai 2019 frei, fair und sicher ablaufen können. Unter anderem forderte er mehr Transparenz bei (oft verdeckter) politischer Werbung im Internet und die Möglichkeit von Sanktionen, wenn personenbezogene Daten rechtswidrig genutzt werden, um das Ergebnis der Europawahl zu beeinflussen.

Auf Betreiben der Europäischen Kommission haben sich Netzwerke wie Facebook, Twitter und Youtube auf einen Verhaltenskodex (»Code of Practice on Disinformation«) geeinigt, um gegen Desinformation und Fake Accounts auf ihren Plattformen vorzugehen. Im Oktober 2018 wurde dieser Kodex von Facebook, Google, Twitter und Mozilla sowie von Berufsverbänden der Online-Plattformen und der Werbebranche unterzeichnet.

Zwei Monate später legten die Kommission und die Hohe Vertreterin der EU für Außen- und Sicherheitspolitik einen Aktionsplan gegen Desinformation vor. Mit Blick auf die Europawahlen wurde begonnen, ein Frühwarnsystem für Desinformation einzurichten. Dafür wurden 5 Millionen Euro und 50 Personalstellen bewilligt. Das System soll Kampagnen in Echtzeit erkennen und es soll für das Problem sensibilisieren.

Weil die EU befürchtet, auch jenseits ihrer Grenzen falsch dargestellt zu werden, beobachten weitere Teams die Verbreitung von Falschinformationen in Nordafrika, im Nahen Osten und auf dem Balkan. Ferner

wurde ein Wahlnetzwerk eingerichtet, zudem wurden ein Leitfaden zur Anwendung des EU-Datenschutzrechts im Wahlkontext sowie Handreichungen zur Cybersicherheit erarbeitet. Ab Februar 2019 sollen die Mitgliedstaaten in einem Planspiel üben, was bei einem Angriff zu tun wäre. Die Staaten der EU setzen auf Erfahrungsaustausch. Im Frühjahr 2019 soll es weitere Treffen geben. Die Kommission ermahnte Ende Januar 2019 die Internetunternehmen, dass die Transparenzinitiativen gegen verdeckte Wahlwerbung nicht ausreichten, um die Integrität der Europawahlen zu schützen.

Cybersicherheitsmaßnahmen

Was unternimmt die EU gegen IT-gestützte Desinformation? Der Schutz kritischer Infrastrukturen ist schon länger Gegenstand von EU-Regulierung. Die Mitgliedstaaten konnten sich aber nicht darauf einigen, Wahlsysteme gemäß der Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie) von 2016 als kritische Infrastruktur zu definieren. Die IT-Sicherheit von Wahltechnologie galt als rein nationale Aufgabe. Nachdem jedoch über angebliche Beeinflussung des Brexit-Referendums sowie von Wahlen in Frankreich, Katalonien und Belgien berichtet worden war, stieg die Sensibilität für die Problematik. So schlug die EU im September 2017 ein ganzes Bündel an Cybersicherheitsmaßnahmen vor, unter anderem ein europaweites Kooperationsnetz zwischen Datenschutzbehörden, um Wissen über Methoden der Wahlbeeinflussung auszutauschen. Erst im Dezember 2018 verständigten sich die EU-Staaten auf ein Cybersicherheitsgesetz, das die Cybersicherheitsagentur (ENISA) stärken und erstmals einen Zertifizierungsrahmen für den Schutz kritischer Infrastrukturen schaffen wird.

Als im selben Monat ein Hacker unter dem Pseudonym »0rbit« bei Twitter brisante Daten veröffentlichte, forderten Politiker einen »Notfallplan, um innerhalb kurzer Zeit auf den Abfluss sensibler Daten, digitale Wirtschaftsspionage oder Sabotage reagieren zu können«. Verlangt werden auch einheitliche gesetzliche Mindeststandards für die Sicherheit informationstechnischer Geräte, was hieße, dass der freiwillige Zertifizierungsrahmen der EU durch eine europäische Verordnung zu ersetzen wäre. Das soll etwa für Endverbraucher-Geräte wie Mobiltelefone und Laptops gelten. Anbieter von Online-Diensten und Hersteller von Geräten, die mit dem Internet vernetzt sind, sollen ihre Angebote so gestalten, dass die Benutzer starke Passwörter wählen und sie regelmäßig aktualisieren.

Neben der Härtung technischer Infrastrukturen setzt die EU auf operative Cybersicherheitsmaßnahmen. Dazu gehören die Entwicklung besserer Attributionsfähigkeiten bei Cyberangriffen, ein Informationsaustausch und eine stärkere Rolle von Europol in der Cyberkriminalitätsbekämpfung. Werden Mitgliedstaaten Ziel solcher Angriffe, sollen sie selbst herausfinden können, woher der Angreifer kam, welche Sicherheitslücken genutzt wurden und welche Daten betroffen waren oder abgeflossen sind. Diskutiert werden härtere Strafen für Cyberkriminelle und neue Straftatbestände, etwa für das Betreiben krimineller Infrastrukturen. Mit Prinzipien wie »security by design«, also der Entwicklung von Hard- und Software, die Schwachstellen und Manipulationen von vornherein zu vermeiden sucht, ist in der Datenschutzgrundverordnung (DSGVO) ein weiterer Baustein für das Vorgehen gegen Cyberangriffe und Desinformation angelegt. Im Januar 2019 einigte sich die EU zudem auf Eckdaten für ein einschlägiges Gesetz. Auf seiner Grundlage können künftig Geldstrafen gegen Parteien und politische Stiftungen verhängt werden, wenn sie im Europawahlkampf gegen Datenschutzregeln verstoßen, um Wähler zu beeinflussen. Parteien können sogar alle Ansprüche an die Parteienfinanzierung der EU verlieren. Anlass für diese Regelung war, dass Facebook Nutzerdaten an das britische Unternehmen Cambridge Analytica weitergegeben hatte. Die Firma wertete die Datensätze von 220 Millionen amerikanischen Facebook-Nutzern aus und erstellte daraus Nutzerprofile für gezielte Werbung.

Cybersicherheit bei Wahlen

Welche Maßnahmen werden ergriffen, um Vertraulichkeit, Verfügbarkeit und Integrität elektronischer Wahlsysteme zu gewährleisten? Seit berichtet wurde, US-Wahlen seien angeblich unrechtmäßig beeinflusst worden, steht die sogenannte Venedig-Kommission des Europarats mit den Wahldurchführungsstellen der 61 Europaratsmitglieder in engem Austausch. Die elektronischen Wahlsysteme in den Mitgliedstaaten sind sehr unterschiedlich. Elektronisch gewählt wurde in der EU bisher nur in Belgien, Bulgarien, Estland und Frankreich. In Belgien verwenden vor allem flämische Kommunen Wahlmaschinen. In Bulgarien sollen solche Maschinen bei der EP-Wahl 2019 nur in kleineren Wahllokalen eingesetzt werden. Und in Frankreich wurde wegen der angeblichen Vorfälle bei der US-Wahl die Nutzung von Wahlmaschinen bei der Präsidentenwahl 2017 ausgesetzt. In anderen Staaten wie Deutschland oder Österreich gibt es nur die Wahl per Stimmzettel. Um das Wahlergebnis festzustellen, wird Informationstechnik eingesetzt. Bei der Ermittlung des vorläufigen Wahlergebnisses ist daher die Absicherung der IT-Systeme essentiell. Estland ist weltweit das einzige Land, das die Online-Wahl über das Internet zulässt.

Die technische Vulnerabilität elektronischer Wahlsysteme lässt sich nicht übergreifend beurteilen, da EU-Staaten unterschiedliche Wahlcomputer und -systeme nutzen. Da aber alle Wahlcomputer manipulierbar sind, raten Experten zu einem physischen Papierausdruck bei jeder einzelnen Abstimmung. Gemäß Artikel 11 der NIS-Richtlinie haben Vertreter aus 20 Mitgliedstaaten im Juli 2018 ein Kompendium zur Cybersicherheit von Wahlen erarbeitet. Die Mitgliedstaaten wurden darin aufgefordert, gezielte Sicherheitsvorkehrungen zu treffen und Kontaktstellen für ein übergeordnetes europäisches Kooperationsnetzwerk aufzubauen.

Kommen in einzelnen Wahlbezirken Unregelmäßigkeiten beim Wahlakt oder technische Probleme bei der Stimmauszählung vor, könnten die Wahlen in einzelnen Ländern kurzfristig nachgeholt werden, ohne dass das gesamte Europäische Parlament noch einmal gewählt werden müsste. Ein Cyberangriff auf einen Mitgliedstaat hätte zur Folge, dass die Sitzvergabe im EP nicht sofort bestätigt werden könnte. Gezielte Cyberangriffe aus Drittstaaten auf einzelne Wahlen können sanktioniert werden, indem die EU ihren Diplomatischen Reaktionsrahmen anwendet. Ein umfassender schwerwiegender Angriff auf die Wahlen zum EP würde als Angriff auf die EU gewertet. Unter bestimmten Voraussetzungen ließe das den Rückgriff auf die Solidaritätsklausel gemäß Artikel 222 AEUV oder sogar auf die Beistandsklausel nach Artikel 42 Absatz 7 EUV zu.

Unabhängige Forschung fördern

Die Europawahlen entscheiden über die Neubesetzung des Europäischen Parlaments, doch die Regeln für die Wahl liegen in nationaler Kompetenz. In vielen EU-Ländern sind lokale Wahlbehörden mit der Durchführung der Wahl betraut. Zwar sind sie sich der Gefahr von Desinformation und Cyberangriffen bewusst, aber technisch nicht ausreichend darauf vorbereitet. Auf dem Spiel steht die Glaubwürdigkeit der EP-Wahl und damit auch der EU. Um Desinformation zu bekämpfen und Cybersicherheitsübungen abzuhalten, greift die europäische Politik bevorzugt auf kurzfristige, eher technisch ausgelegte Aktionspläne in Kooperation mit Internetunternehmen zurück. Ursachenforschung dagegen fehlt. Daher empfiehlt es sich, die Erkenntnisse besser zu berücksichtigen, welche die unterschiedlichen wissenschaftlichen Disziplinen zu Desinformation, Cyberangriffen und den Bedingungen von Demokratie erbracht haben.

Hybride Bedrohungen?

Zwischen Sicherheits- und Verteidigungspolitik auf der einen und Innenpolitik auf der anderen Seite existiert eine Konkurrenz um Zuständigkeiten und Ressourcen. Aus verteidigungspolitischer Sicht gehört das

Phänomen Desinformation in die Kategorie hybride Bedrohungen. Doch es greift zu kurz, das Thema auf diese Weise zu verengen. Chefs amerikanischer Geheimdienste stellten in einer Kongressanhörung 2017 zu Recht fest, dass Desinformation eine neue Normalität darstelle. Nach Auffassung der Nato und der Europäischen Kommission ist Russland führend bei der gezielten Verbreitung von Falschinformationen, doch mehr als 30 weitere Länder betreiben ebenfalls Desinformation. Regierungen beauftragen Think-Tanks und Nichtregierungsorganisationen, Analysen zum Thema vorzulegen, so dass es an einschlägigen Berichten nicht mangelt. Die amerikanische Alliance for Securing Democracy zum Beispiel oder das Digital Forensic Research Lab, finanziert durch den Atlantic Council und Facebook, konzentrieren sich bei ihrer Arbeit vorwiegend auf Russland und China. Wichtig ist, dass Think-Tanks und politische Stiftungen, die sich mit Desinformation befassen, Auftraggeber und Finanziers ihrer Projekte kenntlich machen, um nicht in den Verdacht der Parteilichkeit zu geraten.

Falschinformationen stammen aber nicht nur aus Ländern außerhalb der EU, sondern werden auch innerhalb ihrer Mitgliedstaaten verbreitet. Mindestens genauso wichtig wie externe Versuche der Beeinflussung sind politischer Aktivismus, gerade aus dem europafeindlichen Spektrum, das Vortäuschen einer Graswurzelbewegung (Astroturfing) und die Rolle der Boulevardmedien. Deren Einfluss auf den Brexit etwa wog vermutlich schwerer als jener von Twitter-Bots, die höchstens 17 Prozent der britischen Bevölkerung erreichen können.

Die Wirksamkeit digitaler Desinformation ist wissenschaftlich nicht eindeutig belegt. Jüngste Studien über die Relevanz von Filterblasen kommen zu differenzierten Ergebnissen. Empirische Daten deuten darauf hin, dass Nutzer bewusst bestimmte Formate und Inhalte wählen, die von denen der etablierten Medien abweichen. Filterblasen des Dissenses entstehen offenbar nicht deshalb, weil die Nutzer sich nicht bewusst sind, dass Informationen einseitig oder falsch sein können. Vielmehr scheint hier das ausdrückliche Interesse der Nutzer an abweichenden Meinungen den Ausschlag zu geben. Dies geht einher mit dem stetigen Verlust des Vertrauens demokratischer Gesellschaften in politische und öffentliche Institutionen. Die Vorstellung, Filterblasen würden bewusst gebildet und kontrolliert, wird dadurch verstärkt, dass es sich eher um kleine Gruppen zu handeln scheint, die »alternative Fakten«, Desinformationen und offenkundig falsche Berichte besonders lautstark verbreiten. Daher dürfte die Befürchtung, digitale Algorithmen könnten soziale Kommunikation in weiten Teilen zerstören, eher übertrieben sein.

IT-gestützte Desinformation

Technische Maßnahmen der EU zur Bekämpfung von Desinformationskampagnen und Cyberangriffen sind nur ein erster Schritt. Im Idealfall bewirken sie, dass die Mitgliedstaaten die Europawahlen während Wahlkampf, Wahlakt und Auszählung besser zu schützen versuchen. Stetiger Austausch und regelmäßige Cybersicherheitsübungen sind nötig, um Gefahren zu minimieren. Allerdings wurde bisher in den meisten Mitgliedstaaten versäumt, Wahlen als für die Demokratie kritische Infrastruktur zu begreifen und deshalb auf hohem Niveau zu sichern. Daher müssen Hersteller und Anbieter kritischer IT-Produkte dringend stärker in die Pflicht genommen werden. Ungesicherte IT-Hard- und Software in der Wahltechnologie ist nach wie vor ein unterschätztes Problem. Zudem muss die EU langfristig in die Lage versetzt werden, auf Wahlmanipulationsversuche strategisch, kommunikativ und technisch wirkungsvoll zu reagieren, und dafür finanziell und personell ausgestattet werden. Solange dieses Ziel nicht erreicht ist, können während der Wahlen rund um die Uhr Notfallteams eingesetzt werden.

Übermacht der Internetkonzerne

Fraglich ist allerdings, ob die genannten Schwächen von Demokratien in Europa mit

kurzfristigen Taskforces und mittelfristigen Aktionsplänen effektiv angegangen werden können. Sprachwissenschaftliche Forschung zeigt, dass bloßes Fact-Checking eher zur unbeabsichtigten Bestärkung von Falschinformationen führt. Überschätzt wird auch die Wirksamkeit automatisierter Systeme Künstlicher Intelligenz zur Desinformationsbekämpfung. Offenbar ist es illusorisch, Falschinformationen völlig aus der Welt schaffen zu wollen. Statt Symptome zu bekämpfen, wäre es sinnvoll, unabhängige Forschung zu fördern, um Vorschläge für kurzfristige technische und politische Maßnahmen zu analysieren. Sie sollten die Basis für grundsätzliche Reformen bilden.

Googles globaler Marktanteil von 80 Prozent aller Suchanfragen sowie Facebooks und Youtubes Marktanteil von 70 Prozent bei den sozialen Netzwerken sind Ausdruck des beispiellosen Konzentrationsprozesses der kommunikativen Infrastrukturen. Mit der wachsenden Bedeutung digitaler Öffentlichkeiten verlagert sich die Kommunikation in der Gesellschaft hin zu einem marktorientierten Bereich, in dem jeder Sprechakt seinen Preis hat. Private Unternehmen stellen öffentliche digitale Diskursräume bereit; der Zugang zu ihnen wird kontrolliert. Mitspracherecht hat nur, wer ein privates Vertragsverhältnis eingeht und seinen Beitrag entweder finanziell oder in Form wirtschaftlich nutzbarer Daten leistet.

Eine bedingungslose demokratische Beteiligung, die nur den Bürgerstatus voraussetzt, ist in diesen für Vermarktungszwecke entwickelten sozialen Netzwerken nicht vorgesehen. Dies wäre in etwa mit einer Situation zu vergleichen, in der nicht nur das Parlamentsgebäude im Besitz eines privaten Anbieters ist und der Zugang zu ihm nach wirtschaftlichen Kriterien geregelt wird, sondern auch die Lautstärke der Lautsprecher und die Übertragung von Reden nach außen marktgerecht bewertet werden. Dieser Machtkonzentration werden die bisherigen Regulierungsansätze der EU, zum Beispiel das Drängen auf freiwillige Selbstverpflichtungen, nicht gerecht. Folgerichtig kritisieren Rat und Kommission den zurzeit gültigen Verhaltenskodex. Er enthalte »keine gemeinsamen Maßnahmen, keine substantiellen Verpflichtungen, keine ›compliance‹ oder Durchsetzungsmaßnahmen«. Als im Dezember 2018 persönliche Daten zahlreicher deutscher Politiker illegal veröffentlicht wurden, reagierte die Online-Plattform Twitter trotz der Selbstverpflichtung des Kodexes nur schleppend. Große Plattformenanbieter haben in Europa kaum Konkurrenz zu befürchten, so dass nur eine grundsätzliche Reform der Kartellgesetzgebung bleibt. Die bisherigen Verfahren zu Bewertung und Kontrolle von Monopolen greifen oftmals zu kurz.

Ein zentrales Problem besteht in der Fusionskontrolle. Große Firmen kaufen aufkeimende, kleinere Konkurrenz-Startups, bevor diese zu einer Bedrohung des Geschäftsmodells werden können. Schlagendes Beispiel dafür ist die Übernahme von WhatsApp und Instagram und die Zusammenführung von Nutzerdaten durch Facebook. Nicht mehr Wahlwerbung im Fernsehen oder der Stand in der Einkaufsstraße sind wahlentscheidend, sondern Technologien Künstlicher Intelligenz wie Microtargeting. Mit ihnen werden gezielt wechselbereite Wähler angesprochen, die oft das Zünglein an der Waage ausmachen. Nur die EU mit ihrer Wirtschaftskraft als Ganzes kann gegen die Macht transnationaler Digitalkonzerne angehen. In diesem Zusammenhang sind die EP-Wahlen ein historischer Wendepunkt: Europapolitik bedeutet, die großen, grundsätzlichen Themen der europäischen Kommunikationsordnung anzugehen, etwa die Kontrolle von Plattformmonopolen und übermäßiger kommunikativer Machtmacht. Im Europawahlkampf müssen Parteien und politische Organisationen sich verpflichten, Transparenz in ihre Kampagnentätigkeit zu bringen und den Einsatz von social bots zu unterbinden.

Dr. Annegret Bendiek ist stellvertretende Leiterin (a.i.) der Forschungsgruppe EU/Europa. Dr. Matthias Schulze ist Wissenschaftler in der Forschungsgruppe Sicherheitspolitik.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6364
doi: 10.18449/2019A10