Freie Universität Berlin

Fachbereich Rechtswissenschaft
Lehrstuhl für Öffentliches Recht und Europarecht

Prof. Dr. Christian Calliess, LL.M.
Boltzmannstr. 3
14195 Berlin

Telefon +49 30 838-51456
Fax +49 30 838-53012
E-Mail europarecht@fu-berlin.de

Schriftliche Stellungnahme von Prof. Dr. Christian Calliess*

zur Öffentlichen Anhörung des Ausschusses für die Angelegenheiten der Europäischen Union des Deutschen Bundestages

am Montag, den 2. März 2020

zum Thema

„Wehrhaftigkeit der demokratischen Verfasstheit der Europäischen Union und Integrität von Willensbildungsprozessen“

* Von 2015 bis 2018 war der Verfasser von seiner Professur beurlaubt, um als Rechtsberater und Leiter des Institutionellen Teams des European Political Strategy Centre (EPSC), dem Strategieteam des Präsidenten der Europäischen Kommission, zu arbeiten. In diesem Kontext hat er auch zu den Themen „Security Union“ und Cybersecurity“ gearbeitet (siehe Fn. 7). Auf dieser Basis war er wiederum an Arbeiten des EPSC (siehe Fn. 1 und 5) beteiligt, die für das Thema der vorliegenden Anhörung relevant sind. In vielen Punkten geht die schriftliche Stellungnahme jedoch über diesen politischen Diskussionsstand akademisch hinaus. In jedem Fall gibt die Stellungnahme ausschließlich die persönliche Auffassung des Verfassers wieder und bindet in keiner Weise die Institution, der er angehörte.

1) **Mit Blick auf Frage 1:** Der Antrag „Schutz der liberalen Demokratie in Europa“ (BT-Drucksache 19/9225) thematisiert ein Phänomen, dem die deutsche und europäische Politik im Rahmen der deutschen Ratspräsidentschaft **erhöhte Aufmerksamkeit** widmen sollte. **Desinformation, politisches Hacking und aus Drittstaaten finanzierte politische Online-Werbung sind nachweislich zu politischen Instrumenten geworden, mit denen externe und interne Akteure die Demokratie in Deutschland und Europa schwächen wollen.** Facebook, Twitter, Google und andere Social-Media-Plattformen gerieten in Europa und den Vereinigten Staaten in den Fokus der Kritik als bekannt wurde, dass staatliche Geheimdienste ebenso wie (mitunter von ihnen unterstützte) europäische und amerikanische Akteure diese Plattformen nutzen, um aktiv Desinformationen und „Leaks“ von politischen Hackern zu verbreiten. Insoweit geht es also nicht mehr um die von der Informations- und Meinungsfreiheit geschützte Aktivität der 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 Bürger in die Demokratie der EU und ihrer Mitgliedstaaten durch Lüge und Hetze sowie illegale erlangte Informationen zu erschüttern. **Zahlreiche Beispiele sind insoweit dokumentiert**[1], unlängst wurde durch einen Bericht des britischen Parlaments bekannt, dass auch die Abstimmung über den Brexit durch gezielte Desinformation beeinflusst war[2].

Mit Blick auf das hohe Schutzgut der Demokratie und der für ihre Vertrauenswürdigkeit bedeutsamen Wahlen und Abstimmungen, können die demokratischen Verfassungsstaaten in der EU ebenso wenig wie die EU selbst tatenlos zusehen, wie sich ihre Grundlagen von innen heraus selbst auflösen. Empirische Belege, die insoweit eine **hinreichende**

[1] Vgl. dazu die Papiere des European Political Strategy Centre (EPSC) der Europäischen Kommission, https://ec.europa.eu/epsc/sites/epsc/files/epsc_democracy_10trends.pdf; https://ec.europa.eu/epsc/events/high-level-hearing-preserving-democracy-digital-age_en; https://ec.europa.eu/epsc/sites/epsc/files/epsc_-_election_interference_thinkpieces.pdf.; Dachwitz/Kurz, Microtargeting und Manipulation – Von Cambridge Analytica zur Europawahl, https://www.bpb.de/gesellschaft/digitales/digitale-desinformation/290522/micro-targeting-und-manipulation-von-cambridge-analytica-zur-europawahl vom 2. Mai 2019.

[2] Vgl. Disinformation and ‘fake news’: Final Report, https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-re - port-published-17-19/ vom 18. Februar 2019; ferner Spence/Di Stefano: A Mysterious Hard Brexit Group Run By A Young Tory Writer Is Now Britain’s Biggest Spending Political Campaign On Facebook https://www.buzzfeed.com/alexspence/mysterious-facebook-brexit-group-britains-future-tim-dawson vom 9. März 2019.

Wahrscheinlichkeit im Sinne der Gefahrenabwehr begründen, erlauben und erfordern ein Handeln der verantwortlichen staatlichen Institutionen 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.

Angesichts der bestehenden **Grauzone zur für die Demokratie unabdingbaren Informations- und Meinungsfreiheit** ist ein **differenziertes und abgestuftes Vorgehen** erforderlich, das von Aufklärung und Bildung zum eigenverantwortlichen und kritischen Umgang mit Nachrichten in den sozialen Medien bis hin zu robusten Maßnahmen gegenüber von Geheimdiensten in Drittstaaten gesteuerten Aktionen reichen kann.

Zutreffend wird im Antrag festgestellt, dass die Beeinflussung von Politik, Bevölkerung und Wahlen mittels Propaganda und Desinformation zwar kein neues Thema ist, sich jedoch die Methoden im digitalen Zeitalter weiterentwickelt haben.

Was den **Titel des Antrags** „Schutz der liberalen Demokratie in Europa“ (BT-Drucksache 19/9225) betrifft, so scheint mir der Begriff der „liberalen“ Demokratie – zumindest aus rechtlicher Sicht – nicht zielführend. Das Grundgesetz kennt diesen Begriff ebenso wenig wie die EU-Verträge. Beide Verfassungen definieren Elemente der Demokratie (vgl. Art. 20 GG sowie Art. 2 i.V.m. Art. 9 bis 12 EUV), die es zu wahren und zu verteidigen gilt.[3] Vor diesem Hintergrund könnte der Titel des Antrags zu dem Missverständnis verleiten, dass nicht die verfassungsrechtlich garantierte Demokratie, sondern eine bestimmte, nach politischen Präferenzen definierte Form der Demokratie geschützt werden soll. Aus diesen Gründen rege ich an, die Formulierung „liberalen“ zu streichen.

2) **Mit Blick auf Frage 11 und 2:** Neben diesen auch im Antrag „Schutz der liberalen Demokratie in Europa“ (BT-Drucksache 19/9225) benannten und beschriebenen Instrumenten erscheinen mir **zwei weitere Herausforderungen** im Zusammenhang mit politischem Hacking **noch größere Aufmerksamkeit** zu verdienen:

[3] Vgl. zu diesem komplexen Thema die Beiträge in: Heinig/Terhechte (Hrsg.), Postnationale Demokratie, Postdemokratie, Neoetatismus, Wandel klassischer Demokratievorstellungen in der Rechtswissenschaft, 2013 sowie Calliess/Hartmann, Zur Demokratie in Europa: Unionsbürgerschaft und europäische Öffentlichkeit, 2014, S. 71 ff.

- Zum einen können Cyberangriffe den Zugang zu elektronischen Wahlmaschinen oder digital verwalteten Wahlergebnissen ermöglichen und diese, ohne Spuren zu hinterlassen, manipulieren. In Deutschland gibt es zwar nicht die Möglichkeit einer elektronischen Stimmabgabe, aber der Zugang zu den Systemen der Stimmauszählung, mit denen Wahlbeamte die Wahlergebnisse der 70.000 Stimmbezirke verschicken, erscheint nicht sicher[4]. In den Vereinigten Staaten hackte ein Universitätsforscher auf der DEFCON, der weltweit größten Hackerkonferenz in Las Vegas, in wenigen Minuten eine der 25 am häufigsten verwendeten dortigen Wahlmaschinen. Es gelang die Wahlprotokolle zu ändern. Die Maschine lief mit veralteter Software und hatte das Passwort "abcde", das von den Wahlbeamten nicht geändert werden konnte. Darüber hinaus sind die amerikanischen Wahlmaschinen mit ausländischer Hard- und Software ausgestattet, in die Malware und Sleeper-Befehle eingebettet werden können. Insoweit **fehlt es an verbindlichen Sicherheitsvorgaben für Hersteller und Lieferanten und einer daran anknüpfenden europaweit gültigen Zertifizierung**.[5] 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.

- Mit größter Aufmerksamkeit sollte auch die nächste Stufe der Desinformation verfolgt werden: Zunehmend werden **Techniken zur Manipulation von Videos** perfekter; Forscher haben mit Hilfe künstlicher Intelligenz ein Programm entwickelt, mit dem sie modellierten, wie sich Präsident Obamas Mund bewegt, wenn er spricht. Diese Technik erlaubte es ihnen, beliebige Worte in den Mund ihres „synthetischen“ Obamas zu legen.

3) **Mit Blick auf Frage 6:** Bislang fehlt es den demokratischen Verfassungsstaaten an einer gemeinsamen und umfassenden Strategie. Die **Definition einer solchen Strategie ist aus verschiedenen Gründen nicht ganz einfach**: Erstens kennen wir das genaue Ausmaß

[4] http://www.zeit.de/digital/datenschutz/2017-09/bundestagswahl-wahlsoftware-hackerangriff-sicherheit-bsi-bundeswahlleiter (zuletzt aufgerufen am 26.02.2020)

[5] http://www.politico.com/story/2017/10/09/russia-voting-machines-hacking-243603 (zuletzt aufgerufen am 26.02.2020)

der Herausforderungen noch nicht. Zweitens werden Ausmaß und Art der Herausforderungen noch zunehmen, wenn ihr Potential bekannter und weiter entwickelt wird. Im Zuge dessen werden auch in Europa zunehmend legale, kriminelle oder in einer Grauzone operierende Unternehmen entstehen, die einige der oben beschriebenen „Dienstleistungen" für externe und interne Akteure erbringen. Politische Parteien könnten einen Bedarf sehen, einige dieser „Dienstleistungen" zu kaufen, zumal wenn immer mehr Daten zum soziopolitischen Profiling der Bürger von privaten Unternehmen gesammelt und vorgehalten werden. Zutreffend beschreibt der Antrag „Schutz der liberalen Demokratie in Europa" (BT-Drucksache 19/9225) insoweit unter Punkt 17 des Antrags die Rolle von des amerikanischen Unternehmens Cambridge Analytica. Drittens wird die digitale Gesellschaft wachsen. Die Zahl der Europäer mit Internetzugang wächst und die sozialen Medien entwickeln sich zunehmend zu einer intergierten Plattform, die eine Fülle von Diensten vorhalten. **Der Markt für Werbung wird wachsen und die KI-Technologie wird ausgefeilter werden - von stumpfen Bots zu besser glaubwürdigen Simulationen von Menschen**.

4) **Mit Blick auf Frage 6 und 12:** Die EU und einige ihrer Mitgliedstaaten beginnen vor dem Hintergrund dieser neuen Herausforderungen erst langsam aktiv zu werden. Angesichts ihrer begrenzten Kompetenzen bzw. der Zurückhaltung der Mitgliedstaaten auf diesem Gebiet der EU eine starke Rolle zuzuweisen, beschränken sich die Maßnahmen der EU auf eine **Koordinierung der Mitgliedstaaten** in Reaktion auf Desinformation, eine Plattform für die interinstitutionelle Zusammenarbeit mit der NATO und erste mittel- und langfristige Maßnahmen und Vorschläge der EU[6] in Form der Mitteilung der Europäischen Kommission (KOM(2018) 236 endg) sowie dem gemeinsamen Aktionsplan gegen Desinformation der EU-Institutionen (JOIN(2018) 36 endg.), die in dem Antrag „Schutz der liberalen Demokratie in Europa" (BT-Drucksache 19/9225) unter 13., 14. und 15. erwähnt sind.

Diese Maßnahmen können jedoch mit Blick auf die Bedeutung der Bedrohung erst einen Anfang darstellen: **Zum einen leiden die Maßnahmen unter vielfältigen Defiziten in der Praxis, zum anderen müssen sie zum Teil robuster werden**:

[6] Siehe dazu auch die Vorschläge des European Political Strategy Centre (EPSC) der Europäischen Kommission, https://ec.europa.eu/epsc/sites/epsc/files/epsc_democracy_10trends.pdf; https://ec.europa.eu/epsc/events/high-level-hearing-preserving-democracy-digital-age_en; https://ec.europa.eu/epsc/events/election-interference-digital-age-building-resilience-cyber-enabled-threats_en

So reagiert der Europäische Auswärtige Dienst (EAD) zwar **zum Beispiel** mit StratCom East auf russische Desinformation. Das Team führt Kommunikationskampagnen in den Regionen der östlichen Partnerschaften durch und entlarvt in Abstimmung mit anderen EU-Akteuren gefälschte Nachrichten, die von für diese Zwecke instrumentalisierten Medienseiten stammen. Das Team setzt sich jedoch hauptsächlich aus abgeordneten nationalen Experten zusammen. Dies kann ein Vorteil sein, wenn es darum geht, die Eigenverantwortung mit den Mitgliedsstaaten zu stärken und bei Bedarf auf mehr Ressourcen und Wissen zuzugreifen, birgt aber auch die Gefahr plötzlicher Veränderungen oder des Verlusts von Expertise. 2018 bestand das Team aus nur 14 Personen, zusätzlich zu weiteren 10 Personen, die auf dem Westbalkan und in der MENA-Region arbeiten.

Auch die sog. Hybrid-Fusioncell, die im EU-Nachrichtenzentrum INTCEN des EAD untergebracht ist, muss gestärkt werden. Sie dient der Aufdeckung von Querschnittsfragen, auch im Bereich der Desinformation und des politischen Hacking. Sie wurde im April 2015 eingerichtet und bestand 2018 aus 7 Analysten, die einen faktenbasierten analytischen Überblick geben, während StratCom eine sofortige qualitative, aber quantitativ begrenzte Reaktion ermöglicht.

5) **Mit Blick auf Frage 6:** Deutschland und die EU sollten sich bei all ihren Maßnahmen auf die folgenden **vier Leitprinzipien** stützen:

- Transparenz. Die Öffentlichkeit soll wissen können, wer die Quelle einer Anzeige ist und mit wem oder was die Bürger über soziale Medien interagieren. Es sollte erkennbar sein, was ein Bot ist und was nicht, und ob eine „Nachricht“ aufgrund der Interaktion mit dem Bot einen realen Trend darstellt. Die bislang selbstverständliche Anonymität im Internet wird ganz allgemein zunehmend zu einer Herausforderung. Je mehr sich der Cyberraum zu einer zweiten (sog. virtuellen) Lebenswelt der Menschen entwickelt, desto mehr sollte über Möglichkeiten nachgedacht werden, Identitätsfeststellungen analog der klassischen (sog. realen) Lebenswelt zu ermöglichen.

- Vielfalt. Mittelfristig geht es darum, die Medienkompetenz der Bürger, insbesondere der Jugend in der Schule, zu erhöhen und sicherzustellen, dass journalistische Qualitätsprodukte in den Ergebnissen von Suchmaschinen besser dargestellt werden.

- Glaubwürdigkeit. Ohne feststellbare Identitäten wird das Vertrauen der Bürgerinnen und Bürger in Social-Media-Plattformen und in die digitale demokratische Konversation im Allgemeinen mit der Zeit schwinden. Die Medien sollten versuchen, ihre eigene Glaubwürdigkeit und Integrität zu wahren, vielleicht sogar eine **nichtstaatliche Rating-Agentur** schaffen. Die Mitgliedstaaten sollten **Anreize erhalten, ihre Wahlgesetze und -vorschriften zu modernisieren**. Gemeinsam mit der EU sollten sie gleichermaßen die Strukturen der Krisenreaktion stärken und anpassen und mehr Kompetenz und Expertise im Bereich der sozialen Medien generieren.

- Geteilte Verantwortung. Demokratie ist im demokratischen Verfassungsstaat eine gemeinsame Verantwortung von Politik und Gesellschaft, EU und Mitgliedstaaten, Unternehmen und Verbrauchern. Es bedarf daher **gemeinsamer Ziele und vernetzter Strategien, entsprechender Investitionen und eines arbeitsteiligen Zusammenwirkens aller Akteure**. Vor diesem Hintergrund sollte die EU über ihre im Rahmen der Wettbewerbspolitik angestrengten individuellen Maßnahmen hinaus – ähnlich wie bei der Datenschutz-Grundverordnung – **Standards für die sozialen Medien und die Datenerhebung durch Plattformen** formulieren.

Aufbauend auf diesen Leitprinzipien können ganz konkret verschiedene Aktionsfelder und diesbezügliche Maßnahmen identifiziert werden.

6) **Mit Blick auf Frage 6 und 9:** Kein einzelner Akteur kann den Schutz der europäischen Demokratie im europäischen Staaten- und Verfassungsverbund allein lösen. Die EU sollte daher die Mitgliedsstaaten, Unternehmen und Akteure der Zivilgesellschaft mobilisieren, um zu einer **umfassenden Strategie** und deren Umsetzung beizutragen.

Diese Arbeit könnte auf dem in der Europäischen Kommission von der Generaldirektion CONNECT und der High-Level-Group gestarteten Prozess aufbauen. Dazu könnte die Dynamik des **Digital Summits** genutzt werden, um ein Format für einen **Digital Council** zu schaffen. Zusammen mit Experten aus der Zivilgesellschaft könnte dieser Rat Grundsätze für die **digitale Governance** in der EU festlegen, die von den Technologieunternehmen zu beachten sind. Der im Antrag „Schutz der liberalen Demokratie in Europa“ (BT-Drucksache 19/9225) erwähnte Verhaltenskodex für Online-Plattformen, den die Kommission im

September 2018 vorgelegt hat, stellt insoweit einen ersten Schritt dar. Dessen Wirksamkeit ist genau zu beobachten, gegebenenfalls ist nachzubessern und Verbindlichkeit herzustellen.

Zugleich 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 eine sofortige Identifizierung gefälschter Online-Nachrichten gewährleisten.

Überdies könnten ein **Narrativ und ein Leitbild** für ein stärker auf den Menschen ausgerichtetes Internet, dass die europäischen Grundwerte unterstützt, entwickelt werden (z.B. aufbauend auf der EU-Plattform der Internet-Initiative der nächsten Generation). Denn die EU sollte wie andere Regionen in der Welt massiv in Technologie investieren und diese dabei so gestalten, dass sie ihren Werten entspricht. Daran anknüpfend sollte eine Ausrichtung der Finanzierung und Förderung von Technologie, die die demokratische Werte betont, erfolgen.

- Für Unternehmen, NGOs und Forschungseinrichtungen sollten Anreizstrukturen geschaffen werden, um darüber nachzudenken, wie sich Desinformation oder gefälschte Nachrichten im Laufe der Zeit entwickeln könnten (z.B. die Ausweitung auf Audio und wahrscheinlich bald auch auf Video). Forscher sollten mit Unternehmen zusammenarbeiten, um im Rahmen von durch die EU, private Investoren und Stiftungen finanzierten Projekten zusammenzuarbeiten und neue Methoden zur Bewertung des Wahrheitsgehalts von Nachrichten (auch durch spezialisierte Beobachtungsstellen) zu entwickeln, z.B. im Rahmen des Arbeitsprogramms "Horizon EU" für die nächsten Jahre.

- Im Rahmen der Kohäsionspolitik könnten die Ziele der Fonds um digitale Resilienz erweitert werden, um so die Städte und Gemeinden in ganz Europa zu stärken und Inspiration und Vorbilder für andere Städte zu schaffen.

7) **Mit Blick auf Frage 7 und 10:** Darüber hinaus könnte die EU Gesetzgebung auf den Weg bringen, mit der (über das NetzDG hinaus) die **Verantwortung für Inhalte in den sozialen Medien** angelehnt an das europäische Presserecht, jedoch nach der Technologie modifizierend, geregelt wird. 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 – unterstützt durch europäische Fördergelder mit einem dem Demokratieprinzip verpflichteten Informationsauftrag zur Grundversorgung aufgebaut werden. Im Interesse der Vertrauenswürdigkeit und Glaubwürdigkeit muss eine solche öffentlich-rechtliche Grundversorgung der strikten Kontrolle durch politisch unabhängige und sachverständige 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“ [7] so definiert werden, dass er im Zuge seiner Begrenzung auf die europäische Grundversorgung nicht nur eine sinnvolle Koexistenz mit privaten Medien tritt, sondern privaten Qualitätsmedien vielleicht sogar neue Einnahmequellen erschließt, indem er (statt Google) auch als Plattform für bereits vorhandene journalistische Inhalte fungiert.

8) **Mit Blick auf Frage 6, 12 und 14:** Auf EU-Ebene sollten zudem über **institutionelle Strukturen nachgedacht werden, die ein „Ownership“** im Hinblick auf den Schutz der Demokratie in Europa gewährleisten:

Dem Präsidenten der Europäischen Kommission sollte eine **Struktur für das Krisen<u>management</u>** 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 4 Mitarbeitern, Western Balkans mit 2 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

[7] So z.B. auch der Vorschlag des damaligen Abgeordneten im Europäischen Parlament Jakob von Weizsäcker: https://www.spiegel.de/kultur/gesellschaft/europaeische-union-jakob-von-weizsaecker-fordert-europafunk-a-1071803.html; ferner Riecher, Ein Europafunk nach dem Vorbild von ARD und ZDF, in: Hooffacker/Kenntemich/Kulisch (Hrsg.), Die neue Öffentlichkeit, 2019.

Forschung und Projekte in Auftrag zu geben. Überdies sollten die Mitgliedstaaten Anreize erhalten, um nationale Experten längerfristig abzuordnen und solchermaßen ein arbeitsteiliges Zusammenwirken zwischen EU und Mitgliedstaaten zu gewährleisten.

Die **EU-Agentur für Netz- und Informationssicherheit (ENISA)** könnte 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. Auf dem Erfahrungsaustausch basierend könnten **Leitlinien und Regelbücher** für den Umgang mit diesen Herausforderungen formuliert werden.

Die EU-Institutionen laufen ebenso wie die nationalen Ministerien Gefahr, in der Welt von Morgen ins Abseits zu geraten, wenn sie nicht **mehr Mitarbeiter mit digitalem Verständnis und technischen Fähigkeiten** gewinnen. Indem sie Digital-Ingenieure aus Technologieunternehmen einsetzt und sie mit langjährigen Experten der Kommission in Verbindung bringt, könnte die EU eine natürliche Gemeinschaft für die Diskussion von Werten in der Technologie innerhalb „der Blase“ schaffen.

9) **Mit Blick auf Frage 6, 12 und 14:** 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 gesetzlicher Rahmen, der es den angegriffenen Mitgliedsstaaten erlaubt, schnell mit Strafverfolgungsbehörden und Internetanbietern außerhalb ihrer eigenen Grenzen zu interagieren und den Angriff abzuschalten**.

Zugleich **fehlt der EU ein wirksamer Krisen<u>reaktionsmechanismus</u>**, der sofort auf gegen die EU gerichtete Angriffe reagieren und die Ressourcen der EU insgesamt, vor allem aber auch der zuständigen Generaldirektionen der Europäischen Kommission wirksam koordinieren kann. Dies gilt auch für Krisen, die mehrere Mitgliedstaaten betreffen.

- Insoweit könnte ein erster Schritt darin bestehen, beim Präsidenten der Europäischen Kommission eine **Task Force** zu etablieren, die alle Akteure innerhalb der Kommission regelmäßig zusammenführt. Zugleich könnte das **EU-Koordinierungszentrum für Notfallmaßnahmen** dem Generalsekretariat der Kommission unterstellt werden, wobei der Standort bei der Generaldirektion ECHO

beibehalten werden könnte, um dessen kontinuierliche Konzentration auf Naturkatastrophen und andere Notfälle nicht zu gefährden.

- Ein zweiter Schritt wäre die Einrichtung einer EU-Plattform, die ENISA, die erwähnten Einrichtungen des EAD (INTCEN, StratCom, Hybrid-Fusionszelle usw.), 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.[8] 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.

- Unter dieser Prämisse sehe ich keine Notwendigkeit für die Einrichtung der von Präsident Macron vorgeschlagenen europäischen **Agentur für den Schutz der Demokratie**. Das in einer **Europäischen Agentur für Cybersicherheit** versammelte Know-How ist besser in der Lage die komplexen Bedrohungslagen einzuschätzen und könnte in Zusammenarbeit mit den zuständigen Generaldirektionen der Europäischen Kommission Experten entsenden, die den Mitgliedstaaten mit Rat und Tat zur Seite stehen.

[8] Ausführlich dazu Europäische Kommission, European Political Strategy Centre (EPSC): Building an Effective European Cybershield, Issue 24, 8 May 2017: https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en; ähnlich CEPS, Strengthening the EU's Cyber Defence Capabilities, Report of a CEPS Task Force, November 2018: https://www.ceps.eu/system/files/CEPS_TFR on Cyber Defence_1.pdf

10) **Mit Blick auf Frage 8 und 11:** Darüber hinaus sollten nationale Wahlen als Schutzgut und Wahltechnologie als „kritische Infrastruktur“ in die 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 v**erbindliche Sicherheitsvorgaben für Hersteller und Lieferanten und einer daran anknüpfenden europaweit gültigen Zertifizierung**.[9]

Schließlich könnte die EU eine Gesetzgebung auf den Weg bringen, die von **ausländisch kontrollierten Medienunternehmen die Offenlegung ihrer Finanzierungsquellen** verlangt, wie dies im Vorschlag des US-Kongresses für einen "Foreign Agents Modernization and Enforcement Act" gesehen wird.

11) Zugleich sollte sich die EU auf der anderen Seite des Atlantiks und in anderen Teilen der Welt nach Partnern umsehen, die sich den Bemühungen um die Sicherung der Demokratie und der Stärkung der digitalen Widerstandsfähigkeit anschließen wollen. Diese Bemühungen könnten in der OECD oder in einer neuen "**Allianz für digitale Demokratie**" verankert werden und zu einem Forum werden, in dem Praktiken und neue Anliegen ausgetauscht werden.

Christian Calliess

[9] Zu Bedeutung und Begriff “kritischer Infrastruktur” und zur Notwendigkeit der Zertifizierung: Europäische Kommission, European Political Strategy Centre (EPSC): Building an Effective European Cybershield, Issue 24, 8 May 2017: https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en