Digitale Agenda und Cybersicherheit

Hans-Wilhelm Dünn/Lukas W. Schäfer

Seitdem die Europäische Union 2010 die Digitale Agenda als eine der sieben Leitinitiativen der Europa 2020-Strategie verabschiedet hat, um mit dem Prozess der europäischen Integration einen ebenso fairen, offenen und sicheren digitalen Raum zu schaffen, sind immer stärkere Interdependenzen zwischen den relevanten Politik- und Themenfeldern entstanden. So kann der Fortschritt des Digitalen Binnenmarktes nicht ohne Entwicklungen im Bereich der Cybersicherheit betrachtet werden. Vielmehr steigt durch die anhaltende Digitalisierung von Politik, Wirtschaft und Gesellschaft der Bedarf an Sicherheitslösungen, sodass die damit einhergehende Forschung und Entwicklung von Cybersicherheitstechnologien die Stärke und Wettbewerbsfähigkeit des digitalen Binnenmarktes gewährleistet.

Cybersicherheit im Kontext der Europawahlen 2019

Angesichts der Europawahlen 2019 war Cybersicherheit zuletzt ein zentrales Thema der Europäischen Union und wurde mit hoher Priorität auf der politischen Ebene verfolgt. Vor dem Hintergrund der Erfahrungen mit dem französischen Präsidentschaftswahlkampf 2017 oder dem Cambridge Analytica-Datenmissbrauch zum Zwecke des Mikrotargeting, schlug die Europäische Kommission am 12. September 2018 per Mitteilung ein Maßnahmenpaket zur Gewährleistung freier und fairer Europawahlen vor.[1] Es stellt gewissermaßen eine für die Europawahl konkretisierte Ausarbeitung der bereits im Juni 2018 von der Europäischen Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik geforderten Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen dar.[2] Hervorzuheben ist in diesem Maßnahmenpaket die Empfehlung zur Installation eines europäischen Wahlkooperationsnetzes. Darin sollen die beteiligten nationalen Behörden, etwa aus den Feldern Datenschutz, Medienaufsicht und IT-Sicherheit, Informationen zum Schutz des Wahlprozesses in Echtzeit austauschen, sowie effektiv Reaktionen auf Desinformationskampagnen koordinieren können. Es ist zudem vorgesehen, diese Zusammenarbeit über die Europawahl hinaus aufrecht zu erhalten, um die Integrität aller kommenden nationalen, regionalen und lokalen Wahlen der Europäischen Union sicherzustellen. Die ersten beiden der für das Europawahljahr vorgesehenen vier Sitzungen fanden im Januar beziehungsweise Februar 2019 statt.[3]

Darüber hinaus erarbeitete die Europäische Kommission mit dem Maßnahmenpaket Leitlinien zur Anwendung der seit dem 25. Mai 2018 gültigen Europäischen Datenschutzgrundverordnung (DSGVO) auf den Wahlprozess und dazugehörigen Wahlkampf. Ziel der

1 Europäische Kommission: Mitteilung der Kommission, Freie und faire Europawahlen gewährleisten, 12.9.2018, COM(2018) 637 final.

2 Europäische Kommission: Gemeinsame Mitteilung, Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen, 13.6.2018, JOIN(2018) 16 final.

3 Europäische Kommission: Erklärung, Verhaltenskodex zur Bekämpfung von Desinformation, 28.2.2019, STATEMENT/19/1379.

Ausarbeitung war die Aufklärung aller beteiligten Akteure, von nationalen Wahlbehörden und Parteibüros bis hin zu Kommunikationsagenturen, über die legale Auslegung der Vorschriften. Zur Prävention des Missbrauchs personenbezogener Daten wurden zudem Änderungen an der Verordnung über das Statut und die Finanzierung europäischer politischer Parteien und Stiftungen vorgenommen. Demnach können Parteien oder Verbände, die geltende Datenschutzvorschriften für die eigene Vorteilsnahme missbrauchen, mit einem Bußgeld von bis zu fünf Prozent des Jahresbudgets durch die Behörde für europäische politische Parteien und europäische politische Stiftungen sanktioniert werden. Ferner können für das Folgejahr vorgesehene finanzielle Mittel gestrichen werden.[4] Für die Gewährleistung freier, fairer und sicherer Wahlen wurde gleichzeitig die Zusammenarbeit mit Onlineplattformen, sozialen Netzwerken und der Wirtschaft gesucht: Wirtschaftsverbände, die Non-Profit Mozilla Foundation sowie die Digitalkonzerne Google, Facebook und Twitter unterzeichneten den am 26. September 2018 von der Europäischen Kommission vorgelegten Verhaltenskodex zur Bekämpfung von Desinformation.[5] Im Rahmen der Bewertung der in Folge ergriffenen Maßnahmen sprach die Europäische Kommission knapp zwei Wochen vor der Wahl ihre Anerkennung für Fortschritte vornehmlich in den Bereichen Transparenz bei themenbezogener Werbung, Entfernung von nach europäischem Recht illegalen Werbeinhalten sowie Entfernung von Falschkonten aus.[6]

Neben der Kompetenzerweiterung zum Onlineschutz der Wahlen wurden bestehende Strukturen gestärkt. Der im Dezember 2018 verabschiedete und auf dem Maßnahmenpaket aufbauende Aktionsplan gegen Desinformation erhöhte das Budget des bisherigen Flaggschiffes für strategische Kommunikation des Europäischen Auswärtigen Dienstes – die 2015 eingerichtete East StratCom Task Force (East Strategic Communication Task Force beziehungsweise Strategisches Kommunikationsteam Ost) – im Vergleich zu 2018 um drei Mio. Euro auf fünf Mio. Euro im Jahr 2019.[7] Zudem wurden der Taskforce, deren Fokus auf einer proaktiven Kommunikation europäischer Politik in den Ländern der Östlichen Partnerschaft[8] sowie dem Entgegenwirken russischer, diffamierender Propaganda liegt, 50 bis 55 neue Stellen zugesprochen.

Die Cybersicherheit im Sinne von Resilienz europäischer beziehungsweise nationaler Wahlinfrastrukturen wurde Anfang April 2019 in Form einer Simulation zur Erprobung der Reaktions- und Notfallpläne für mögliche Cybersicherheitsvorfälle getestet.[9] Angesichts der Tatsache, dass die Hauptverantwortung für den Schutz der Integrität von Wahlen den Mitgliedstaaten vorbehalten ist, waren insbesondere die aus der Übung abgeleiteten Erkenntnisse zur Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden auf nationaler Ebene und der grenzüberschreitenden Kooperation mit den verantwortlichen Stellen auf europäischer Ebene von großem Wert. Fortwährend wird den Mitgliedstaaten

4 Rat der Europäischen Union: Mitteilung an die Presse. Europawahl: neue EU-Vorschriften sollen den Missbrauch personenbezogener Daten durch die europäischen Parteien verhindern, Brüssel, 19.3.2019, Dok. 200/19.

5 Europäische Kommission: Erklärung, Verhaltenskodex für Online-Desinformation, 26.9.2018, STATEMENT/18/5914.

6 Europäische Kommission: Erklärung, Verhaltenskodex zur Bekämpfung von Desinformation: Kommission begrüßt Maßnahmen von Online-Plattformen im Vorfeld der Europawahlen, 23.4.2019, Dok. 19/2174.

7 Europäische Kommission: Factsheet, Fragen und Antworten – EU verstärkt Maßnahmen gegen Desinformation, Brüssel, 5.12.2018. MEMO/18/6648.

8 Vgl. hierzu auch den Beitrag „Östliche Partnerschaft“ in diesem Jahrbuch.

9 Europäische Kommission: Pressemitteilung, EU-Mitgliedstaaten testen ihre Abwehrbereitschaft im Bereich der Cybersicherheit im Hinblick auf faire und freie Europawahlen 2019, 5.4.2019, IP/19/2011.

die Umsetzung des bereits im Juli 2018 veröffentlichten Kompendiums zur Cybersicherheit von Wahltechnologie der Kooperationsgruppe für Netz- und Informationssicherheit (NIS[10]) empfohlen, welches praktische Hinweise für Cybersicherheitsbehörden und Wahlgremien enthält.[11] Letztendlich fanden im Rahmen der Europawahlen nach gegenwärtigem Erkenntnisstand jedoch keine erfolgreichen Cyberangriffe oder großangelegten Desinformationskampagnen statt.

Ausbau der europäischen Cybersicherheitsarchitektur

Gleichzeitig mit dem Maßnahmenpaket vom 12. September 2018 reichte die Europäische Kommission einen Vorschlag für eine Verordnung zur Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und eines tragenden Netzes nationaler Koordinierungszentren ein, dessen legislative Bearbeitung durch Trilogsitzungen des Europäischen Parlaments, der Europäischen Kommission und des Rates der Europäischen Union alsbald möglich nach den Europawahlen fortgesetzt werden soll.[12] Dem übergeordneten Ziel eines in allen Mitgliedstaaten vorhandenen Höchstmaßes an Cybersicherheit soll das Kompetenzzentrum durch die Steigerung der Wettbewerbsfähigkeit von Produkten und Dienstleistungen des europäischen Cybersicherheitsmarktes zur Minderung der Abhängigkeit von außereuropäischen Anbietern dienen. Außerdem sollen das Entwicklungsprinzip „Security by Design", angemessene Zertifizierungsverfahren sowie ein gesellschaftlicher Sensibilisierungsprozess entwickelt und fortgeführt werden. In den Mitgliedstaaten sind nationale Koordinierungszentren zu benennen, die neben ausreichenden Verwaltungskapazitäten über technisches Fachwissen im Bereich Cybersicherheit – zum Beispiel in den Feldern Kryptografie oder Software- und Anwendungssicherheit – verfügen.

Die beteiligten Ausschüsse des Europäischen Parlaments, allen voran der Ausschuss für Industrie, Forschung und Energie (ITRE), begrüßten in großen Teilen den Vorschlag, verlangten allerdings nach einer genaueren Ausarbeitung, insbesondere bezüglich Finanzierung sowie Leistungs- und Umsetzungsstruktur. Denn einerseits sollen unterschiedliche europäische Förderprogramme als Investitionsquellen herangezogen werden, während die Finanzierung seitens der Mitgliedstaaten auf freiwilliger Basis erfolgen soll. Andererseits wird auf eine klare Trennungslinie zwischen dem Aufgabenbereich des Kompetenzzentrums und der Arbeit der Europäischen Agentur für Netzwerk- und Informationssicherheit (ENISA) gedrängt. Schließlich wurde diese jüngst durch das Inkrafttreten des im September 2017 von der Europäischen Kommission initiierten Rechtsakts zur Cybersicherheit in ihrer Position gestärkt, nachdem das Vertragswerk im März 2019 zuerst vom Europäischen Parlament und im Folgemonat vom Rat der Europäischen Union final angenommen wurde. Neben einem ständigen Mandat wurden der ENISA als Cybersicherheitsagentur der Europäischen Union die Unterstützung der Mitgliedstaaten in Fragen der Cybersicherheit, die Durchführung von Cybersicherheitsübungen auf europäi-

10 Vgl. Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, in: Amtsblatt der Europäischen Union Nr. L 194/1, 19.7.2016.

11 NIS Cooperation Group: Compendium on Cyber Security of Election Technology, CG Publication 03/2018, Juli 2018, abrufbar unter: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53645 (letzter Zugriff: 17.6.2019).

12 Europäische Kommission: Vorschlag für eine Verordnung, Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren, 12.9.2018, COM(2018) 630 final.

scher Ebene und die Förderung eines einheitlichen Zertifizierungsverfahrens für cybersichere Produkte, Verfahren und Dienste aufgetragen.[13] Tatsächlich wäre die Erarbeitung beziehungsweise Umsetzung eines angemessenen Zertifizierungsverfahrens für den Digitalen Binnenmarkt und die Cybersicherheitsarchitektur vielversprechend, da durch die anhaltende Digitalisierung von Industrie- und Produktionsketten angesichts der Expansion des „Internets der Dinge" Wirtschaft und Gesellschaft zwar immer digitaler, aber auch angreifbarer werden. Einheitliche und gleichermaßen transparente Standards sind von daher als Kernbestandteil einer sicheren digitalen Infrastruktur zu betrachten, welche Erfolg, Wachstum und Innovation ermöglicht. Zudem könnten einheitliche Sicherheitsstandards einen großen Beitrag zu der Debatte um die zu verwendenden Komponenten und Technologien für den Ausbau des Netzes der fünften Mobilfunkgeneration (5G) leisten.

Wichtige Entscheidungen für Cybersicherheit und digitale Wettbewerbsfähigkeit

Ein belastbares 5G-Netz ist Grundvoraussetzung für die Wettbewerbsfähigkeit und Innovationskraft des gesamten Europäischen, und nicht nur Digitalen Binnenmarktes.[14] Auf europäischer beziehungsweise transatlantischer Ebene ist diesbezüglich eine Sicherheitsdebatte um die Verwendung von 5G-Komponenten des chinesischen Telekommunikationsunternehmens Huawei entbrannt: Dem 5G-Marktführer wird das Vorhandensein von Hintertüren in Produkten und Softwares vorgeworfen, die von der chinesischen Regierung zu Spionagezwecken genutzt werden könnten. Durch die Abhängigkeit digitaler Infrastrukturen und kritischer Dienste von 5G-Netzen und die kontinuierliche Zunahme von Cyberangriffen ist eine Entscheidung bezüglich der Verwendung von Netzkomponenten von Huawei für die Europäische Union demnach von höchster strategischer Bedeutung. Aufgrund dessen verabschiedete die Europäische Kommission im März 2019 entsprechende Empfehlungen zum weiteren Verfahren in dieser Angelegenheit. In erster Linie wurde folgerichtig die Relevanz eines europäischen Rahmens für Cybersicherheitszertifizierungen betont, welcher ein kohärentes Sicherheitsniveau für Unternehmen und Bürger etablieren könnte. Darüber hinaus soll in einem nächsten Schritt eine Risikobewertung zur 5G-Netzinfrastruktur auf nationaler Ebene durchgeführt werden, inklusive der Bestimmung kritischer Komponenten, bei denen Sicherheitsvorfälle erhebliche Störungen nach sich ziehen würden. Mit der Einreichung der Risikobewertungen bis zum 15. Juli 2019 zu Händen der Europäischen Kommission und der ENISA werde dann die Koordination des weiteren Vorgehens der Europäischen Union erfolgen.[15]

Im Zuge der Diskussion um Huawei wurden Stimmen um eine generelle Besinnung auf Produkte und Lösungen „made in Europe" laut, wenngleich diese gegenüber chinesischen Technologien erhebliche Mehrkosten und einen großen Zeitaufwand nach sich ziehen würden. Dennoch wiegen Argumente um die in Europa gegebene Rechtssicherheit und den starken Datenschutz im Lichte der Vorwürfe möglicher chinesischer Spionage schwer.

13 Verordnung (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) vom 17. April 2019, in: Amtsblatt der Europäischen Union L 151/15, 7.6.2019.

14 Vgl. hierzu auch den Beitrag „Forschungs-, Technologie- und Telekommunikationspolitik" in diesem Jahrbuch.

15 Empfehlung (EU) 2019/534 der Kommission zur Cybersicherheit der 5G-Netze vom 26. März 2019, in: Amtsblatt der EU L 88/42, 29.3,2019.

Umso mehr ist es für die zukünftige Wettbewerbsfähigkeit und das Wachstumspotential des Digitalen Binnenmarkts entscheidend, angemessene Investitionsrahmen für europäische Technologien, Lösungen und Innovationen zu schaffen. So erzielten die EU-Institutionen eine Einigung bezüglich des Budgetrahmens des Horizon-2020-Nachfolgerprogramms Horizont Europa, welche im April 2019 vom Europäischen Parlament bestätigt wurde.[16] Mit insgesamt 100 Mrd. Euro soll die europäische Forschung und Entwicklung von 2021 bis 2027 unterstützt werden. Ergänzt wird das Paket durch das für den gleichen Zeitraum vorgesehene Förderprogramm Digitales Europa in Höhe von insgesamt 9,2 Mrd. Euro. Damit sollen ausschließlich Projekte in den Bereichen Hochleistungsrechner, künstliche Intelligenz, Cybersicherheit, fortgeschrittene digitale Kompetenzen und Verbreitung digitaler Technologien in Wirtschaft und Gesellschaft finanziert werden. Eine zügige Aufnahme der weiteren Verhandlungen zwischen den Institutionen wird nach der Konstitution des neuen Europäischen Parlaments erwartet.[17]

Eine europaweite, vom öffentlichen Diskurs begleitete Entwicklung im Digitalen Binnenmarkt stellte die Reform des Urheberrechts dar. Der Legislativprozess wurde mit einem entsprechenden Vorschlag der Europäischen Kommission bereits 2016 angestoßen und nach einigen Anpassungen im März 2019 abgeschlossen.[18] Die Reform, die bis zum 7. Juni 2021 in nationales Recht umgesetzt werden muss, beabsichtigt in erster Linie eine europaweite Verfügbarkeit urheberrechtlich geschützter Werke bei einer gleichzeitigen fairen Vergütung der Kreativschaffenden. Zudem sollte das Urheberrecht eine dem digitalen Zeitalter angemessene sowie einheitliche Auslegung in den Mitgliedstaaten erfahren und so insgesamt den Digitalen Binnenmarkt stärken. Allerdings wurde die an sich überfällige Reform insbesondere aufgrund von Artikel 13 vielseitig kritisiert. Dieser verpflichtet die Betreiber von Internetplattformen zur Überprüfung aller hochgeladener Dateien auf mögliche Urheberrechtsverstöße, was angesichts der schieren Masse an hochgeladenen Daten pro Tag voraussichtlich zu der Anwendung von sogenannten Uploadfiltern führen wird. Aufgrund dessen wird eine massive Einschränkung der künstlerischen Vielfalt sowie der Darstellungs- und Meinungsfreiheit befürchtet, da deren Algorithmen-basierte Funktionsweise allzu häufig legale Inhalte fälschlicherweise entfernt.

Synergien für den Europäischen Integrationsprozess nutzen

Es wird deutlich, dass durch die anhaltende Digitalisierung ein starker Bedeutungszuwachs der Cybersicherheit – auch in Zukunft – auszumachen ist. Beispielsweise gilt die Netzwerkresilienz mittlerweile als entscheidend für gesamteuropäische Wahlprozesse und die freie, öffentliche Meinungsbildung. Gleichermaßen stellt sich heraus, dass Entwicklungen und Entscheidungen im Feld der Cybersicherheit die Dynamiken der gesamten Digitalen Agenda und umgekehrt immer stärker beeinflussen. Herausforderungen können demnach nur noch mit politikfeldübergreifenden Ansätzen erfolgreich adressiert werden. In den dabei entstehenden Synergien besteht eine große Chance für den europäischen Integrationsprozess: Bisweilen wird Cybersicherheit noch als Angelegenheit der inneren

16 Europäische Kommission: Erklärung, Abstimmung des Europäischen Parlaments über Horizont Europa, 17.4.2019, STATEMENT/19/2163.

17 Rat der Europäischen Union: Mitteilung an die Presse. Tagung des Rates. Ausschuss der Ständigen Vertreter. Brüssel, 13.3.2019, Dok. 192/19.

18 Richtlinie (EU) 2019/790 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG vom 17. April 2019, in: Amtsblatt der Europäischen Union L 130/92, 17.5.2019.

Sicherheit von den Nationalstaaten wahrgenommen und beansprucht, sodass sich die Verbindlichkeit notwendiger gesamteuropäischer Ansätze zumeist auf unverbindliche Richtlinien beschränkt. Falls es jedoch gelingt, Cybersicherheit als Faktor für Wirtschaftswachstum und Innovationskraft zu platzieren, ist eine höhere Bereitschaft der Mitgliedstaaten für eine verbindlichere Kooperation, wie bereits etwa in der Wirtschafts- und Handelspolitik, möglich.

Weiterführende Literatur

George Christou: The collective securitisation of cyberspace in the European Union, in: West European Politics 2/2019, S. 278-301.

Annegret Bendiek/Matthias Schulze: Desinformation und die Wahlen zum Europäischen Parlament, in: SWP Aktuell 2019, S. 1-8.

Sebastian Tetzlaff: Entfaltungsspielräume und Risiken für die europäische Integration, in: integration 1/2019, S. 67-73.

László Kovács: Cyber Security Policy and Strategy in the European Union and Nato, in: Land Forces Academy Review 1/2018, S. 16-24.

Andrzej Kozlowski: The European Union Effective System of Sanctions Against Cyberattacks, in: The Visio Journal 3/2018, S. 9-18.