Digitale Agenda und Cybersicherheit

Hans-Wilhelm Dünn/Lukas W. Schäfer

Ziel der europäischen Integration ist die Schaffung und Wahrung eines starken gemeinsamen Wirtschaftsraums sowie die Etablierung der Europäischen Union als außen- und sicherheitspolitisch gewichtigen Akteur der Weltpolitik, um transnationalen Herausforderungen geschlossen entgegentreten zu können. Mit der fortschreitenden digitalen Transformation von Politik, Wirtschaft, Wissenschaft und Gesellschaft sowie der anhaltenden globalen Vernetzung und der Expansion des Cyberraums ist die Digitale Agenda für Europa 2020 folgerichtig eine der gegenwärtig wichtigsten Facetten europäischer Integration. Dabei verfolgt die Europäische Union eine ‚Digitaltrias' mit Synergien und Interdependenzen zwischen Digitalem Binnenmarkt, digitaler Infrastruktur und Cybersicherheit als Teil der Sicherheitsunion. Während etwa eine flächendeckend verfügbare digitale Infrastruktur die Ausweitung des Digitalen Binnenmarktes ermöglicht, muss diese gleichzeitig geschützt werden. Diese Nachfrage an Cybersicherheit stärkt wiederum den Digitalen Binnenmarkt, zudem steigt mit sicheren digitalen Infrastrukturen das Vertrauen in neue Technologien, was Grundvoraussetzung einer erfolgreichen digitalen Transformation ist. Darauf aufbauend sollen die Wachstumspotenziale der Informations- und Kommunikationstechnologiebranche, einer der zentralen Umsatz- sowie Produktivitätstreiber, ausgenutzt werden.

Cybersicherheit

Die Anstrengungen für Cybersicherheit haben sich innerhalb der Europäischen Union spätestens seit dem großangelegten Cyberangriff auf das Mitgliedsland Estland 2007 verstärkt und manifestierten sich in der Cybersicherheitsstrategie 2013. Tatsächlich ist Cybersicherheit zentrales Integrationsmomentum der Sicherheitsunion und gilt als wichtiger Indikator in den dazugehörigen, monatlich erscheinenden Fortschrittsberichten der Europäischen Kommission. Die Relevanz der Thematik für elementare Säulen der Sicherheitsunion – vornehmlich „Bekämpfung des Terrorismus und der organisierten Kriminalität sowie der Instrumente zu ihrer Unterstützung" sowie „Stärkung der Abwehrbereitschaft und Widerstandsfähigkeit gegen diese Bedrohungen" – erschließt sich unter anderem aus der Grenzenlosigkeit des Cyberraums. Großangelegte Desinformationskampagnen zur Untergrabung des gesamteuropäischen demokratischen Meinungsbildungsprozesses verlangen etwa koordinierte Gegenmaßnahmen. An dieser Stelle sei beispielhaft der Dialog der europäischen Institutionen für ein einheitliches Konzept zur Bekämpfung von Desinformation genannt. Diesbezüglich erfolgte zuletzt im April 2018 eine Mitteilung der Europäischen Kommission an das Europäische Parlament, den Europäischen Rat, an den Europäischen Wirtschafts- und Sozialausschuss und an den Ausschuss der Regionen.[1]

1 Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, 26.4.2018, COM(2018) 236 final.

Weitere koordinierte Gegenmaßnahmen haben ihren Ursprung in einem dem Rat der Europäischen Union im Juni 2017 vorgelegten Entwurf von Schlussfolgerungen zur Schaffung eines „Rahmens für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten" (Cyber Diplomacy Toolbox). Nach Abstimmung mit den Mitgliedstaaten, der Europäischen Kommission und dem Europäischen Auswärtigen Dienst nahm der Rat der Europäischen Union die Schlussfolgerungen, beziehungsweise die „Toolbox" im April 2018 an.[2] Mithilfe der darin vorgesehenen Werkzeuge sollen einheitliche und unmittelbare diplomatische Reaktionen der Mitgliedstaaten auf Cyberangriffe ermöglicht, sowie langfristige normativ und somit befriedend wirkende Effekte auf potenzielle Täter etabliert werden. Insgesamt wurde auf die Benennung konkreter Handlungsrichtlinien verzichtet. Es wird lediglich attestiert, dass – falls nötig restriktive – Maßnahmen aus dem Reaktionsrahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP) angemessen erscheinen, allerdings stets in Relation zum Ausmaß des Cyberangriffes erfolgen müssen. Vielmehr wird die Notwendigkeit einer kohärenten, friedfertigen und auf Dialog ausgerichteten Cyberaußenpolitik zur Festigung internationaler Normen als Richtlinie für staatliches Handeln im Cyberraum unterstrichen. Interessanterweise fiel die Verabschiedung des diplomatischen Reaktionsrahmens in eine Zeit, in der die internationalen Bemühungen um diplomatische Verständigung im Cyberraum stagnierten. Die letzte Sitzung der sich mit ebendiesen Themen befassenden Expertengruppe der Vereinten Nationen,[3] deren Arbeit im Entwurfstext des diplomatischen Reaktionsrahmens noch als international maßgebend bezeichnet wurde, blieb aufgrund unüberwindbaren Dissens der teilnehmenden Parteien ohne Abschlussdokument, was die Bemühungen der vorangegangenen Sitzungen quasi zunichtemachte.[4] Die Europäische Union wurde mit dem Vorstoß also zu einem der gegenwärtig gefestigsten Projekten der internationalen Cyberdiplomatie.

Neben der Harmonisierung diplomatischer Reaktionen auf Cyberangriffe forcierte die Europäische Union eine Steigerung der Cyberabwehrfähigkeit. Am 13. September 2017 stellte die Europäische Kommission gemeinsam mit der Hohen Vertreterin der Europäischen Union für die Außen- und Sicherheitspolitik mit der gemeinsamen Mitteilung „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit der EU wirksam erhöhen"[5] dem Europäischen Parlament und dem Rat der Europäischen Union ein Cybersicherheitspaket vor.[6] Dieser „Rechtsakt zur Cybersicherheit" basierte auf der vorangegangenen Evaluation des Mandats der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) sowie der Cybersicherheitsstrategie 2013 und der Erörterung von Möglichkeiten eines einheitlichen europäischen Zertifizierungsverfahrens.

2 Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat und den Rat. Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Vierzehnter Fortschrittsbericht, 17.4.2018, COM(2018) 211 final.

3 Der volle Titel der Expertengruppe lautet „United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security".

4 Geneva Internet Platform Digital Watch Obervatory: UN GGE, abrufbar unter: https://dig.watch/processes/ungge (letzter Zugriff: 31.5.2018).

5 Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Gemeinsame Mitteilung an das Europäische Parlament und den Rat. Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, JOIN (2017) 450 final.

6 European Commission: Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, an on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 0477 final – 2017/0225 (COD).

Primär wird eine Stärkung der ENISA als zentrale europäische Cybersicherheitsagentur vorgesehen. Neben dem Erhalt eines ständigen Mandats und größeren Budgets, soll die Agentur das sich durch die europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) im Aufbau befindende Netzwerk der Computer Emergency Response Teams (CERTs) der Mitgliedstaaten koordinieren. Ferner soll sie die Umsetzung ebendieser Richtlinie unterstützen, europaweite Cyberübungen durchführen, eine Schlüsselfunktion bei der Etablierung eines europäischen Zertifizierungsverfahrens einnehmen und generell stärker operativ als beratend agieren.

Das europäische Zertifizierungsverfahren für Informations- und Kommunikationstechnik-Produkte, als weiterer zentraler Bestandteil des Pakets, ist vor allem eine Antwort auf das exponentiell wachsende Internet der Dinge und zielt gleichzeitig auf eine Harmonisierung der größtenteils fragmentierten Zertifizierungsverfahren der Mitgliedstaaten ab. Der Aufbau obliegt einer „European Cybersecurity Certification Group" unter Leitung der ENISA und soll sich aus den von den Mitgliedstaaten zu benennenden Zulassungsstellen zusammensetzen. Die Teilnahme beruht vorerst jedoch nur auf Freiwilligkeit. Die vorgesehenen Maßnahmen sowie die Ergebnisse einer anschließenden Folgenabschätzung wurden daraufhin zur Stellungnahme und Diskussion in den Haushaltsausschuss und die Ausschüsse für Industrie, Forschung und Energie, für Binnenmarkt und Verbraucherschutz und für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments eingereicht. Eine Stellungnahme in Form einer allgemeinen Ausrichtung seitens des Rates der Europäischen Union erfolgte Ende Mai 2018,[7] dessen finale Zustimmung neben der des Europäischen Parlaments für ein Inkrafttreten des Rechtsaktes noch aussteht.

Eine weitere Säule der Cyberabwehrfähigkeit der EU bildet ein kooperatives, europaweites Netzwerk aus CERTs. Während auf Basis einer institutionellen Vereinbarung im Dezember 2017 ein ständiges CERT für Einrichtungen der Europäischen Union im Falle von IT-Notfällen eingerichtet wurde,[8] verlangt die NIS-Richtlinie neben einheitlichen Cybersicherheitsniveaus in „wesentlichen Diensten" (kritische Infrastrukturen inklusive Anbieter digitaler Dienste) die Aufstellung nationaler CERTs in den Mitgliedstaaten.[9] Obwohl die Richtlinie bereits im Juni 2016 verabschiedet wurde und mit einer Umsetzungsfrist bis zum 10. Mai 2018 versehen wurde, mangelt es in einigen Mitgliedstaten noch an der vollständigen Implementierung.[10] Cybersicherheit ist jedoch nicht nur aufgrund des Verlangens nach sicheren digitalen Infrastrukturen erstrebenswert. Denn analog zu der Prämisse, dass die Grenzsicherheit der Europäischen Union die vier Grundfreiheiten des Binnenmarkts erst ermöglicht, ist Cybersicherheit Grundvorausset-

7 Rat der Europäischen Union: Mitteilung an die Presse. EU schafft einen gemeinsamen Rahmen für die Zertifizierung der Cybersicherheit und stärkt ihre Agentur – Rat legt seinen Standpunkt fest. Brüssel, 8.6.2018, Dok. 318/18.

8 Rat der Europäischen Union: Mitteilung an die Presse. Cybersicherheit: EU-Institutionen verstärken Zusammenarbeit gegen Cyberangriffe. Brüssel, 20.12.2017, Dok. 827/17.

9 Europäisches Parlament/Rat der Europäischen Union: Richtlinie 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 EU L194/1, 19. Juli 2016.

10 Casey Howard: 20 EU member states haven't implemented the NIS Directive, 22.5.2018, abrufbar unter https://www.itgovernance.eu/blog/en/20-eu-member-states-havent-implemented-the-nis-directive (letzter Zugriff: 4.6.2018).

zung für den freien Fluss von Daten, dem zentralen Rohstoff des Digitalen Binnenmarkts. Die stetig anwachsende Datenökonomie erfuhr zuletzt durch die Europäische Datenschutzgrundverordnung (DSGVO) eine Zäsur.

Stärkung der Datenökonomie

Die DSGVO trat am 24. Mai 2016 in Kraft, musste bis zum 25. Mai 2018 umgesetzt werden und steht für die Stärkung von Bürgerrechten, die Verpflichtung von Unternehmen zu hoher Datensicherheit aufgrund von Haftungspflichten und für faire Ausgangsbedingungen eines Digitalen Binnenmarkts. Denn im Gegensatz zu den bisherigen Verordnungen gilt die DSGVO unmittelbar, verdrängt somit nationales Recht und verhindert eine unterschiedliche Auslegung innerhalb der Mitgliedstaaten. Zusammen mit dem eingeführten Marktortsprinzip wird es für außereuropäische Unternehmen unmöglich, sich durch eine gezielte Standortwahl den strengen Auflagen zu entziehen. Das einheitliche Datenschutzniveau und die gegebene Rechtssicherheit beseitigen demnach datenschutzrechtliche Differenzen sowie Marktverzerrungen, die den freien Fluss von Daten und somit den Fortschritt des Digitalen Binnenmarktes behindern. Eine fristgerechte Umsetzung der Verordnung stellte vor allem für kleine und mittelständische Unternehmen eine finanzielle, personelle und rechtliche Herausforderung dar. Auch die teils fehlende Verständlichkeit und Eindeutigkeit der Bestimmungen ist ein Hauptkritikpunkt der Unternehmen und Verbände. Inwiefern sich die DSGVO als ein erhoffter Treiber des Digitalen Binnenmarktes herausstellt, wird demnach sicherlich erst innerhalb der nächsten Monate zu bewerten sein. Dennoch ist die Verordnung als Voraussetzung für Wettbewerbsgleichheit datenverarbeitender Unternehmen sowie als eine essentielle Stärkung von Datensouveränität und Transparenz anzuerkennen. Gleichermaßen wirkt die DSGVO im Bereich Daten- und somit Cybersicherheit. Einerseits haften Unternehmen für die sichere Verwahrung personenbezogener Daten und können im Falle unrechtmäßiger Entwendungen mit empfindlichen Bußgeldern von bis zu 20 Mio. Euro oder 5 Prozent des weltweiten Jahresumsatzes belegt werden. Angemessene IT-Sicherheitsvorkehrungen werden somit im Eigeninteresse der Unternehmen verankert. Andererseits kann die DSGVO im Verbund mit der wirtschaftlichen Macht der Europäischen Union als Verhandlungsbasis gegenüber zentralen Akteuren der digitalen Infrastruktur herangezogen werden. Die Europäische Kommission gestaltete etwa den Reformprozess des WHOIS-Identifikationsprotokolls der Zentralstelle für die Vergabe von Internet-Namen und -Adressen (ICANN) dahingehend mit, als dass DSGVO-Konformität, der Erhalt des öffentlichen Nutzens für Strafverfolgung im Cyberraum und die Verpflichtung zu einer weiteren Zusammenarbeit gewährleistet wurde.[11]

Ein einheitliches Regelwerk für Datenverarbeitungsprozesse erscheint des Weiteren angesichts der Bestrebungen der Europäischen Union um eine Vergrößerung des verfügbaren Datenvolumens angemessen: Im September 2017 wurde von der Europäischen Kommission ein Verordnungsentwurf zur Beseitigung von Hindernissen für den freien und einfachen grenzüberschreitenden Verkehr nicht-personenbezogener Daten vorgelegt.[12] Auf diesem Weg soll der Binnenmarkt für Datenspeicherungs- und Verarbeitungsdienste

11 Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat und den Rat. Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Fünfzehnter Fortschrittsbericht, 13.6.2018, Com(2018) 470 final.

12 Europäische Kommission: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union, 13.9.2017, COM(2017) 495 final, 2017/0228 (COD).

gestärkt sowie der Zugriff von Behörden der Mitgliedstaaten auf Datenbanken sichergestellt werden. Der Verordnungsvorschlag wurde an den Ausschuss für Binnenmarkt und Verbraucherschutz des Europäischen Parlaments weitergeleitet, der nach einigen Änderungsvorschlägen im Juni 2018 für die Aufnahme von Verhandlungen mit dem Rat der Europäischen Union stimmte.[13] Ein weiteres Unterfangen zur Stärkung eines fairen Datenökonomiesektors stellt die Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-Richtlinie) dar. Diese trat bereits 2003 in Kraft und wurde nach Aufruf der Europäischen Kommission von September bis Dezember 2017 in Form einer öffentlichen Konsultation geprüft. Die dabei ermittelten Umsetzungsschwierigkeiten wurden von der Europäischen Kommission angenommen und gemeinsam mit dem Rat der Europäischen Union über einen Legislativvorschlag zu einer Umgestaltung der PSI-Richtlinie am 25. April 2018 kommuniziert.[14] Vor dem Hintergrund eines zu erwartenden steigenden Marktpotenzials der Weiterverwendung von Informationen des öffentlichen Sektors – von 52 Mrd. Euro 2018 auf 194 Mrd. Euro 2030[15] – sollen vor allem Verbesserungen hinsichtlich des Geltungsbereiches der Richtlinie, der Verfügbarkeit von Echtzeitinformationen und des Marktzugangs insbesondere für kleine und mittelständische Unternehmen angestrengt werden.

Förderung digitaler Infrastruktur und Zukunftstechnologien

Um die kontinuierlich wachsende Masse an Daten effektiv und effizient verarbeiten zu können, bedarf es einer entsprechenden Infrastruktur. Hier wurde in erster Linie an einer weiteren Konkretisierung des Aktionsplans der Europäischen Kommission „5G für Europa“ gearbeitet, der etwa eine Anbindung von Schulen, kritischen Infrastrukturen und Digitalunternehmen an ein Gigabitnetzwerk bis 2025 vorsieht.[16] Nachdem der Rat für Verkehr, Telekommunikation und Energie im Juli 2017 mit der Unterzeichnung einer 5G-Absichtserklärung bekräftigte, Europa als Marktführer des „Next Generation Mobile Networks“, einem Mobilfunkverband von Mobilfunkanbietern, Herstellern und Forschungsinstituten, etablieren zu wollen, wurde im folgenden Dezember eine Roadmap mit präzisen Umsetzungsfristen für notwendige Harmonisierungen zur europaweiten Gigabit-Netzanbindung verabschiedet. Ein flächendeckendes, schnelles Internet soll zudem die bereits stattfindende Forschung an Zukunftstechnologien weiter fördern.

Im Januar 2018 stellte die Europäische Kommission ihre Strategie für das gemeinsame Vorhaben zum European High Performance Computing (EuroHPC) vor. Mit einer Investitionssumme von mehr als einer Milliarde Euro, getragen von den Mitgliedstaaten, dem Förderprogramm für Innovation und Forschung Horizon 2020 und dem Privatsektor, soll Europa im Bereich des High Performance Computing (HPC) Anschluss an die Weltspitze

13 European Parliament: No barriers to free flow of non-personal data in the EU, 4.6.2018, abrufbar unter: http://www.europarl.europa.eu/news/en/press-room/20180604IPR04926/no-barriers-to-free-flow-of-non-personal-data-in-the-eu (letzter Zugriff: 6.6.2018).

14 European Commission: Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (recast), 25.4.2018, COM(2018) 234 final, 2018/0111 (COD).

15 European Commission: Study to support the review of Directive 2003/98/EC on the re-use of public sector information, Deloitte, abrufbar unter: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51491 (letzter Zugriff: 5.6.2018).

16 European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 5G for Europe. An Action Plan, 14.9.2018, COM(2016) 588 final.

finden.[17] Tatsächlich wird dieser zukunftsweisenden Technologie strategische Relevanz für Forschung, Wirtschaft und nationaler Sicherheit zugemessen. Weitere Investitionen in dieser Größenordnung – ca. 1,5 Mrd. Euro bis 2020 – sind ferner für die Forschung am Einsatz Künstlicher Intelligenz vorgesehen.[18] Diese Technologie birgt großes Potential, wird aber auch sozioökonomische Folgen durch die Revolution von Arbeit, Mobilität oder Medizin mit sich bringen. Umso wichtiger ist daher eine enge Abstimmung der Mitgliedstaaten, wie die gemeinsame Erklärung von 25 Mitgliedstaaten im April 2018 ausdrückt.[19]

Digitale Agenda als Voraussetzung zukünftiger europäischer Politik

Im Gesamten betrachtet verzeichnet die Europäische Union Fortschritte zur Stärkung der eingangs beschriebenen Digitaltrias. Gleichzeitig bleibt die Digitale Agenda weiterhin im Fokus und verlangt nach Gestaltungswillen, Fortschritt und Anpassung. Wie so oft im Rahmen der europäischen Integration ist es dabei eine große Herausforderung einen gemeinsamen Nenner für eine effiziente und kohärente Digitalpolitik zu finden. Während eine Vertiefung des gemeinsamen Digitalen Binnenmarkts aufgrund des Wachstumspotenzials oder verbraucherfreundlicher Entwicklungen wie die Abschaffung unrechtmäßiger Zugriffsbeschränkungen auf digitale Angebote (Geoblocking) von der Wirtschaft und den BürgerInnen begrüßt wird, begegnen Cybersicherheitsinitiativen oftmals den traditionellen Vorbehalten der Mitgliedstaaten, Souveränität in Fragen der Außen- und Sicherheitspolitik abzutreten. Darüber hinaus muss an steigenden Investitionen und Kooperationen im Bereich der Forschung an zukunftsweisenden Technologien festgehalten werden. Andere Regionen der Welt haben hier einen Vorsprung erlangt, verfolgen dabei jedoch andere Ziele als das liberal-demokratische Europa. Ein resolutes Vorantreiben der Digitalen Agenda ist für die Europäische Union somit nicht nur aus wirtschaftlicher und sicherheitspolitischer, sondern auch hinsichtlich einer wertebasierten Außenpolitik anzustrengen.

Weiterführende Literatur

Annegret Bendiek/Raphael Bossong/Matthias Schulze: Die erneuerte Strategie der EU zur Cybersicherheit, in: SWP-Aktuell 72, Oktober 2017.

Helena Carrapico/André Barrinha: The EU as a Coherent (Cyber)Security Actor, in: Journal of Common Market Studies 6/2017, S. 1254-1272.

Myriam Dunn Cavelty: Europe's cyber power, in: European Politics and Society 3/2018, S. 304-320.

17 European Commission: Proposal for a Council Regulation on establishing the European High Performance Computing Joint Undertaking, COM(2018) 8 final, 2018/0003 (NLE).

18 European Commission: Press Release. Artificial intelligence: Commission outlines a European approach to boost investment and set ethical guidelines. Brussels, 25.4.2018, Dok. IP/18/3362.

19 Declaration Cooperation on Artificial Intelligence, abrufbar unter: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50951 (letzter Zugriff: 6.6.2018).