Digitale Agenda und Cybersicherheit

Hans-Wilhelm Dünn

Die Digitale Agenda der EU wird dieses Jahr zehn Jahre alt.[1] Seitdem sie im Jahre 2010 als einer der sieben Leitinitiativen der Europa 2020-Strategie ins Leben gerufen wurde, leitet sie die Integration von fairen, offenen und sicheren digitalen Räumen und etablierte stärkere Interdependenzen zwischen relevanten Themenfeldern in der Politik, wie zum Beispiel in der Außen- und Sicherheitspolitik, beim Ausbau von 5G oder der Gesundheitspolitik.[2] Das Thema Cybersicherheit gelangte immer mehr in den Vordergrund und die Idee eines digitalen Binnenmarkts, der auch das Thema Cybersicherheit umfasst und global wettbewerbsfähig ist, wurde integraler Teil der Agenda der europäischen Institutionen.[3] Die Jahre 2019 und 2020 waren schwierige Jahre für diese Initiative. Die bisher ungeregelten künftigen Beziehungen zwischen dem Vereinigten Königreich und der EU nach dem britischen Austritt aus der Staatengemeinschaft[4] und die anhaltende Covid-19-Pandemie haben die verschiedenen Säulen der EU grundlegend erschüttert. Nichtsdestotrotz gab es Weiterentwicklungen im Bereich der Cybersicherheit; Fortschritte wurden erzielt und Neuerungen zur allgemeinen Verbesserung der digitalen Sicherheit in Europa angestoßen.

Der Cybersecurity Act

Zwei Jahre nachdem der europäische Rechtsakt zur Cybersicherheit (EU) 2019/881 (auch Cybersecurity Act) erstmalig beim Europäischen Parlament, dem Rat der EU und der Europäischen Kommission vorgeschlagen wurde, ist er nun am 27. Juni 2019 in Kraft getreten und gilt seit dem 27. Juli 2019 für alle EU-Länder. Der Cybersecurity Act ist Teil eines Maßnahmenpakets, das zur Bekämpfung von Cyberangriffen dient und so eine stärkere Cybersicherheit mit sich bringen soll. Die Idee hinter dem Cybersecurity Act ist es, den digitalen Binnenmarkt zu fördern, eine robuste Verpflichtung im Bereich der Cybersicherheit für digitale Produkte, Dienstleistungen und Prozesse zu garantieren und einen langfristigen Fokus auf die Cybersicherheit im EU-Haushalt zu sichern. Mit dem Rechtsakt sind einige Änderungen auf die Agentur der Europäischen Union für Cybersicherheit (European Union Agency for Cybersecurity, ENISA) zugekommen, welche im Jahr 2019 ihr fünfzehnjähriges Bestehen feierte.[5] Er verleiht ihr ein permanentes Mandat, mehr Ressourcen und neue Aufgaben.[6] Zum einen hat die ENISA nun die Aufgabe, die Zusammenarbeit zu stärken, indem sie EU-Mitgliedern bei der Bekämpfung von Cybersicherheitsvorfällen hilft und grenzüberschreitende Cyberangriffe europaweit koordiniert.

1 Europäisches Parlament: Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates vom 11. März 2009, in: Amtsblatt der EU, Nr. L 87/164, 31.3.2009.
2 Europäisches Parlament: Digitale Agenda für Europa, 1.4.2020, abrufbar unter: https://www.europarl.europa.eu/factsheets/de/sheet/64/digital-agenda-for-europe (letzter Zugriff: 5.8.2020).
3 Vgl. hierzu auch den Beitrag „Binnenmarkt" in diesem Jahrbuch.
4 Vgl. hierzu auch den Beitrag „Brexit" in diesem Jahrbuch.
5 Vgl. hierzu auch den Beitrag „Europäische Agenturen" in diesem Jahrbuch.
6 Agentur der Europäischen Union für Cybersicherheit: ENISA – Sichert Europas Informationsgesellschaft, abrufbar unter: https://www.enisa.europa.eu/media/enisa-auf-deutsch/ (letzter Zugriff: 5.8.2020).

Außerdem soll die ENISA von nun an die Schlüsselrolle bei der Koordination und Einrichtung eines einheitlichen Zertifizierungsrahmens für Cybersicherheit im europäischen Binnenmarkt übernehmen. Damit sollen alle nationalen Zertifizierungsrahmen, die im Bereich der Cybersicherheit bestehen, ersetzt werden. Dies gewährleistet die Anwendung eines einzigen Zertifizierungsstandards für Produkte, Prozesse und Dienste im Bereich der Informations- und Kommunikationstechnik (IKT). Momentan gibt es in der EU keine einheitlichen Zertifizierungsstandards zur Cybersicherheit. Mitgliedstaaten selbst sind für die Zertifizierung und Klassifizierung von IKT-Produkten und IKT-Diensten zuständig, die festlegen, ob ein Produkt konform gemäß der Cybersicherheit ist oder nicht. In der Praxis bedeutet das einen Flickenteppich von Zertifizierungen und Zertifizierungsverfahren, da jedes EU-Land nationale Normen und Standardisierungen vorschreibt und IKT-Hersteller sich entsprechend verschiedenen Konformitätsbewertungen unterziehen müssen, um ihre Produkte auf den Markt zu bringen. Der Cybersecurity Act bedeutet für die Hersteller, dass sie zukünftig innerhalb der EU im Idealfall ihre Produkte und Dienstleistungen nur den EU-Cybersicherheitsstandards entsprechend zertifizieren lassen müssen, um damit ihre Konformität von allen Ländern der Union anerkannt zu bekommen. Vorerst wird die Zertifizierung der Cybersicherheit aber freiwillig sein.[7]

Um die einheitlichen Zertifizierungsstandards in die Wege zu leiten, bei strategischen Fragen der Cybersicherheitszertifizierung zu beraten und die Kommission bei der Vorbereitung des fortlaufenden Arbeitsprogramms zu unterstützen, hat die Europäische Kommission die „Stakeholder Cybersecurity Certification Group" (SCCG) und die „European Cybersecurity Certification Group" (ECCG) ins Leben gerufen.[8] Die ECCG setzt sich aus nationalen Zertifizierungsaufsichtsbehörden oder Vertretern anderer relevanter nationaler Behörden zusammen. Sie sind mit der Verwaltung der Zertifizierungsausgabe, der Konformität und der damit verbundenen Strafen bei Nichteinhaltung beauftragt. Demgegenüber wird die SCCG sich aus 50 Mitgliedern, die aus verschiedensten Industrien kommen, zusammensetzen. Sowohl die Nachfrageseite und als auch die Angebotsseite von IKT-Produkten und IKT-Dienstleistungen sind vertreten.[9] Während die ECCG sich bis Stand Juni 2020 drei Mal getroffen hat, stehen bei der SCCG bisher weder Mitglieder noch eine konkrete Agenda fest.[10]

Die digitale Wettbewerbsfähigkeit, 5G und Cybersicherheit

Der anstehende Ausbau der Kommunikationsnetze auf den neuesten Stand der sogenannten 5G-Technik wurde angesichts der damit einhergehenden sicherheitspolitischen internationalen Diskussionen und Debatten auch auf der EU-Ebene zu einem maßgeblichen Thema und gelangte von diesen angestoßen zu einer der Top-Prioritäten im Bereich der digitalen Agenda. Während die Technologie und Standards der 5G-Netze viele Vorteile mit sich bringen, gibt es wie bei allen IKT-Technologien immer auch gewisse Risiken für die Cybersicherheit. Die Cybersicherheit der 5G-Netze ist daher ein wesentlicher Bestand-

7 Rat der EU: EU erhöht die Cybersicherheit: Rat billigt Einigung über die gemeinsame Zertifizierung und die Stärkung der Agentur, 19.12.2018, Pressemitteilung.

8 Europäische Kommission: The EU cybersecurity certification framework, 24.6.2020, abrufbar unter: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (letzter Zugriff: 5.8.2020).

9 Europäische Kommission: Call for applications for the selection of members of the stakeholders cybersecurity certification group, 28.8.2019, abrufbar unter: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=61037 (letzter Zugriff: 5.8.2020).

10 Europäische Kommission: The EU cybersecurity certification framework, 2020.

teil für den Schutz des europäischen Marktes und der strategischen Autonomie der EU. Das 5G-Netz soll eine wesentliche digitale Infrastruktur in der EU bilden, die auch „Kritische Infrastrukturen“ (KRITIS), wie beispielsweise Krankenhäuser[11], miteinander verbindet, Internetverbindungen schneller macht und Anwendungen der Künstlichen Intelligenz (KI) und des „Internet of Things“ (IoT) ermöglicht. Es verwundert daher nicht, dass seit der Verabschiedung der Empfehlung zur Cybersicherheit der 5G-Netze im März 2019 weitere Mitteilungen und Papiere der Europäischen Kommission herauskamen. Diese beinhalten eine Reihe von operativen Schritten und Maßnahmen, um ein hohes Maß an Cybersicherheit von 5G-Netzen in der gesamten EU zu gewährleisten. Bei diesen Debatten stand insbesondere die Frage im Vordergrund, welche Hersteller am Ende das grüne Licht für den Ausbau des 5G-Netzs bekommen sollten. Getrieben war die Debatte von der Sorge, dass über die technischen Ausrüster der 5G-Netze möglicherweise Eingriffe in die Cybersicherheit der EU-Länder erfolgen könnten und entsprechender Schaden angerichtet werden könnte. Um keinen Hersteller grundsätzlich zu diskriminieren, hat sich die Europäische Kommission aber klar gegen einen teilweise geforderten europaweiten Ausschluss einzelner Hersteller entschieden. Stattdessen hat die Europäische Kommission am Anfang des Jahres 2020 einen „Werkzeugkasten“ für die Sicherheit von 5G-Netzen veröffentlicht, in dem Maßnahmen zur Abschwächung von Cybersicherheitsrisiken von 5G-Netzen auf nationaler und auf der europäischen Ebene vorgestellt wurden.[12] Der Werkzeugkasten stellt damit eine Anleitung für Infrastrukturbetreiber und EU-Länder dar, um selbst zu entscheiden, welche Firmen sie in ihrem 5G-Netz-Ausbau einbinden. Der Werkzeugkasten macht damit keinen konkreten Vorschlag zu den einzelnen Herstellern, gibt aber Empfehlungen zur Kontrolle von ausländischen Investitionen im 5G-Bereich und zur Diversifizierung von verschiedenen 5G-Anbietern. Das Ergebnis ist das Resultat eines monatelangen Austauschs der EU-Länder und folgte der Veröffentlichung der ENISA am 9. Oktober 2019 zur aktuellen Bedrohungslandschaft für 5G-Netzwerke.[13]

Cybersicherheit im Kontext der Covid-19-Pandemie

Die Covid-19-Pandemie hat einen weltweiten Ausnahmezustand hervorgerufen, der auch im Cyberraum deutlich zu spüren ist. Laut Europol hat sich die Anzahl an Cyberangriffen gegen Organisationen und Einzelpersonen während der Pandemie drastisch erhöht.[14] Cyberkriminelle nutzen die Unruhe und Unsicherheit der Menschen, um verschiedene Schadsoftware durch Social Engineering-Angriffe im Zusammenhang mit der Pandemie zu verbreiten. Hinzu kommt, dass viele Mitarbeitende europaweit im Home Office sind und sich so das Risiko für Angriffe beispielsweise über unsichere Privatgeräte erhöht. Um insbesondere im letzten Bereich kurzfristig Abhilfe zu schaffen, boten verschiedene europäische Institutionen, aber auch von der EU unterstützte privatwirtschaftliche Initiativen Unterstützungsangebote an. Beispielsweise hat das „European network of cybersecurity centres and competence Hub for innovation and Operations“ (auch ECHO-Netzwerk) eine

11 Vgl. hierzu auch den Beitrag „Gesundheits- und Verbraucherpolitik“ in diesem Jahrbuch.

12 Europäische Kommission: Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures, Januar 2020, abrufbar unter: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468 (letzter Zugriff: 5.8.2020).

13 Europäische Kommission: EU coordinated risk assessment of the cybersecurity of 5G networks, 9.10.2019, abrufbar unter: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132 (letzter Zugriff: 5.8.2020).

14 Europol: Press Release, How criminals profit from the covid-19 pandemic, 27.3.2020; vgl. hierzu auch den Beitrag „Polizeiliche und justizielle Zusammenarbeit“ in diesem Jahrbuch.

Covid-19-Cyberabwehr-Allianz etabliert, die das Ziel verfolgt, Initiativen zu unterstützen, die EU-Mitgliedstaaten, wichtige Dienste und KRITIS vor Cyberangriffen schützen.[15] Ergänzend hat Europol eine Übersicht erstellt, wie Hacker von der aktuellen Covid-19-Pandemie profitieren[16] und die ENISA hat Tipps für die Cybersicherheit im Home Office zusammengestellt.[17]

Auch finanziell hat die Covid-19-Pandemie Europa vor eine harte Probe gestellt. Es wird geschätzt, dass die Wirtschaft in der EU im Jahr 2020 um 7,4 Prozent schrumpfen wird.[18] Um diese finanziellen Schäden am Binnenmarkt zu beheben beziehungsweise zu minimieren und um gleichzeitig für Wohlstand zu sorgen, hat die Europäische Kommission ein 750 Mrd. Euro schweres Aufbauinstrument unter dem Namen „Next Generation EU" vorgeschlagen.[19] Die Ausschüttung soll bis zum Jahre 2027 geschehen und auf drei Säulen verteilt werden. Eines der Hauptthemen ist dabei die „Unterstützung von Schlüsselbranchen und -technologien".[20] Mit dem Ziel, die europaweite Cybersicherheitsstrategie und den digitalen Binnenmarkt zu stärken, sollen beispielsweise:

1. Investitionen in Konnektivität fließen, um insbesondere den Ausbau des 5G-Netzes zu fördern;
2. eine stärkere industrielle und technologische Präsenz in strategisch wichtigen Sektoren, wie zum Beispiel der KI, Cloud- und Cybersicherheit geschaffen werden;
3. durch eine verstärkte Datenwirtschaft Motoren für Innovation geschaffen werden;
4. neue Ideen und Entwicklungen zur Erhöhung der Cyberresilienz gefördert werden.

Die Strategie wird auch kleine und mittelständige Unternehmen (KMUs) in diesen Bereichen fördern. Diese zusätzlichen Mittel passen zu den bereits bestehenden politischen Prioritäten der Europäischen Kommission für 2019–2024.[21] Denn schon vor der Pandemie hatte sich Ursula von der Leyen als Präsidentin der Europäischen Kommission[22] mit ihrer Agenda für Europa für den technologiegetriebenen Wandel eingesetzt, um Europa als „digitale Macht" zu positionieren.[23] Seit Beginn ihrer Präsidentschaft machte sich von der Leyen für das Voranschreiten einer ganzheitlichen Digitalisierung der Euro-

15 ECHO-Netzwerk: The COVID-19 Hackers Mind-set. ECHO White Paper #1, 8.4.2020, abrufbar unter: https://echonetwork.eu/wp-content/uploads/2020/04/20200408-ECHO-WhitePaper-Hackers-Mindset-FINAL.pdf (letzter Zugriff: 11.6.2020).

16 Europol: Press Release, How criminals profit from the covid-19 pandemic, 2020.

17 ENISA: Press Release, Tips for cybersecurity when working from home, 24.3.2020, abrufbar unter: https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home (letzter Zugriff: 5.8.2020).

18 Statista: Real gross domestic product growth rate forecasts in selected European countries from 2020 to 2021, Mai 2020, abrufbar unter: https://www.statista.com/statistics/1102546/coronavirus-european-gdp-growth/ (letzter Zugriff: 5.8.2020); vgl. hierzu auch den Beitrag „Wirtschaftspolitik" in diesem Jahrbuch.

19 Europäische Kommission: Der EU-Haushalt als Triebfeder für den Europäischen Aufbauplan, 27.5.2020, abrufbar unter: https://ec.europa.eu/info/sites/info/files/factsheet_1_de_v2.pdf (letzter Zugriff: 5.8.2020); vgl. hierzu auch den Beitrag „Haushaltspolitik" in diesem Jahrbuch.

20 Europäische Kommission: Pressemitteilung: Die Stunde Europas: Schäden beheben und Perspektiven für die nächste Generation eröffnen, 27.5.2020, IP/20/940.

21 Vgl. hierzu auch den Beitrag „Europäische Kommission" in diesem Jahrbuch.

22 Europäische Kommission: Ankündigung, Gestaltung der digitalen Zukunft Europas: Gastbeitrag von Ursula von der Leyen, Präsidentin der Europäischen Kommission, 19.2.2020, Brüssel, AC/20/260.

23 Ursula von der Leyen: Eine Union, die mehr erreichen will. Meine Agenda für Europa, 29.1.2020, abrufbar unter: https://ec.europa.eu/info/sites/info/files/political-guidelines-next-commission_de.pdf (letzter Zugriff: 5.8.2020).

päischen Kommission stark.[24] Dabei schlug sie neue Gesetze zu Haftungs- und Sicherheitsvorschriften für digitale Plattformen, Dienste und Produkte sowie zur Beschleunigung des Informationsaustauschs vor. Top-Priorität war seitdem die Vollendung des digitalen Binnenmarkts. Neue Vorschriften für die Cybersicherheit von KRITIS und Diensten wurden diskutiert und im Rahmen der Planungen der Konferenz zur Zukunft Europas zur Sprache gebracht.[25]

Blick in die nahe Zukunft

Auch wenn die Covid-19-Pandemie sich im Sommer 2020 in Europa zunächst abzuschwächen scheint, so sind deren Ausgang und die Folgen im Rahmen der EU und die entsprechenden genauen Auswirkungen auf die Digitale Agenda und die Cybersicherheit bisher schwierig abschätzbar. Viele Cyberkriminelle haben die Situation genutzt und eine erhöhte Anzahl von Cyberangriffen in ganz Europa gestartet.[27] Für Unternehmen und Bürger hat sich so die Gefahr, Opfer eines Cyber-Angriffs zu werden, erhöht. Positiv ist hier aber anzumerken, dass viele europäische Unternehmen, insbesondere die KMUs, welche besonders von Cyberangriffen betroffen sind, durch diese besondere Situation viel dazu lernen. Es wird mehr Interesse und Aufmerksamkeit auf das Thema Cybersicherheit gelegt und immer stärker als Triebfeder in der digitalen Transformation wahrgenommen.[28] Sollte dieses Interesse nachhaltig sein und dauerhaft in bessere Schutzmaßnahmen münden, könnte die Covid-19-Pandemie sogar als Katalysator einer höheren allgemeinen Cybersicherheit wirken.

Zudem wird es spannend sein zu beobachten, wie sich das Konjunkturpaket von „Next Generation EU“ im Detail auf die weitere Praxis der Cybersicherheit und der entsprechenden Technologien in Europa auswirkt. Ein weiterer Prozess, der abhängig vom Ausgang Folgen für den Bereich der Cybersicherheit der EU und auch für die damit einhergehenden Themen Datensicherheit und Datenschutz haben wird, ist der britische Austritt aus der EU. Angesichts der geringen Übergangszeit bis zum Austritt Ende des Jahres 2020 wird es interessant sein zu sehen, welche rechtlichen Grundlagen, Regulierungen und Zertifizierungen zwischen der EU und dem Vereinigten Königreich im Cyberraum festgelegt werden. Wichtig wird es sein, dass weiterhin ein guter Austausch mit dem Vereinigten Königreich im Bereich der Cybersicherheit etabliert wird. Denn auch hier wird wieder die generelle Tatsache Anwendung finden, dass im Bereich der Cybersicherheit angesichts begrenzter Ressourcen und einer sich stetig zuspitzenden Bedrohungslage nur durch eine vermehrte Kooperation aller Staaten und Institutionen eine Verbesserung der Lage erreicht werden kann. Die EU hat auch im vergangenen Jahr wieder einige wichtige Schritte in diesem Bereich unternommen und Entwicklungen angestoßen. Es bleibt spannend und wichtig, diese weiterzuverfolgen und je nach Bedarf weiter zu ergänzen.

24 Von der Leyen: Eine Union, die mehr erreichen will, 2020.

25 Europäische Kommission: Pressemitteilung: Eine Union, die mehr erreichen will: die ersten 100 Tage, 6.3.2020, Brüssel, IP/20/403; Europäische Kommission – Vertretung in Deutschland: EU-Nachrichten #02 2020, 30.1.2020, abrufbar unter: https://ec.europa.eu/germany/sites/germany/files/docs/eu_nachrichten_02_2020web.pdf (letzter Zugriff: 5.8.2020).

27 Europol: Press Release, How criminals profit from the covid-19 pandemic, 2020.

28 Europäischer Wirtschafts- und Sozialausschuss: „European companies (especially SMEs) face growing risk of cyber attacks – study“, 4.6.2018, abrufbar unter: https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study (letzter Zugriff: 5.8.2020).

Weiterführende Literatur

Jens Baas (Hrsg.): Digitale Gesundheit in Europa. Menschlich, vernetzt, nachhaltig, Berlin 2020.
Hans-Wilhelm Dünn et al. (Hrsg.): Cybersicherheit im Krankenhaus, Berlin 2020.