Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale
Politik und Sicherheit

DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

DSI Industrial & Policy Recommendations (IPR) Series

Europas dritter Weg im Cyberraum

Der Beitrag der neuen Cybersicherheitsverordnung

Annegret Bendiek (Stiftung Wissenschaft und Politik, Forschungsgruppe EU) und Martin Schallbruch (Digital Society Institute, ESMT Berlin)

Issue 1, 2019

Cybersicherheit ist für Europa zu einer Schlüsselfrage der globalen digitalen Transformation geworden. Mit dem Cybersecurity Act, also der Cybersicherheitsverordnung, hat die EU einen rechtlichen Rahmen mit dem Anspruch globaler Ausstrahlung vorgelegt. Eingebettet in eine Politik, die digitale Souveränität mit strategischer Verflechtung kombiniert, kann die Verordnung das Tor zu einem dritten Weg Europas im Cyberraum sein, der zwischen dem US-amerikanischen Modell der Marktfreiheit und dem chinesischen Modell des autoritären Staatskapitalismus verläuft. Der Cybersecurity Act wird verbindlicher Handlungsrahmen und Rückenwind für die bundesdeutsche Cybersicherheitspolitik sein.

Open Cyberbedrohungen sind ein Bestandteil und zugleich die Speerspitze des globalen Wettbewerbs zwischen liberalen Demokratien und autoritären Systemen. Das unterschiedliche Verständnis von Cyber- bzw. Informationssicherheit zwischen westlichen Ländern einerseits und Staaten wie China und Russland andererseits ist ein zentraler Konflikt in der internationalen Politik. Eine Übereinkunft über globale Normen und Regulierungen ist nach über 10 Jahren erfolgloser Verhandlungen vor dem Hintergrund einer wachsenden Rivalität zwischen den USA und China in weite Ferne gerückt. Die EU versucht, jenseits dieser Rivalität einen dritten Weg zu finden. Dies wird unter anderem in der 5G-Debatte deutlich. Die Kommission ist geneigt zuzulassen, dass das chinesische Unternehmen Huawei am Aufbau der europäischen Infrastrukturen beteiligt wird, unter der Voraussetzung einer engen Kontrolle und nur, wenn alle Marktteilnehmer strenge Zertifizierungskriterien für Hard- und Software erfüllen. Die Frage der Vertrauenswürdigkeit chinesischer Telekommunikationskomponenten wird zugunsten einer Marktregulierungslösung zurückgestellt. Bereits mit der Datenschutz-Grundverordnung (DSGVO), die die Mitgliedstaaten seit Mai 2018 anwenden müssen, und mit ihrem konsequenten Auftreten in der Wettbewerbspolitik hat die EU eine effektive und weltweit beachtete Rolle als Regulierungsmacht eingenommen und dabei einen Ausgleich hergestellt zwischen dem Schutz der Konsumenten und der Wettbewerbsfähigkeit der Industrie. Mit dem EU Cybersecurity Act, der Cybersicherheitsverordnung, wird diese europäische Regulierungsmacht noch gestärkt. Die mit dem Inkrafttreten der Verordnung im Juni 2019 definierte europäische Cybersicherheitszertifizierung wird aber nur dann Modellcharakter auf globaler Ebene entfalten können, wenn sie durch eine europäische Strategie für den digitalen Raum flankiert wird. Regulierung, Wettbewerbs- und Industriepolitik sowie Innovationsförderung müssen in Beziehung gesetzt werden zu Sicherheits- und Cyber-Außenpolitik. Die wesentliche Frage wird sein, ob und wie es der EU gelingt, einerseits die europäische digitale Souveränität zu stärken, die unsere liberalen demokratischen Traditionen im digitalen Raum bewahrt, und andererseits eine nötige strategische Verflechtung mit anderen Weltregionen zu gewährleisten.

Cybersicherheit im Brennpunkt globaler Konflikte

Die aktuellen Konflikte zwischen den USA, China und der EU gehen in ihrer Relevanz weit über handels- und

investitionspolitische Fragen hinaus. Sie sind deshalb so brisant, weil digitale Technologien die kommunikative Infrastruktur hochentwickelter Informationsgesellschaften bilden. Wer die Kontrolle über Hard- und Software hat, der bestimmt auch darüber, welche Innovationen und Geschäftsmodelle möglich sind und wer auf welche Informationen Zugriff hat. Zu beobachten ist eine immer engere Kooperation zwischen privaten Technologiekonzernen und Institutionen, die hoheitliche Aufgaben wahrnehmen, zum Beispiel beim Schutz Kritischer Infrastrukturen. Diese Tendenz lässt sich in der EU und in den USA feststellen, weit stärker aber in China und Russland, deren Führungen Cybersicherheit in noch viel höherem Maße als Eckpfeiler ihres staatlichen Kontrollanspruchs im Cyberraum ansehen. Konzerne, die in China und Russland an der Ausweitung der gesellschaftlichen Überwachung arbeiten oder die in den USA mit der NSA kooperieren, behandelt die EU nicht mehr nur als unpolitische, rein marktwirtschaftliche Akteure.

Wertekonflikt

Die Hoffnung, dass das Internet Freiheit und Menschenrechte überall befördert, ist spätestens seit den Enthüllungen Edward Snowdens und der Nutzung digitaler Technologien für staatliche Überwachung nur noch bedingt realistisch. Es ist evident, dass das Internet heute ein Raum ist, in dem Verteilungs- und Wertekonflikte ausgetragen und die zukünftigen Modalitäten der individuellen und gesellschaftlichen Selbstbestimmung ausgehandelt werden. Die Technologie des Netzes und die dazugehörigen Anwendungen sind keine wertneutralen Instrumente, sondern sie normieren Entscheidungen und Handlungsweisen. Sie sind Instrumente wertebezogener Politik, wie der Streit um den chinesischen Technologiekonzern Huawei zeigt. In der US-Administration wird Huawei nicht nur als Marktteilnehmer, sondern zugleich als trojanisches Pferd einer nicht wohlgesonnenen Regierung wahrgenommen. Peking verwahrt sich gegen diese Vorwürfe und betrachtet den Ausschluss des Konzerns vom US-Markt als eine Maßnahme, die gegen Chinas Position auf dem Weltmarkt insgesamt gerichtet ist.

Der Konflikt um Huawei markiert einen Bruch mit der rein marktwirtschaftlichen Logik globaler Handelsbeziehungen und befördert einen wachsenden digitalen Merkantilismus. Viele sehen in dem Zusammenwachsen der Märkte heute nicht mehr nur eine Chance für Wohlstandsverbesserung, sondern eine Gefahr für Selbstbestimmung und öffentliche Sicherheit. Sie argumentieren, dass die digitalen Produkte geeignet seien, Werteordnungen auszuhöhlen und die staatliche Gestaltungs- und Steuerungskompetenz durch technische Hintertüren zu unterlaufen. Begriffe wie »technologische Souveränität« und »ökonomische Verwundbarkeit« sind ein Indikator für die wachsende Bereitschaft, Innovation und Wettbewerb in Bezug auf digitale Produkte und Dienste einzuschränken. Die neue Konflikthaftigkeit in der digitalen Welt ist allerdings nicht auf das Verhältnis zwischen dem Westen und China beschränkt. Auch in den transatlantischen Beziehungen prallen heute Wertvorstellungen aufeinander, die schwer miteinander vereinbar sind. Die vielbeschworene transatlantische Wertegemeinschaft stößt dort an ihre Grenzen, wo die Idee des freien (digitalen) Binnenmarkts mit dem Gebot des Schutzes persönlicher Daten und der informationellen Selbstbestimmung und mit dem europäischen Wettbewerbsrecht kollidiert. Die von der Politik lange ignorierte Dominanz der US-Internetkonzerne zwingt Europa zu einem Kurs der digitalen Selbstbehauptung – vom Datenschutz über das Wettbewerbsrecht bis zur Besteuerung.

Cybersicherheitskonflikt

Cyberangriffe und ihre Abwehr sind eine gravierende Herausforderung für die internationale Kooperation. Während die Komplexität und die Interdependenz von digitalen Systemen schnell zunehmen, bleibt die Qualität der hierfür verwendeten Hardware und Software mangelhaft und fehlen die nötigen personellen Kapazitäten zu deren Absicherung. Permanent entstehen im Cyberraum neue Angriffsvektoren und -ziele. Die kriminelle Nutzung von Schwachstellen, zum Beispiel der Einsatz von Ransomware zur Erpressung von Unternehmen, und staatliche Cyberattacken, die der Aufklärung oder Destabilisierung dienen sollen oder Teil der hybriden Kriegsführung sind, verstärken sich gegenseitig negativ. Extremstes Beispiel ist Nordkorea, das mit globalen Cyberoperationen Einnahmen zur Beschaffung von Raketentechnologie generiert. Zwar hat eine Gruppe von Regierungsexperten auf VN-Ebene (GGE) in fünf Verhandlungsrunden über die internationale Ächtung bzw. Beschränkung von Cyberangriffen und über die Einrichtung einer völkerrechtlich verankerten Organisation zur Cyberabwehr debattiert – aber erfolglos. Auch von der aktuellen sechsten Runde der GGE sind kurzfristig keine Fortschritte zu erwarten, genauso wenig wie von den Verhandlungen, die parallel auf Initiative Russlands in einer Open Ended Working Group (OEWG) geführt werden.

Handelskonflikt

Der Handelskonflikt zwischen den USA und China speist sich wesentlich aus der Entwicklung der Märkte hin zu einer stärkeren Bedeutung digitaler Produkte und Dienste. Die digitale Transformation der globalen Märkte geht nicht nur mit einer wachsenden ökonomischen Interdependenz einher, sie hat gleichzeitig auch

die Steuerungsfähigkeit der Staaten zunehmend reduziert. Wenn US-Präsident Trump Handelsbeschränkungen anordnet, so ist dies auch Ausdruck eines Versuchs, die Kontrolle über die Auswirkungen eines von Innovationen befeuerten weltweiten Wettbewerbs auf die USA zurückzugewinnen. Gleichzeitig sind die Produkte und Dienste der amerikanischen Tech-Unternehmen für Washington ein wesentliches Instrument der staatlichen Kontrolle und der internationalen Einflussnahme. Die Diskussion über die Produkte von Huawei hat aber einen Aspekt, der weit darüber hinausweist: Komplexe digitale Systeme wie die Netzwerktechnik für 5G könnten sich als kaum kontrollierbare Technologie erweisen, die für Jahrzehnte in den Infrastrukturen eines Staates verbaut ist und letztlich der Steuerung eines autoritären Staates unterliegt. Netzwerkprodukte entwickeln sich derzeit zu einer im Wesentlichen auf Software gestützten Technologie weiter. Die dafür erforderlichen regelmäßigen Updates bringen für den einsetzenden Betreiber kaum nachvollziehbare Neuerungen in der Funktionalität mit sich. Gleichzeitig verändert die digitale Transformation alle Marktsegmente, von landwirtschaftlichen Produkten über die Medizintechnik bis zum Maschinenbau. Handelsfragen werden immer stärker verschränkt mit dem Ringen um digitale Kontrollfähigkeit.

Die EU als Regulierungsmacht

Um sich in dieser konfliktträchtigen Welt ohne Grenzen behaupten zu können, greift die EU zum Mittel der Regulierung. Europa steht hierbei für einen sehr spezifischen Weg, der sich grundlegend sowohl vom libertären Modell des Silicon Valley als auch dem autoritären chinesischen Modell unterscheidet. Der europäische Regulierungsansatz basiert auf den europäischen Verträgen. Er geht von der Prämisse aus, dass die Freiheit des Einzelnen und seine Verantwortung gegenüber der Gesellschaft (Art. 2 EUV) gleichrangige Güter sind. Im Einklang mit dem Gebot eines rechtsstaatlich-demokratischen Verfahrens wird der Marktteilnehmer als Regulierungsadressat bei der Formulierung von Rechtsakten und bei deren Umsetzung im Rahmen der EU-Komitologie eingebunden.

In Artikel 3 und 10 EUV betont die EU mit dem Bekenntnis zu den Marktfreiheiten und zur Demokratie die individuelle Selbstbestimmungsfähigkeit der Bürger Europas. Sie bindet verschiedene Stakeholder bzw. Marktteilnehmer in die EU-Verfahren ein, die beispielsweise zu grundlegenden ethischen Fragen Position beziehen. Der Europarat, der Europäische Rat, das Europäische Parlament und die Kommission haben in den letzten Jahren eine Reihe von Grundsätzen formuliert, in denen sich die Idee einer gleichzeitig gesellschafts- und individualzentrierten digitalen Gesellschaft widerspiegelt. Neue Technologien müssen sich demnach auch daran messen lassen, ob sie der Demokratie förderlich sind und mit ihrem Einsatz die Menschenrechte gewahrt werden. Regulierungsmaßnahmen können hier den entscheidenden Beitrag leisten, um einen Ausgleich zu schaffen zwischen Chancen und Risiken einer Technologie, zwischen den Interessen von Unternehmen, Verbrauchern, Staat und Zivilgesellschaft. Ein eindrückliches Beispiel für diesen regulativen Zugriff sind die Leitlinien der EU in Sachen Künstliche Intelligenz (KI). KI wird darin nicht als Selbstzweck verstanden, sondern als »a tool operating in the service of humanity and the public good«. Der im April 2019 erschienene Abschlussbericht einer von der Kommission eingesetzten Expertengruppe betont die Notwendigkeit, im Rahmen des Einsatzes von KI menschliche Autonomie zu wahren, Schäden für Menschen zu vermeiden und allgemein den Prinzipien von Fairness und Verstehbarkeit Rechnung zu tragen. Trotz des grundlegenden europäischen Konsenses in dem Punkt, dass Marktfreiheit, Datenschutz und Sicherheit in einer engen Verbindung zueinander stehen und regulatorisch ausgeglichen werden müssen, gibt es allerdings noch kaum Einigkeit darüber, wie nationale Standards im Sicherheitsbereich mit der liberalen Marktlogik in Einklang gebracht werden können. Sehr deutlich wird dies beim Umgang mit dem chinesischen Konzern Huawei.

Datenschutz und Datensicherheit als EU-Interesse

Der spezifisch europäische Zugriff beim Thema Digitalisierung kommt gerade in den Rechtsakten der EU zum Datenschutz und zur Datensicherheit zum Ausdruck. Die Datenschutz-Grundverordnung, die seit Mai 2018 bereits von allen Unternehmen anzuwenden ist, setzte neue Maßstäbe bei der Aufgabe, eine Balance zwischen dem Schutz personenbezogener Daten und der Gestaltung eines freien Datenverkehrs im Binnenmarkt zu finden. Datenschutz und Cybersicherheit wurden bislang getrennt betrachtet. Tatsächlich wachsen beide Materien zunehmend zusammen. Dies zeigt sich beispielsweise bei den digitalen Stromzählern (SmartMeter). An deren Betrieb müssen nicht nur hohe Sicherheits-, sondern auch höchste Datenschutzanforderungen gestellt werden, damit die Nutzer nicht in ihren häuslichen Gewohnheiten ausgeforscht werden können. Indem sie ein umfassendes System der Definition und Zertifizierung technischer Cybersicherheit etabliert, unternimmt die EU einen großen Schritt, um ihre Rolle als Regulierungsmacht, die sie mit der DSGVO erfolgreich ausgefüllt

hat, in der Ausgestaltung des digitalen Raums weiter zu festigen.

Cybersicherheitsverordnung

Am 10. Dezember 2018 haben sich das Europäische Parlament, der Europäische Rat und die Europäische Kommission politisch über einen Rechtsakt zur Cybersicherheit geeinigt. Die Verordnung über die EU-Cybersicherheitsagentur (ENISA) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (»Rechtsakt zur Cybersicherheit«) wurde im Juni 2019 verkündet. Der Rechtsakt beinhaltet zwei wesentliche Reformen: Die EU-Cybersicherheitsagentur (Agentur der Europäischen Union für Netz- und Informationssicherheit, ENISA) erhält ein über das Jahr 2020 hinaus geltendes Mandat, um die Mitgliedstaaten im Umgang mit Cyberangriffen unterstützen zu können. Es wird eine Cybersicherheitszertifizierung von Produkten, Verfahren und Diensten eingeführt (europäischer Zertifizierungsrahmen). Zertifizierung basiert auf der Idee, dass sich mit Standards und Normen ein Ausgleich schaffen lässt zwischen dem Gebot des Konsumentenschutzes und dem legitimen Anspruch der Industrie auf Wettbewerbsfähigkeit. Beides sind hohe Prinzipien, die miteinander vereinbart werden müssen. Konsumentenschutz bedeutet, dass Verbraucher vor negativen Konsequenzen wie einer nichtautorisierten Weitergabe und Verwendung ihrer Daten bewahrt und ihnen generell verlässliche und qualitativ hochwertige Produkte zur Verfügung gestellt werden müssen. Diese Ziele können unter Umständen allerdings mit Fragen der Konkurrenzfähigkeit von Produktanbietern konfligieren. Zum Beispiel betrachten Unternehmen hohe Standards im Datenschutz und in der Datensicherheit häufig als Hürde im Wettbewerb.

Die Cybersicherheitsverordnung sieht eine sogenannte freiwillige »Konformitätsbewertung« für Produkte der Informations- und Kommunikationstechnik (IKT) vor, also einen EU-weit geltenden europäischen Zertifizierungsrahmen für die Cybersicherheit von Produkten, Diensten und Verfahren. Das Prozedere der Festlegung von Mindeststandards und von deren Überprüfung ist bereits aus den Regulierungen zur allgemeinen Produktsicherheit bekannt. Die Verordnung richtet sich insoweit auf die Harmonisierung von Sicherheitsstandards. Die Einhaltung der festgelegten Cybersicherheitsmerkmale von IKT-Produkten, Diensten und Prozessen soll durch die jeweils zuständige nationale Stelle überprüfbar sein. Voraussetzung für die positive Konformitätsbewertung einer Produktkategorie ist die Erfüllung entsprechender Prüfkriterien, von der Verordnung als »Schema für die Cybersicherheitszertifizierung« bezeichnet. Für welche Produkte solche Schemata erstellt werden, legen Europäische Kommission, Vertreter der Mitgliedstaaten und der Stakeholder gemeinsam fest. Die ENISA erarbeitet die Entwürfe der Schemata. Nationale Schemata werden verdrängt, sobald für die Produktgruppen europäische Schemata verabschiedet wurden.

ENISA wird Sicherheitsstufen für IKT-Produkte und -Dienste festlegen. Für die jeweilige Cybersicherheitszertifizierung wird das einzelne IKT-Produkt bzw. der IKT-Dienst einer dieser Sicherheitsstufen zugeordnet. Künftig sollen drei Sicherheitsstufen Anwendung finden, »niedrig«, »mittel« und »hoch«, je nachdem, wie resilient die Produkte und Dienste gegen Cyberangriffe sind und welcher Grad an Vertrauenswürdigkeit mit ihnen verbunden werden kann. Die Entscheidung zur Zertifizierung eines Produkts nach einem vorhandenen Schema ist für den Hersteller freiwillig. Die Zertifizierung kann, je nach angestrebter Sicherheitsstufe, durch Herstellererklärungen oder durch unabhängige Konformitätsbewertungsstellen erfolgen. Das Vertrauen in IKT-Produkte von Unternehmen soll im Rahmen der Zertifizierung durch diverse Maßnahmen gefestigt werden. So müssen Hersteller:

- für ihre Produkte sichere Voreinstellungen wählen;
- den Endnutzern Hilfsmittel für einen sicheren Einsatz des Produkts bereitstellen;
- Sicherheitslücken bekanntmachen;
- Endkunden informieren, wenn die Unterstützung bzw. der Support für die individuell erteilte Sicherheitsgarantie endet.

Die ENISA wird schließlich Checklisten führen und öffentlich zur Verfügung stellen, um das Cyberrisiko des jeweiligen IKT-Produkts und -Dienstes vorab einzuschätzen. Sie soll ferner eine Liste von IKT-Produkten und -Diensten führen und fortwährend aktualisieren, für die sie eine Cybersicherheitszertifizierung für notwendig erachtet (Priority-List).

Allein schon wegen der Größe des europäischen Marktes wird das europäische Cybersicherheitszertifikat eine globale Relevanz erhalten. Zudem sorgen zwei ergänzende Mechanismen für eine schnellere Verbreitung der Zertifikate nach der Cybersicherheitsverordnung: In ihrer IT-Sicherheitsgesetzgebung für kritische Infrastrukturen und digitale Dienste (NIS-Richtlinie) fordert die EU von den Betreibern entsprechender Dienste, dass sie IT-Sicherheitsmaßnahmen »nach dem Stand der Technik« ergreifen. Dem Betreiber selbst obliegt es, diese unbestimmte rechtliche Vorgabe zu erfüllen. Die Nutzung von zertifizierten Produkten wird es ihm erleichtern nachzuweisen, dass er sich am Stand der Technik orientiert hat. Zudem schränkt die Verordnung die Freiwilligkeit der Zertifizierung durch den ausdrücklichen Hinweis ein, dass das EU-Recht an anderer Stelle, zum Beispiel sektoral, eine Zertifizierung fordern wird.

Es ist anzunehmen, dass Kommission und Parlament von dieser Einladung Gebrauch machen werden, um die Konformität neuer technischer Anwendungen mit den Cybersicherheitsanforderungen sicherzustellen.

Wie effektiv die neue europäische Cybersicherheitszertifizierung ist, wird maßgeblich davon abhängen, wie die EU bei der Erarbeitung der Schemata vorgeht. Manche Äußerungen der Kommission lassen darauf schließen, dass sie eine Priorität bei vernetzten Gegenständen (Internet of Things, IoT) im Verbrauchermarkt sieht. An anderer Stelle plädiert sie für einen Start der Zertifizierung im Bereich industrieller Anwendungen. Bereits bestehende Zertifizierungsschemata im Hochsicherheitsbereich, die vor allem für staatliche Anwendungen genutzt werden, sollen in das europäische System überführt werden.

Auch die nationale Gesetzgebung in Deutschland wird die Zertifizierung voraussichtlich ausweiten. Die Entwürfe für ein IT-Sicherheitsgesetz 2.0 enthalten zum Beispiel eine neue System-Kategorie »KRITIS-Kernkomponenten«. Gemeint sind IT-Systeme, die für das Funktionieren einer kritischen Infrastruktur von besonderer Bedeutung sind. Für sie soll Zertifizierung obligatorisch werden können. Die Bundesnetzagentur will gemeinsam mit dem BSI ersten Gebrauch von den neuen Bestimmungen machen und – gemäß dem unlängst vorgestellten Sicherheitskatalog – die Zertifizierung von Kernkomponenten der Telekommunikationsnetze anordnen. Dieser Schritt ist eine direkte Folge der Debatte über die zweifelhafte Vertrauenswürdigkeit von Huawei-Produkten für 5G-Netze.

Wie könnte eine Strategie des Dritten Weges gestaltet sein?

Mit der Verschmelzung der digitalen Märkte entwickeln sich global verschiedene Typen von regulatorischen Ordnungsmodellen. Das chinesische Vorbild, dem in ähnlicher Form Russland, der Iran und einige arabische Staaten folgen, steht für ein Modell der autoritären Reglementierung des digitalen Raums, das mit dem Anspruch gleichwertiger Legitimität neben das Modell der liberalen und offenen Gesellschaft tritt. Bereits heute lassen sich in einigen Mitgliedstaaten der EU Versuche beobachten, illiberale Entwicklungswege einzuschlagen. Angesichts der oben beschriebenen Konflikte drängt sich auch im Hinblick auf den digitalen Raum die Frage auf, welcher Umgang mit anderen Weltregionen angemessen ist. Sollte Europa in diesem Bereich eine konsequente Politik der digitalen Souveränität einschlagen? Und sollte es in der Folge mit Hilfe nationaler Förderprogramme eigene Mobilfunkdatennetze entwickeln, ein eigenes Google, ein eigenes WhatsApp und so weiter? So überzeugend eine solche Idee auf den ersten Blick zu sein scheint, so riskant könnten die langfristigen Konsequenzen eines Autonomiestrebens sein – innovationspolitisch wie sicherheitspolitisch.

Digitale Souveränität *und…*

Der Begriff digitale Souveränität bezeichnet die Fähigkeit eines Völkerrechtssubjekts zur Kontrolle und Steuerung des Cyberraums. Die Zertifizierungsschemata und die Datenschutzregeln der EU sind Instrumente zur Ausübung digitaler Souveränität, denn mit ihnen signalisiert die Union, dass sie sich das Recht vorbehält zu bestimmen, wie digitale Produkte und Dienste auf der Grundlage unserer Verfassungsprinzipien und eines demokratisch legitimierten Interessenausgleichs unter den Marktteilnehmern auszugestalten und einzusetzen sind. Dieser Anspruch, der sich aus dem Binnenmarktprinzip ergibt, gilt so lange und reicht so weit, wie der EU-Regulierungsansatz faktische Wirkung entfaltet und entsprechende Produkte und Dienste verfügbar sind. Leitplanken allein sorgen jedoch noch nicht für fahrfähige Autos. Teil der Ausübung digitaler Souveränität müsste es darüber hinaus auch sein, die Fähigkeit und vor allem die Innovationskraft der europäischen Ökonomie so zu fördern, dass diese geeignete Lösungen entwickeln kann. Schlüssel dazu sind (1) die Erhaltung und der Ausbau der globalen Wettbewerbsfähigkeit, (2) möglichst faire Wettbewerbsregeln und (3) Investitionen in digitale Infrastrukturen. Die EU hat einen eigenen Wertekosmos und auch gute Gründe, diesen in den Mittelpunkt ihrer Binnenmarktpolitik zu stellen. Sie beweist ihre digitale Souveränität, indem sie diese Werte in die Regulierung digitaler Produkte und deren Anwendung sowie bei der Steuerung und Implementierung von Innovationen einbringt.

Die Orientierung am Leitbild der digitalen Souveränität droht indes auch alte Konfrontationsmuster wiederzubeleben, denn das Konzept setzt auf Gefahrenabwehr und Territorialverteidigung. Im Bestreben, weniger anfällig zu sein für äußere Risiken und Bedrohungen, sollte Europa nicht den Fehler begehen, genau das zu befördern, was es eigentlich zu verhindern beabsichtigt. Nicht Abschottung, sondern vertrauens- und sicherheitsbildende Maßnahmen auf der Grundlage eigener Beurteilungs- und Steuerungsfähigkeiten müssen das Mittel der Wahl sein. Ein angemessenes Ziel ist vor diesem Hintergrund, digitale Souveränität mit strategischer Verflechtung zu verbinden.

… strategische Verflechtung

Unter strategischer Verflechtung ist eine Strategie zu verstehen, die die Komplexität der Realität unter den Bedingungen der Globalisierung und Digitalisierung anerkennt. Sicherheit wird in diesem Denken nicht durch Abgrenzung vom Anderen, sondern als Ergebnis eines Prozesses der ökonomischen und politischen Integration und der Steigerung wechselseitiger Abhängigkeit erreicht. Kooperatives Schnittstellenmanagement wie zum Beispiel die gegenseitige Anerkennung von Zertifizierungen im Bereich Produktsicherheit tritt an die Stelle konfrontativer Abgrenzung. Die europäische Integration ist das beste Beispiel dafür, wie durch Verflechtung Frieden und Stabilität in Europa geschaffen werden konnte.

Es gibt Stimmen, die einen solchen europäischen Weg »naiv« nennen und befürchten, dass die hohen Standards der EU Wettbewerbsnachteile bedeuten und dass die EU noch weiter hinter die USA und China zurückfallen werde. Konsumenten wären nicht bereit, für anspruchsvolle Standards zu bezahlen. Wie zuvor schon beim Datenschutz stellt sich auch beim Thema Cybersicherheit die Frage der Relevanz und Durchsetzungsfähigkeit europäischer Vorgaben: Muss Europa erst globaler Technologieführer werden, um sich anspruchsvolle lokale Standards leisten zu können? Ein genauerer Blick auf das Argument zeigt schnell, dass dessen Prämissen unplausibel sind: Europa, so die erste Annahme, sei nicht in der Lage, eigenständige Standards zu setzen, da der Ort der Standardsetzung nicht der Binnen-, sondern der Weltmarkt ist. Hier aber würden, so die zweite Annahme, die USA und China so lange dominieren, wie sie die leistungsfähigeren Produkte entwickelten. Diese Vorherrschaft qua Leistungsfähigkeit werde wiederum dadurch noch zementiert, so die dritte Annahme, dass Konsumenten nicht bereit wären, ethische Standards als Leistungsmerkmale anzuerkennen und entsprechend dafür zu bezahlen.

Keine der drei Annahmen hält allerdings einer näheren Überprüfung stand: Die Datenschutz-Grundverordnung hat deutlich gezeigt, dass Europa durchaus in der Lage ist, eigenständig anspruchsvolle Standards zu setzen und ihre Anwendung europaweit zu gewährleisten. Europäische Standards wirken sogar weit über die EU hinaus. Japan orientiert sich am europäischen Recht ebenso wie Indien und – ab 2020 – Brasilien. Für viele weltweit aktive Konzerne ist es sinnvoller, die anspruchsvollen EU-Regularien überall anzuwenden, als auf unterschiedlichen Märkten mit unterschiedlichen Standards zu operieren. Facebook fordert mittlerweile eine globale Regulierung nach dem Vorbild der DSGVO. Gerade in Drittmärkten außerhalb Europas (und außerhalb der USA, Chinas und Russlands) haben europäische Standards gute Chancen. Im Bereich der globalen Produktregulierung greift letztlich die gleiche Logik, die sich auch schon bei der Produktregulierung in der EU beobachten ließ: Der sogenannte California-Effekt sorgt dafür, dass hohe Standards niedrige Standards dann verdrängen, wenn sie in relevanten Teilmärkten gesetzlich verbindlich sind. Damit ist dann auch die dritte Annahme falsifiziert, dass Konsumenten nicht bereit wären, für hohe ethische Standards zu bezahlen. Die hohe Qualität europäischer Normen, angefangen bei der Maschinensicherheit und bis hin zur Lebensmittelreinheit, ist ein wesentlicher Bestandteil der Erfolgsgeschichte der europäischen Integration und ein zentraler Wettbewerbsvorteil gegenüber anderen Regionen. Es gibt wenig Grund zu der Annahme, dass sich diese Logik nicht auch auf digitale Produkte und deren Cybersicherheit übertragen lässt, zukünftig vielleicht auch auf Komponenten künstlicher Intelligenz.

Die digitale Souveränität Europas lässt sich mit einer strukturellen Offenheit und globalen Vernetzung des digitalen Binnenmarkts vereinbaren, wenn diese Güter strategisch miteinander verbunden werden:

1. Europa sollte Kernbereiche digitaler Technologien und Infrastrukturen definieren, die eine Beurteilungs- und Steuerungsfähigkeit erfordern. Netzwerktechnik und Cloud-Dienste zum Beispiel müssen sicherlich vertrauenswürdig sein.
2. Die europäische Cybersicherheitszertifizierung muss in diesen Bereichen schnell und konsequent genutzt werden. Sie muss eine politische Agenda bekommen. Deutschland könnte dies während seiner bevorstehenden Ratspräsidentschaft vorantreiben.
3. Interoperabilität von Systemen und Offenheit von Plattformen müssen ein Grundprinzip europäischer digitaler Dienste und Infrastrukturen sein. Die anstehenden nationalen und europäischen Regulierungsvorhaben im digitalen Bereich sollten sich noch stärker an dieser Maxime orientieren.
4. Europäische Infrastrukturinvestitionen müssen in entsprechende, europäisch zertifizierte Dienste gelenkt werden. Das gilt gleichermaßen für die Bereiche Energienetze, digitale Mobilität oder Gesundheitswesen.
   Die Fähigkeit, das Wirken ausländischer Technologien in den definierten Kernbereichen beurteilen und kontrollieren zu können, muss regelmäßig überprüft werden. Entsprechende Zulassungen sollten zeitlich begrenzt erteilt werden. Ähnlich wie bei 5G sollten auch für

andere Technologiebereiche europäische Risk Assessments erarbeitet werden.

5. Die Cyber-Außenpolitik sollte massiv intensiviert werden, um bestehende Bedenken durch bi- und multilaterale sicherheits- und vertrauensbildende-Maßnahmen auf Grundlage des Prinzips der Reziprozität schrittweise zu reduzieren. Erkenntnisse über die Vertrauenswürdigkeit von Herstellern – wie im Beispiel 5G – müssen auf EU-Ebene politisch bewertet und abgestimmt werden. Sie können nicht technisch beseitigt werden.

The DSI Industrial & Policy Recommendations (IPR) Series is published by the Digital Society Institute of ESMT Berlin, http://dsi.esmt.org.