DSI | DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

DSI Industrial & Policy Recommendations (IPR) Series

Europe's Third Way in Cyberspace

What part does the new EU Cybersecurity Act play?

Annegret Bendiek and Martin Schallbruch

DSI-IPR-19-01

Dr. Annegret Bendiek is a Senior Associate in the EU/Europe Research Division. Martin Schallbruch is Deputy Director of the Digital Society Institute at the ESMT Berlin.

Cybersecurity has become a key issue for Europe in the global digital transformation. The EU Cybersecurity Act lays down a legal framework whose aim is to achieve global reach. Embedded in a policy that combines digital sovereignty with strategic interdependence, the Act could represent the gateway to a third European pathway in cyberspace, something in between the US model of a liberal market economy and the Chinese model of authoritarian state capitalism. The Cybersecurity Act will be a binding framework for action and provide a tailwind for German cybersecurity policy.

Cyber threats are a component of and, at the same time, the spearhead of global competition between liberal democracies and authoritarian systems. The different understanding of cybersecurity and information security between Western countries, on the one hand, and states such as China and Russia, on the other, remains a key area of conflict in international politics. After more than ten years of unsuccessful negotiations against a backdrop of growing rivalry between the US and China, an agreement on global standards and regulations is still a long way off. The EU is trying to find a third way which circumvents this rivalry. This has become apparent in, among other things, the 5G debate. The Commission is inclined to allow the Chinese company, Huawei, to be involved in building European 5G infrastructure, subject to tight controls and only if all market participants meet strict hardware and software certification criteria. The question of the trustworthiness of Chinese telecommunications components is being shelved in favour of a market regulation solution. With its General Data Protection Regulation (GDPR), which Member States have been required to apply since May 2018, and its consistent approach to competition policy, the EU has taken on an effective and globally respected role as a regulatory power, achieving a balance between consumer protection and the competitiveness of the industry. The EU Cybersecurity Act further strengthens Europe's regulatory power. However, the European cybersecurity certificate, defined with the entry into force of the Act in June 2019, will only be able to develop into a global model if it is flanked by a European strategy for the digital space. Regulation, competition and industrial policy, as well as support for innovation must relate to security and cyber foreign policy. The key question will be whether and how the EU can successfully strengthen European digital sovereignty whilst preserving its liberal democratic traditions in the digital space and ensure the necessary strategic interdependence with other regions of the world.

DSI Industrial & Policy Recommendations (IPR) Series

Cybersecurity at the heart of global conflicts

The relevance of the current conflicts between the US, China and the EU goes far beyond trade and investment policy issues. They are so contentious because digital technologies form the communicative infrastructure of highly developed information societies. Those who control the hardware and software also determine which innovations and business models are possible and who has access to what information. There is increasing cooperation between private technology companies and institutions that perform tasks of state responsibility, such as protecting critical infrastructure. This trend can be seen both in the EU and in the US, but much more so in China and Russia, whose governments regard cybersecurity to an even greater extent as the cornerstone of their striving for state control over cyberspace. The EU no longer treats companies working in China and Russia to expand social surveillance or cooperating with the NSA in the USA merely as an apolitical, market-economy actor.

Conflict of Values

Since Edward Snowden's revelations and the use of digital technologies for state surveillance, the aspiration that the Internet will promote freedom and human rights everywhere is no longer completely plausible. It is evident that today's Internet is a space in which conflicts of values and distributional conflicts occur and future modalities of individual and social self-determination are negotiated. The technology of the network infrastructure and its associated applications are not value-neutral instruments, instead they are impacting on decisions and actions. They are instruments of value-related policies, as the dispute over Chinese technology company, Huawei, shows. The US administration views Huawei not only as a market participant but, at the same time, as a Trojan horse from an unfriendly government. Beijing refutes these allegations and considers the exclusion of Huawei from the US market as a measure directed against China's position in the global market as a whole.

The conflict over Huawei marks a break with the purely market-based logic of global trade relations and expedites a growing digital mercantilism. Many see converging markets as no longer simply an opportunity to improve prosperity, but also as a danger to self-determination and public safety. They argue that digital products are suitable for undermining value systems and subverting governmental control through technical backdoors. Terms such as 'technological sovereignty' and 'economic vulnerability' or "weaponized interdependence" are an indication and legitimation of the growing willingness to restrict innovation and competition when it comes to digital products and services. However, new confrontations in the digital world are not limited to the relationship between the West and China. Conflicting values that are difficult to reconcile exist even today in transatlantic relations. The much vaunted transatlantic community of shared values reaches its limits where the idea of a free (digital) single market clashes with the requirement to protect personal data and informational self-determination, and with European competition law. The long-ignored dominance of US Internet companies has forced Europe to embark on a course of digital self-assertiveness - from data protection and competition law to taxation.

Cybersecurity Conflict

Cyber attacks and defence are seriously challenging state sovereignty. While the complexity and interdependence of digital systems are rapidly increasing, the safety quality of the hardware and software used for these systems remains underdeveloped and lacks the necessary human resources to secure them. Cyberspace is constantly creating new attack vectors and targets. The criminal exploitation of vulnerabilities, such as the use of ransomware to blackmail companies, and state cyber attacks aimed at eliciting information or causing destabilisation, or as part of hybrid warfare, are mutually reinforcing. The most extreme example is North Korea which generates global revenue from global cyber operations for the procurement of missile technology. In five rounds of negotiations at UN level, a Group of Governmental Experts (GGEs) has been debating the international condemnation of and/or the placing of restrictions on cyber attacks and setting up a cyber defence organisation under international law - but without success. No short-term progress can be expected from the current sixth round of the GGE, nor from parallel negotiations initiated by Russia being conducted in an Open Ended Working Group (OEWG).

Trade Conflict

The trade dispute between the US and China is essentially entangled with the development of markets in goods and services towards a greater emphasis on digital products and services. The digital transformation of global markets is not only accompanied by a growing economic interdependence, it has also increasingly reduced the ability of individual countries to

control them. When US President Trump announces trade restrictions, he intends to regain control over the innovation-driven global competition the US is confronted with. At the same time, the products and services offered by US tech companies are an essential tool of state control and influence for Washington. However, complex digital systems such as 5G network technology could prove to be an almost uncontrollable technology that has been built into a state's infrastructure for decades and is ultimately under the control of an authoritarian state. Network products are currently evolving the software-based technology. The regular updates required for software bring functional improvements that the operator using it hardly notices. At the same time, the digital transformation is affecting all market segments, from agricultural products to medical technology and mechanical engineering. Trade issues matter for digital sovereignty and vice versa.

The EU as regulatory power

In order to assert regulatory power in this conflict-prone world without borders, it has committed itself to a very specific path that is fundamentally different from both Silicon Valley's libertarian regulatory style and China's authoritarian model. Europe's regulatory power is based on the European Treaties and on the premise that individual freedom and social responsibility (Article 2 TEU) are equally important. Democratic decision-making is based on the rule of law and the market participant is involved as a regulatory addressee in formulating and implementing legal acts within EU comitology. In Articles 3 and 10 of the TEU, the EU emphasises the individual self-determination of Europe's citizens with its commitment to market freedoms and democracy. It involves various stakeholders and market participants in formal and informal EU procedures, where they take a position, for example, on fundamental ethical issues. In recent years, the Council of Europe, the European Council, the European Parliament and the Commission have formulated a set of principles which reflect the idea of a digital society centred on the individual and the common good, at the same time. New technologies must, therefore, also be judged by whether they are conducive to democracy and whether their use respects human rights. Regulatory measures can make a decisive contribution to balancing the opportunities and risks of a technology with the interests of companies, consumers, the state and civil society. One impressive example of this regulatory approach is the EU Communication on Artificial Intelligence (AI). AI is not understood as an end in itself but as "a tool operating in the service of humanity and the public good". The final report from an expert group set up by the Commission and published in April 2019 stresses the need to preserve human autonomy in the use of AI, to avoid harming people and to generally respect the principles of fairness and comprehensibility. Despite the general European consensus on the need for market freedom, data protection and security to be closely linked and balanced in regulatory terms, there is still little agreement on how national security standards can be reconciled with the EU's liberal market logic. This lack of agreement is particularly evident in the way it has dealt with the Chinese company Huawei.

Data protection and data security as an EU interest

The specifically European approach to digitisation can be found in the EU's legislative acts on data protection and data security. The General Data Protection Regulation, which has been in force for all companies since May 2018, sets new standards in the task of finding a balance between protecting personal data and ensuring the free movement of data in the Single Market. Data protection and cybersecurity have so far been considered separately. However, the two topics are increasingly merging into one. This can be seen, for instance, in digital energy meters (SmartMeter). Not only are they subject to the highest levels of safety and security standards, they also have the highest data protection requirements in order to ensure that third parties do not gain illegal access to data about users' domestic habits. By establishing a comprehensive system of defining and certifying technical cyber security, the EU is taking a major step towards further consolidating its role as a regulatory power, which it played so successfully with the GDPR.

The Cybersecurity Act

On 10 December 2018, the European Parliament, the European Council and the European Commission agreed on the policy terms of a Cybersecurity Act. The Regulation on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act) entered into force in June 2019. The Act contained two major reforms: The EU cybersecurity agency (European Union Agency for Network and Information Security, ENISA) will have a mandate beyond 2020 to assist Member States in dealing with cyber attacks. It introduces a cybersecurity certification framework for ICT products, services and processes (European certification framework). Certification is based on the idea that standards and norms can create a balance between the need for consumer protection and the industry's legitimate claim to competitiveness. Both are high European principles that need reconciling with one another. Consumer protection means protecting consumers from negative consequences, such as unauthorised disclosure or use of their data, and generally providing them with reliable and high-quality products. However, these objectives may

conflict with the competitiveness of some providers. For example, companies often view high standards of privacy and data security as barriers to competition.

The Cybersecurity Act provides for a voluntary 'conformity assessment' of information and communication technology (ICT) products, i.e. an EU-wide European certification framework for the cybersecurity of products, services and processes. The procedure for setting minimum standards and reviewing them has already been established in the regulations on general product safety. In this respect, the Regulation focuses on harmonising safety standards. The relevant national body should be able to verify that they comply with the established cybersecurity features of ICT products, services and processes. In order for a product category to be deemed compliant it must meet a series of review criteria, referred to in the Regulation as a "European cybersecurity certification scheme". The European Commission, representatives of the Member States and stakeholders shall jointly determine the products for which such schemes are to be drawn up. ENISA shall prepare drafts for the schemes. As soon as European schemes for the product groups have been adopted, they will replace any national schemes.

ENISA will also specify assurance levels for ICT products and services. A European cybersecurity certification scheme may specify one or more assurance levels for ICT products and ICT services. In future, there will be three assurance levels: 'basic', 'substantial' or 'high', depending on how resilient the products and services are against cyber attacks and the degree of trust that can be guaranteed to them. Manufacturers are free to decide whether or not to certify a product according to an existing scheme. Depending on the desired assurance level, certification can be implemented by an independent assessment body or take the form of a manufacturer's declaration. The aim is to boost confidence in company ICT products through the implementation of various measures that are part of the certification process. Consequently, manufacturers must:

- select secure default settings for their products;
- provide end users with the tools to use their products in a safe and secure manner;
- disclose security vulnerabilities;
- inform end customers when support for an individually issued security guarantee ends.

Finally, ENISA will maintain and make publicly available checklists to pre-assess the cyber risk of each ICT product and service. It will also keep and continuously update a list of ICT products and services for which it considers cybersecurity certification to be a necessity (priority list).

The European cybersecurity certificate scheme will acquire global relevance due to the sheer size of the European market. In addition, two complementary mechanisms ensure that adoption of the certification schemes will occur more swiftly under the Cybersecurity Regulation. In its IT security legislation on critical infrastructures and digital services (NIS Directive), the EU requires operators of such services to take 'state-of-the-art' IT security measures. The operators themselves are responsible for meeting this undefined legal requirement. The use of certified products will make it easier for them to prove they have aligned themselves with the state of the art. In addition, the Regulation limits the voluntary nature of certification by explicitly stating that EU law will require certification from another body, for example one in the relevant sector. It is likely that the Commission and Parliament will make use of this invitation to ensure that new technical applications comply with cybersecurity requirements.

The effectiveness of the new European cybersecurity certification will largely depend on the EU's approach to developing these schemes. Some of the Commission's statements suggest that it regards Internet of Things (IoT) products in the consumer market as a priority. Elsewhere, it advocates applying certification schemes in the field of industrial applications. Current certification schemes in the high security sector, which are mainly used for government applications, are to be transferred to the European system.

Germany is also expected to bring in national legislation to broaden certification. For example, the draft IT Security Act 2.0 includes a new system category for 'Critical Infrastructure Core Components'. It refers to IT systems that are of particular importance for the functioning of critical infrastructure. Certification should certainly become obligatory for such systems. The Federal Network Agency (*Bundesnetzagentur*), together with the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI), intends to make initial use of the new provisions - in accordance with the recently introduced safety catalogue - to mandate the certification of the core components of telecommunications networks. This move is a direct consequence of the debate over the lack of trust in Huawei products for 5G networks.

How might the strategy for a third way be designed?

As digital markets start to merge, different types of regulatory models have evolved globally. The Western model for liberal and open societies is increasingly interoperable with the Chinese model, which is similar to ones used in Russia, Iran and some Arab states, representing an authoritarian regimentation of the digital space with an equal claim to legitimacy on a global scale. Some EU Member States are already trying to pursue illiberal development paths. Given the conflicts described above, the burning questions are: what is the most appropriate stance to take in dealing with the digital space in other regions of the world? Should Europe stick to a consistent policy of digital sovereignty on this issue? Should it subsequently develop its own 6G mobile data networks with the aid of national funding programmes, its own Google, its

own WhatsApp and so on? As convincing as this idea may initially sound, the long-term consequences of a desire for digital strategic autonomy may be fraught with risk - both in terms of innovation policy and security policy.

Digital sovereignty *and*...

The term digital sovereignty refers to the ability of a subject of international law to control and regulate cyberspace. The EU's certification schemes and data protection rules are instruments for exercising digital sovereignty, signalling that the Union reserves the right to determine how digital products and services are designed and used based on its constitutional principles and a democratically legitimate balance of interests among market participants. This requirement, derived from the internal market principle, applies for as long as the EU's regulatory power continues to have a real impact and where corresponding products and services are available. Nevertheless, crash barriers alone do not produce roadworthy vehicles. Exercising digital sovereignty should also include promoting the European economy's capability and, above all, its innovation policy in such a way that it can develop appropriate solutions. Key to this are (1) maintaining and enhancing global competitiveness, (2) rules on competition that are as fair as possible (3) investment in digital infrastructures. The EU has its own set of values and good reasons for placing them at the heart of its internal market policy. It demonstrates its digital sovereignty by incorporating these values into its Regulations on digital products and how they are used, as well as in controlling and implementing innovations.

However, heading towards this model of digital sovereignty threatens to revive old patterns of confrontation because the concept is centred around risk prevention, territorial defence and protectionism. In an effort to be less vulnerable to external risks and threats, Europe should not make the mistake of promoting exactly what it intends to prevent. The means of choice for the EU must be measures that build trust and security based on its own assessment and control capabilities, and not protectionism. Against this background, an appropriate objective would be to combine digital sovereignty with strategic interdependence.

... strategic interdependence

Strategic interdependence is a strategy that recognises that, in the context of globalisation and digitisation, the reliance on resource security, production chains and market openness are only a few drivers of complexity. In this perspective, security is not achieved by political self-reference, but as the result of a process of economic and political integration and increasing interdependence by default. Cooperative interface management, such as mutually recognising product safety certifications, replaces confrontational boundaries. European integration is the best example of how interdependence has brought peace and stability to Europe.

There are those who call this European approach naïve and fear that the EU's high standards in data protection and data security will put it at a competitive disadvantages and that the EU will fall even further behind the US and China. They suggest that consumers are not prepared to pay for higher standards. As was the case with data protection, the problem of the relevance and enforceability of European guidelines also rears its ugly head with cybersecurity: Does Europe first have to become a global technology leader in order to be able to afford ambitious local standards? A closer look at the argument quickly reveals that its premises are implausible. According to the first assumption, Europe is not in a position to set its own standards since standards are not set in the Single Market, but in the world market. However, according to the second assumption, in this case the US and China would dominate for as long as they develop better performing products. This supremacy of performance is further cemented, according to the third assumption, in that consumers are unwilling to recognise ethical standards as performance features and pay more for them accordingly.

However, none of the three assumptions holds up under closer scrutiny. The General Data Protection Regulation has clearly shown that Europe is in a position to independently set demanding standards and to ensure they are applied throughout Europe. European standards even have an impact far beyond the EU. Japan aligns itself with European law, as does India and, from 2020, so will Brazil. For many globally active corporations it makes more sense to apply the demanding EU regulations everywhere than to operate with different standards in different markets. Facebook is now calling for global regulation modelled on the GDPR. European standards also have good prospects in third markets outside Europe (and outside the US, China and Russia). Ultimately, the same logic observed in EU product regulation also applies to global product regulation. The 'Brussels effect' ensures that high standards displace low standards when they are legally binding in relevant submarkets. This also falsifies the third assumption that consumers are not prepared to pay for high

ethical standards. The high quality of European standards and their mutual recognition, from machine safety to food purity, is an integral part of the success story of European integration and a key competitive advantage over other regions. There is no reason to assume that this logic cannot be applied to digital products and cybersecurity, and perhaps in the future to components of artificial intelligence as well.

Europe's digital sovereignty can be reconciled with the structural openness and global connectivity of the digital single market if these goods are strategically linked with one another:

1. Europe should define core areas of digital technology and infrastructure that require assessment and accountability. For example, network technology and cloud services must certainly be trustworthy.

2. The uptake of European cybersecurity certification in these areas needs to be swift and consistent. It needs to get a political agenda. Germany could press ahead with this during its forthcoming Council Presidency.

3. System interoperability and platform openness must become the fundamental principles of European digital services and infrastructures. Even greater attention should be paid to these principles in upcoming national and European regulatory projects in the digital sector.

4. European infrastructure investments need to be channelled into services with the corresponding European certification. This applies equally to energy networks, digital mobility and healthcare.

5. The ability to assess and control the work of foreign technologies in defined core areas must be regularly reviewed. The corresponding approvals should be granted for a limited time period. As with 5G, European Risk Assessments should also be developed for other technology areas.

6. Cyber foreign policy should be massively intensified in order to gradually ease current concerns through bilateral and multilateral security and confidence-building measures based on the principle of reciprocity. Insights into the trustworthiness of manufacturers - such as in 5G - need to be politically assessed and agreed at EU level. Doubts cannot be eliminated through the technology.

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

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.