Europe's third way in cyberspace: what part does the new EU Cybersecurity Act play?

Bendiek, Annegret; Schallbruch, Martin

Veröffentlichungsversion / Published Version
Stellungnahme / comment

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

Empfohlene Zitierung / Suggested Citation:
Bendiek, A., & Schallbruch, M. (2019). *Europe's third way in cyberspace: what part does the new EU Cybersecurity Act play?* (SWP Comment, 52/2019). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://doi.org/10.18449/2019C52

SWP

SWP Comment

NO. 52 DECEMBER 2019

Europe's Third Way in Cyberspace

What Part Does the New EU Cybersecurity Act Play?

Annegret Bendiek and Martin Schallbruch

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 digi-

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

tal sovereignty whilst preserving its liberal democratic traditions in the digital space and ensure the necessary strategic interdependence with other regions of the world.

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 a 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-build-

ing 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 online version of this publication contains functioning links to other SWP texts and other relevant sources.

SWP Comments are subject to internal peer review, fact-checking and copy-editing. For further information on our quality control procedures, please visit the SWP website: https://www.swp-berlin.org/en/about-swp/quality-management-for-swp-publications/

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1861-1761
doi: 10.18449/2019C52

Translation by Martin Haynes

(English version of SWP-Aktuell 60/2019)

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.