The EU's Regulatory Approach to Cybersecurity

Annegret Bendiek and Eva Pander Maat
## Contents

1. **“Cybersecurity by Regulation”** 3  
   1.1 The EU’s Cybersecurity Strategy 5  
   1.2 The Role of the ECJ 6  

2. **First Pillar: Single Market** 9  
   2.1 The Digital Single Market 9  
   2.2 Towards a Cyber-resilient Regulatory Framework 11  

3. **Second Pillar: The Area of Freedom, Security and Justice (AFSJ)** 16  
   3.1 The Security Union 17  
   3.2 Substantive Cybercrime Norms 18  
   3.3 Law Enforcement Cooperation 19  

4. **Third Pillar: CSDP** 21  
   4.1 Mutual Defence Clause 21  
   4.2 Common Defence Cooperation 22  
   4.3 Common Defence Investment 23  

5. **Fourth Pillar: CFSP** 24  
   5.1 Cyber Diplomacy Toolbox 24  
   5.2 Cybersecurity Concerns in Foreign Trade 25  

6. **Conclusion** 27  

7. **Annex** 29
1. “Cybersecurity by Regulation”

"While many aspects of cybercrime are firmly established, other areas of cybercrime have witnessed a striking upsurge in activity, including attacks on an unprecedented scale, as cybercrime continues to take new forms and new directions."¹

"A growing amount of illicit trade now has an online component"²

"Criminals increasingly abuse cryptocurrencies to fund criminal activities"³

"By the end of 2016 we had witnessed the first massive attack originating from [Internet of Things] devices, as the Mirai malware transformed around 150 000 routers and CCTV cameras into a DDoS botnet"⁴

"The combination of factors behind the WannaCry and NotPetya attacks of mid-2017 have taken malware attacks to a level where they can be an impossible challenge for national law enforcement agencies to handle alone."⁵

"Criminals continue to use Distributed-Denial-of-Service (DDoS) attacks as a tool against private business and the public sector. Such attacks are used not only for financial gains but for ideological, political or purely malicious reason."⁶

"In a 12-month period, [data-] breaches relating to the disclosure of over 2 billion records were reported, all impacting EU citizens to some degree."⁷

The free trade of data has spurred globalization and brought about an ever-more interconnected world. Cyberspace and the internet were long seen as a source of economic growth, a place primarily belonging to businesses and customers. The EU, too, has long seen the digital world through an economic lens with a free trade perspective. Today still, 'data transfers are seen as crucial to revive the slowing European economy.'⁸ However, as concerns about the privacy rights and security of individuals in cyberspace have grown, cybersecurity has in the past two decades quickly ascended to the top of the political and legislative agenda in the European Union (EU). This is in spite of the

---

fact that cybersecurity remains a legal competence of the Member States, as the Treaties do not provide a unifying legal basis for the EU to regulate cybersecurity. Consequently, the EU mainly has a coordinating role in the area of cybersecurity. The EU's approach to cybersecurity is scattered across the policy domains which are affected by cyber-threats and in which the Treaties do confer powers upon the EU. These include first, and primarily so, the internal market; second the Area of Freedom, Security and Justice (AFSJ); third the Common Security and Defence Policy (CSDP); and fourth the Common Foreign and Security Policy (CFSP). The EU has broad legislative competences to regulate the single market. In contrast, its competences in the AFSJ are mainly restricted to matters of law enforcement. Moreover, although the EU's moderate mandate to formulate within CSDP cyber defence projects have recently gained somewhat of a political momentum, these domains are still mostly nationally governed.

The EU has been driven primarily by an internal market rationale in its approach to cybersecurity. This rationale entails that the EU deploys its political and legal mandate to regulate the internal market to issue common policies and legislation on cybersecurity. Conveniently so, because the foundational Treaties provide the most versatile legislative basis for internal market regulation: the "catch-all provision" of article 114 TFEU. In turn, cybersecurity has functioned as a tool for the EU legislator to expand the range of Union action in domains outside of the internal market. Cybersecurity as a new policy field has proven able to yield relatively broad political support for common action, particularly stretching the Treaty provisions for security and foreign policy. When compared to regional and international organizations in global cyber governance with narrow, clearly defined mandates specifically devoted to cybersecurity, the EU's mandate is limited and can be characterized as "cybersecurity by regulation" (Ramses Wessel).

The EU's approach to cybersecurity is being implemented in a piecemeal fashion. The lack of a unifying legal basis to address cybersecurity has forced the EU to formulate its approach based on other competences, primarily internal market regulation. Two recent major policy projects have been instrumental in this approach. First, in 2014 the Juncker Commission announced that a Digital Single Market strategy (DSM) would be at the top of its political agenda. Cybersecurity forms an integral part of the DSM as

---


10 This categorization is in line with the 2013 Cyber Security Strategy and, in a different order, was presented in Annegret Bendiek, "The EU as a Force for Peace in International Cyber Diplomacy" SWP Comment No. 19, April, 2018.

11 Article 4(2)(a) TFEU provides the EU with shared competences in the area of the internal market, but article 114 TFEU has long proven a fruitful legal basis for legislative development, making the internal market into the most mature area of European policy and law.

12 See paragraph 5 for more on the constitutional construction of the AFSJ.

13 See paragraph 6 and 7 for more on the constitutional construction of the CFSP and CSDP.


an essential tool for averting economic damage to and conserving consumer trust in the European markets. Second, in 2015 the Commission employed the legal basis of the AFSJ for the construction of the so-called Security Union. In line with the internal market rationale, cybersecurity is an integral part of the Security Union to protect the EU’s digital market. The key elements of the EU’s cybersecurity approach stem from either of these two projects, notwithstanding frequent mutual overlaps which demonstrate the unique cross-sectional nature of cybersecurity as a policy field.

1.1 The EU’s Cybersecurity Strategy

The overarching strategy within the EU’s approach to cybersecurity was only consolidated in 2013, when the Cyber Security Strategy (CSS) was agreed upon. However, the construction of the EU’s approach to cybersecurity can be traced back to the completion of the internal market in 1985. The economic opportunities of the emerging global market for digital services and goods led the Commission to identify ICT and the digital domain as a potential area of Union action. In the subsequent decades, this argument was firmly entrenched in EU digital policy-making and prevailed when it became apparent that digitalization brought risks as well as benefits. The risks of digitalization are interpreted in an economic rather than a security discourse: cyber threats undermine citizens’ trust in online services and negatively impact the economy. For this reason, the EU is legitimized to take measures to improve cybersecurity to protect the internal market. Three decades and some later, the internal market rationale is still the primary rationale behind the EU’s approach to cybersecurity and determines the legislative, political and industrial agenda on cybersecurity.

The CSS reflects and, carefully, expands the internal market rationale set out above. The policy priorities set out in 2013, confirmed by the 2017 review and renewal of the CSS, entail 1) achieving cyber resilience, 2) reducing cybercrime, 3) developing cyber defence policy and capabilities related to the CSDP, 4) developing industrial and technological resources necessary for cybersecurity, and 5) establishing a coherent cyberspace policy. The concept of resilience is defined as ‘a capacity to resist and regenerate’ and being ‘crisis-proof’ and features as a common thread through all domains of the EU’s cybersecurity.

19 COM (85) 310 final (Milan, June 14 1985).
policy, as well as the 2016 Global Strategy. To the EU, “security begins internally”. When speaking of cyber resilience, the EU mainly has the resilience of the private sector, providers of essential services and operators of critical infrastructures in mind. The eventual aim, in cyberspace as well as in other areas, is to create “deterrence by resilience”.

The core of the EU’s cybersecurity strategy is the pursuit of internal cyber-resilience, to be achieved by means of a legal-regulatory as well as an industrial agenda that minimizes the economic risks of cyber threats and strengthens repair mechanisms. The objective of achieving internal resilience is complemented by measures aimed at trust-building, creating global interdependence and advocating common norms.

In spite of the 2013 and 2017 Strategies, the institutional and policy cohesion of the EU’s approach to cybersecurity is subject to criticism. Regulatory and policy developments stretch across policy domains at varying speeds. Harmonization has been achieved in some fields, such as the protection of information systems and certification, and lagged behind in others, such as substantive and procedural criminal law. Investments in digital infrastructure and technology have steadily increased but are as of yet insufficient to compensate for the deficient competitiveness of the EU’s ICT market. Cybersecurity efforts in all domains are eventually accessory or complementary to the internal market and serve to protect the internal market’s economic resilience rather than the EU as such. The most concrete legislative and political efforts follow the internal market rationale: the Union is legitimized to devise standards on data protection and security because the regulation of the internal market requires it to.

As the largest internal market in the world, the EU’s resilience-based approach serves as a force for cybersecurity regulation at the GGE level at the United Nations. The EU’s strength, however, lies mainly with the externalization of internal market-related standards. The EU will require a forward-looking regulatory framework which is consistently compatible with norms and values enshrined in the Treaties and the Charter to fulfil its potential as a global digital norm builder.

1.2 The Role of the ECJ

The European Court of Justice (ECJ) oversees the application of the Treaties in line with the law. The ECJ is therefore essential to the effectiveness and resilience of the EU as a legal community, which is founded upon the rule of law and respect for human rights. The Commission employed its exclusive competence on the internal market to regulate cyberspace, article 114 TFEU, which also functioned as the initial legal basis for EU data protection

---

28 The Charter of Fundamental Rights of the European Union.
29 Article 19 TFEU.
30 Article 2 TFEU.
The ECJ has not issued any rulings on cybersecurity specifically, which is not surprising given the novelty of the first comprehensive legislative instruments on cybersecurity. Nevertheless, the ECJ’s case law on data protection sets a clear precedent on the EU’s approach to rights protection in cyberspace. In the case of data protection, the ECJ confirmed internal market regulation as a legal basis for regulating cyberspace, has boosted the prevalence of data security, expanded the fundamental right to data protection, reinforced the extraterritorial scope of the EU’s data protection law and maintained a strong focus on minimum standards overall.

The ECJ in the Digital Rights Ireland decision assessed the contended Data Retention Directive by the fundamental rights to private life and privacy. Notably, the ECJ focused on the Directive’s secondary objective: that of security. This focus illustrates that the suitability of article 114 as a legal basis can be questioned, but is not as such by the ECJ. The ECJ set strict minimum standards for data security and went so far as to invalidate the Directive because these standards were not met. The decision thus made explicit the legal argument that the EU legal community commits to providing a high level of security in cyberspace, even if the constitutional basis to do so stems from the internal market. In Tele2 and Watson, then, the ECJ confirmed that the standards it set out in Digital Rights Ireland are mandatory and that the ECJ is indeed competent to review not only the retention, but also the access to data. The ECJ’s decision in the Google Spain case established the ‘right to be forgotten’. This decision buttressed the relevance of the fundamental right to data protection in the EU’s digital economy, which is weighed heavily in the balancing exercise between privacy and the right to information or Google’s economic interests in a free flow of data. Google Spain confirms that the ECJ takes the perspective of the data subject, i.e. the customer or individual, rather than that of the data processor, i.e. businesses or governments. Following a recurrent pattern in EU law, the ECJ’s rights-oriented approach has now been codified in article 16 TFEU, which provides an express legal basis for the EU to protect the fundamental right to data protection. Article 16 TFEU, in addition to the internal market rationale and the security dimension of data protection, functioned as the legal basis for the General Data Protection Regulation (GDPR).

---

32 The ECJ has as of yet never questioned using article 114 TFEU as a basis for cyberspace regulation. Its choice not to was particularly striking in the case of Digital Rights Ireland, in which the Court assessed the Data Retention Directive exclusive by the extent to which it attained its secondary objective, of attaining security. (Article 114 allows for the issuance of legislation which employs, alongside the objective of the functioning of the internal market, other objectives.)
33 Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union.
34 European Court of Justice, Joined Cases C-293/12 and C-594/12 “Digital Rights Ireland, April 8, 2014.
36 European Court of Justice, Joined Cases C-293/12 and C-594/12 “Digital Rights Ireland, April 8, 2014, para 71.
38 European Court of Justice, Case C-131/12 “Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,” May 13, 2014.
39 European Court of Justice, Case C-131/12 “Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,” May 13, 2014, para 97.
41 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,
The ECJ has also reinforced the extraterritorial effects of the EU’s data protection law. This effect has both a legal and a non-legal dimension. By means of the so-called Brussels effect, EU data protection law is adopted by businesses outside of the EU’s physical borders because of the economic incentive to access the internal market. Complementary to this ‘soft’ effect, third countries are incentivized to adopt EU-level data protection standards by adequacy decisions and data protection standards in bilateral agreements. The EU only categorically allows data transfers to a third country if an “adequate level of protection” is ensured. An adequacy decision, then, exempts data controllers or processors established in or processing personal data belonging to data subjects in the EU from referring to any specific authorization for data transfers. The ECJ’s decision in the Schrems case heightened the standards for adequacy decisions by establishing that third countries need a level of protection which is ‘essentially equivalent’ to that in the EU. Again, these heightened standards are now codified in the GDPR. In its opinion on the bilateral agreement between the EU and Canada on Passenger Name Record (PNR), the ECJ obliged the EU to renegotiate the agreement because it did not provide sufficient protection. The Court thereby reaffirmed that it does not hesitate to impose its data protection standards to the EU’s external relations. The pending Google v. CNIL case on the territorial scope of the right to be forgotten is awaiting a judgment from the ECJ, but the A-G has provided his opinion. Whereas the A-G does not advice in favor of a global application of the right to be forgotten, which would create serious enforcement issues and geopolitical clashes, he does ‘not exclude that there could be situations in which the interest of the Union calls for the application of the provisions of Directive 95/46 outside of the territory of the Union.’

The EU’s norm-shaper position in data protection and data security can serve as an example for the norm-shaper role it seeks to have on all matters in cyberspace, including cybersecurity. Cybersecurity certification and standards for the security of 5G networks would be excellent areas in which to play a similar role. To do so, it is paramount that certification is made mandatory as soon as possible, as suggested in Recital 92 of the Cybersecurity Act, and that the joint EU toolbox on the security of 5G networks provides tangible standards which guarantee a sufficient level of data security.

and repealing Directive 95/46/EC (General Data Protection Regulation). The right to be forgotten is also codified in article 17 of the GDPR.

43 Article 3, article 13(1)(f), article 45(1) Regulation (EU) 2016/679.
44 European Court of Justice, Case C-362/14 “Maximillian Schrems v Data Protection Commissioner,” October 6, 2015.
45 Article 45(1) Regulation (EU) 2016/679.
46 Opinion of Advocate-General Szpunar, January 10, 2019, supra n 4, para. 62.
47 See, for the EU’s commitment to pushing cybersecurity norms, for example the Cybersecurity Strategy stating that the EU shall “Support the development of norms of behaviour and confidence building measures in cybersecurity.” JOIN (2013) 1 final (Brussels, February 7, 2013), p. 16.
2. First Pillar: Single Market

The internal market rationale and its predominance in the EU’s approach to cybersecurity has led to a situation in which the core of the EU’s cybersecurity regulatory framework is founded upon the Union’s legal mandate to regulate the internal market, article 114 TFEU. This mandate is also the source of most vast body of European law to date. As noted by Wessel, the extensive competences of the Union in the internal market have provided several ‘hooks’ to harmonize or approximate legislation relating to cybersecurity with the aim of smoothening the functioning of the internal market.48 As the foundational cornerstone of the European Union, internal market regulation generally also enjoys the most widely shared political support. Moreover, the sheer size of the single market as the largest single market in the world has been identified as a main cause of the external effects of European law.49 The global regulatory potential of internal market regulation is thus considerable.

A central role in the coordination and governance of EU cybersecurity regulation has been reserved for the European Union Agency for Cybersecurity (ENISA). ENISA supports the EU’s market-coordinating role. It was founded in 2005 on temporary mandates, but its position has been significantly solidified. Its mandate since 2019 includes cybersecurity certification, supporting capacity-building, supporting the drafting of cybersecurity policies and helping implement vulnerability disclosure policies.50

2.1 The Digital Single Market

Cybersecurity is an integral part of the EU’s policy towards the digital economy. As noted, the development of the EU digital economy has been on the Commission’s agenda since 1985. The recent strategy for a Digital Single Market (DSM) reinforces this focus and places the competitiveness of the European’s digital economy high on the agenda. The urgency thereof was recently addressed by ENISA in the policy paper announcing a policy consultation with the pressing title ‘EU ICT Industrial Policy: Breaking the Cycle of Failure’.51 ENISA emphasizes the interlinkage of the ICT industry and

---

cybersecurity and notes that the EU is an ‘ICT taker rather than an ICT maker’, ‘sandwiched’ between the U.S. and China.\(^{52}\) The same diagnosis accounts for the European market for cybersecurity products: the EU is a net importer of cybersecurity products and largely dependent upon non-European suppliers.\(^{53}\)

The DSM was presented in 2015 as a key priority of the Juncker Commission’s political agenda.\(^{54}\) Economic growth is consistently cited as the main underlying reason for the DSM, envisioning potential additional growth of EUR 250 billion over the course of the Commission’s mandate.\(^{55}\) A DSM is defined as “one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence”.\(^{56}\) This essentially entails achieving the elimination of internal borders in the digital economy. Despite the cross-border nature of the internet itself, digital economic activity in the EU is still very much compartmentalized across national borders.\(^{57}\) The DSM strategy includes no less than 30 legislative initiatives, 28 of which have been concluded.\(^{58}\) Core initiatives have addressed the obstacles formed by geo-blocking,\(^{59}\) online payments,\(^{60}\) the portability of online content\(^{61}\) and diverging regulatory frameworks regarding data protection,\(^{62}\) copyright\(^{63}\) and electronic communication.\(^{64}\)

Cybersecurity is instrumental to the DSM. The more connected the European digital economy, the more vulnerable it is to cyber threats – a network is only as strong as its weakest link.\(^{65}\) In its market-coordinating role, the EU aims to increase the resilience

---


of internal market as a whole as well as vitalize the single market for cybersecurity products and services. These objectives are mutually complementary: a reinforced European market for cybersecurity products will help facilitate greater resilience, whilst businesses abiding by higher cybersecurity standards will rely more heavily on the European cybersecurity market. Resilience in the CSS refers to ‘the capacities of any technical or natural system to regulate itself’.\textsuperscript{66} In the DSM, resilience means creating minimum standards for cybersecurity and mandatory cyber-hygiene measures for businesses and service operators.\textsuperscript{67} The EU employs regulatory as well as industrial strategies to achieve resilience. Its regulatory strategy focuses on improving cybersecurity standards for all digital products and networks and creating the regulatory framework – a ‘level playing field’ – necessary for a single market for cybersecurity. Cybersecurity certification is essential to both ends. The EU’s industrial strategy focuses on helping develop the industrial and technological resources necessary for cybersecurity by strategically investing in the competitiveness of the EU’s digital and cybersecurity industry and pooling training and expertise.\textsuperscript{68}

### 2.2 Towards a Cyber-resilient Regulatory Framework

The 2016 NIS Directive\textsuperscript{69} was the first piece of horizontal EU legislation on cybersecurity and aims to install a minimum level of security with network and information systems to smoothen the functioning of the internal market.\textsuperscript{70} The NIS directive prescribes security and notification requirements for operators of essential services and digital service providers.\textsuperscript{71} Adherence to these requirements is to be supervised by the competent authorities in Member States.\textsuperscript{72} Whereas the societal function of essential services is obvious, the prescription of security norms and obligations for digital service providers is justified by the internal market rationale, i.e. the dependence of businesses and in extension the functioning of the internal market on digital services.\textsuperscript{73} The Directive is, however, less rigid in its approach to the much broader category of digital services.

\textsuperscript{66} JOIN (2013) 1 final (Brussels, February 7, 2013).
\textsuperscript{68} JOIN (2013) 1 final (Brussels, February 7, 2013), 12
\textsuperscript{69} Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
\textsuperscript{70} Article 1 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
\textsuperscript{71} Recitals 49-54 Directive (EU) 2016/1148.
\textsuperscript{72} Recitals 19 and 59-61 Directive (EU) 2016/1148.
\textsuperscript{73} Recital 48 explains that “The security, continuity and reliability of the type of digital services referred to in this Directive are of the essence for the smooth functioning of many businesses. A disruption of such a digital service could prevent the provision of other services which rely on it and could thus have an impact on key economic and societal activities in the Union. Such digital services might therefore be of crucial importance for the smooth functioning of businesses that depend on them and, moreover, for the participation of such businesses in the internal market and cross-border trade across the Union.”
service providers than in its approach to operators of essential services, which Member States are tasked with identifying. This difference can be justified by the societal function of essential services but becomes more nuanced when essential services or public administration are heavily dependent upon digital services, in which case the Directive suggests further contractual security obligations. In addition, Member States must develop a national cyber security strategy as well as create national computer security incident response teams (CSIRTs). A network of CSIRTs is created at Union level. The implementation deadline of the NIS Directive passed in May 2018. At the time of writing, the NIS Directive has not yet been (fully) transposed in Belgium, Bulgaria, Hungary and Luxembourg. This is despite considerable efforts of the Commission to aid Member States in the implementation.

The Cybersecurity Act was adopted in 2019 and presents a significant step forward in the EU’s approach to cybersecurity. The regulation finally introduced the legal basis to adopt an EU-wide cybersecurity certification scheme for ICT products. Rather detailed provisions on the adoption of such a scheme and provisions that should be included are provided. ENISA will play a central role and prepare a candidate certification scheme, for which an ad hoc working group is currently being assembled. The relevance of an EU-wide certification scheme should not be underestimated. Internally, certification schemes can significantly increase the security of IT products and services and allow customers to make informed decisions, boosting market trust and decreasing costs - disparities in national certification schemes have so far led to fragmentation and higher costs. Externally, an EU-wide certification scheme would put the EU in a stronger position to push for global norms on the security of ICT products. However, the Cybersecurity Act is not as bold as it could have been. The certification schemes provided for will not be made mandatory, although the option of mandatory standards is set out to be explored. This is a missed opportunity, as voluntary approaches are expected to have a limited reach and mandatory standards have much greater potential benefits.
to be externalized to non-EU markets. Furthermore, the Act renewed and expanded ENISA’s now permanent mandate and increased its budget and capacity.

In 2018, the Commission put forward a Proposal for a Regulation for the dissemination of terrorist content online. The Regulation would establish a responsibility with internet platforms to take down terrorist content within one hour and establish a positive obligation to detect content and prevent it from reappearing. The EU Fundamental Rights Agency (FRA) expressed concern that the definition of terrorist content is broader than the definition in the Framework Decision on terrorism and is at odds with the freedom of expression. The Proposal sets out that the Regulation aims to ‘guarantee the smooth functioning of the Digital Single market’, but it was also presented as a legislative priority of the Security Union in the 2018 State of the Union speech by Juncker. The Regulation thereby illustrates the strong interrelation of the Digital Single Market and the Security Union.

2.2.1 Soft Law Instruments

Several soft law instruments complement regulatory initiatives by incorporating cybersecurity concerns into market regulation and industrial policy. One example is the sector-specific recommendations on cybersecurity in the energy sector.

The Commission has also started to formulate an EU-wide approach to the cybersecurity of 5G networks. Following its 2016 Action Plan, heated debate in the European Parliament and concern in the European Council, the Commission published a Recommendation on the cybersecurity of 5G networks. 5G networks will provide the building block of much of the Union’s digital infrastructure of the coming decade, but EU ICT businesses are not the strongest competitors on the market for 5G technology. The EU has defied U.S. requests to blankly ban Chinese companies from participating in the auction to establish 5G structures, which would stand at odds with its consistent commitment to a free and open trade policy. The Commission’s Recommendation is clear in stating that not only technical, but also other factors can influence cybersecurity risks of 5G networks, amongst which “the overall risk of influence by a third country, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data
protection”, hinting at the U.S. and China. The Commission aims to assemble a common EU Toolbox to address the cybersecurity risks connected to 5G networks before 31 December 2019, based on risk assessments by Member States and ENISA’s threat landscape mapping. The extent to which Member States succeed in developing a common approach to the 5G question will prove an important test for the strategic autonomy of the EU on the global digital stage.

2.2.2 Strategic Investments

The digital market and cybersecurity are prominently featured in the Digital Europe and Horizon Europe programs. Both programs have been provisionally agreed upon as part of the EU’s long-term (2021-2027) Multiannual Financial Framework, which is still being negotiated. The first ever Digital Europe program will invest in digital capacity and infrastructure building and lists cybersecurity and trust as one of its five priorities. EUR 2 billion is reserved for “boosting cyber defence and the EU’s cybersecurity industry, financing state-of-the-art cybersecurity equipment and infrastructure as well as supporting the development of the necessary skills and knowledge”. Horizon Europe is a renewal of Horizon 2020, the broader research and innovation program within the EU budget. Cybersecurity is not listed as such in the Horizon Europe proposal, but the program does set out to reinforce technological and industrial capacities under the Global Challenges and Industrial Competitiveness pillar, for which EUR 52.7 billion is reserved. Recently, the Commission declared that EUR 135 million will be made available under Horizon Europe for cybersecurity projects by citizens and SMEs.

The Commission has proposed the establishment of a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centers to more specifically steer the efforts to rejuvenate the European cybersecurity sector. The Centre would implement the allocation of funding for cybersecurity provided under the Horizon Europe and Digital Europe programs by taking into account the whole cybersecurity value chain. It will focus on the cooperation between cybersecurity supply and demand chains, civilian and military efforts, Member States and research and industrial communities and strive for the deployment of the latest cybersecurity-technology.

100 Recital 20 COM (2019) 2335 final (Brussels, March 26, 2019).
106 The legal bases for the establishment of the Centre are the EU’s competences for research and innovation and competitiveness (articles 187 and 173 TFEU). COM (2018) 630 final (Brussels, September 12, 2018).
The lacking human capital of the EU’s ICT market is a key concern to the EU’s competitiveness. A substantial increase in human development is desired and could be facilitated by harmonized training and curricula, but the EU’s lack of competences in the field of education makes this challenging.\(^\text{108}\) A tentative first step is made within the European Cybersecurity Industrial, Technology and Research Competence Centre, which sets out to support education policy makers to create the expertise necessary for a European cybersecurity market.\(^\text{109}\) Moreover, based on CSDP provisions a European Security and Defence College brings together, on a voluntary basis, Member States and academic expertise to train CSDP employees on amongst others cybersecurity.\(^\text{110}\)

It remains to be seen exactly which industrial agenda the incoming Von der Leyen Commission will present. The European Commission’s digital department has in any case given clear directions in its proposal for a Digital Leadership Package in a leaked internal Commission document dated July 2019.\(^\text{111}\) The Package with a ‘strong geostrategic aspect’ would revamp the EU’s industrial policy and build towards the much-cited, elusive term ‘strategic autonomy’.\(^\text{112}\) It would fix investment priorities such as European high-level computing capacities and processor technologies, a research and investment roadmap for technologies such as 5G and 6G, a blockchain infrastructure for public services as well as a European Cybersecurity Shield based on quantum technologies. The package is proposed alongside an update and revision of the e-Commerce Directive, an Action plan to make the ICT sector more sustainable and an AI regulatory framework including a single market legal instrument that ‘should set a world-standard for AI regulation’. Digital competitiveness and cyber-resilience will be top priorities to the Von der Leyen Commission.

---


\(^\text{111}\) Directorate-General for Communications Networks, Content and Technology. The leaked document was obtained by Politico. See Laurens Cerulus and Bjarke Smith-Meyer, “Commission pitched ‘leadership package’ for digital autonomy”, Politico Pro, August 22, 2019, https://www.politico.eu/pro/commission-pitched-leadership-package-for-digital-autonomy/?utm_source=POLITICO.EU&utm_campaign=d6d64f016-EMAIL_CAMPAIGN.2019_08_22.10_54&utm_medium=email&utm_term=0_10959edeb5-d6d64f016-190421257


“In March 2018, a two-year long cybercrime investigation between the Romanian National Police and the Italian National Police, with the support of Europol, its J-CAT and Eurojust, led to the arrest of 20 suspects in Romania and Italy over a banking fraud which netted EUR 1 million from hundreds of customers of two major banking institutions. The OCG, comprised largely of Italian nationals, used spear phishing emails impersonating tax authorities to harvest the online banking credentials of their victims.”

Cybercrime is an economic risk to the EU. Cybersecurity is a measure to avert this risk and increase investors’ and consumers’ trust in the internal market. Drastically reducing cybercrime is the second policy aim in the CSS and has been an objective since 2005. The EU’s action on cybercrime legally falls within the Area of Freedom, Security and Justice (AFSJ). The AFSJ is joined by most Member States and provides no basis for the harmonization of criminal law, merely for the approximation of national

---

114 Cybercrime is not comprehensively defined in European law, but only in the Cyber Security Strategy, as criminal activity using information systems or computers as a primary means and/or a target. Proxies, i.e. private criminal actors without reported ties to state actors, non-state actors, are reportedly used by states. JOIN (2013) 1 final (Brussels, February 7, 2013), 3.
116 JOIN (2013) 1 final (Brussels, February 7, 2013), p. 4; the first legislative instrument on cybercrime was Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.
117 The creation of an AFSJ was one of the objectives of the EU as noted in article 3(2) TEU and was realized by the 1999 Tampere Council. The AFSJ is regulated in Title V, Chapters 2-5 of the TFEU and became fully effective on December 1, 2014. The AFSJ encompasses the Schengen acquis, i.e. the elimination of all internal borders, and includes the establishment of common policies on border checks, asylum, immigration, judicial cooperation in civil and criminal matters and police cooperation. The AFSJ is an area of shared competence following Article 4(2)(j) TFEU and is subject to the regular legislative procedure, save for some exceptions which require unanimity in the Council. The requirement of unanimity applies to modifications of article 77(3) TFEU; article 81(3) TFEU; article 82(2)(d) TFEU; the identification of the areas of serious crime prescribed in article 83(1) TFEU; article 86(1) TFEU; article 87(3) TFEU and article 89 TFEU.
118 The AFSJ accommodates opt-out possibilities for the UK, Ireland and Denmark and opt-in possibilities for non-Member States which are part of the Schengen area (Norway, Iceland, Switzerland and Liechtenstein).
law by prescribing minimum rules on certain areas of serious crime, including cyber-
crime. Consequently, the centre of gravity of integration in the AFSJ lies with judicial
and law enforcement matters, although recent proposals do include issues of proce-
dural criminal law. The establishment of Europol and EC3, Eurojust, OLAF and, since
recently, EPPO have helped facilitate this cooperation. Europol in particular has ma-
tured into an important point of coordination for law enforcement in the EU and has
functioned as the platform for several cooperative initiatives on cybercrime.

3.1 The Security Union

In recent years, legislative developments regarding cybersecurity within the AFSJ have
been boosted by the economic imperative to combat cybercrime as reinforced by the
DSM strategy and the fortified security narrative of the EU as propagated in the Security
Union. The Juncker Commission in 2015 published its European Agenda on Security
(EAS) which frames cross-border threats, amongst which cybercrime, as a European
task which must be responded to by the deepening of European cooperation. In
2016, the Commission followed up on the EAS by announcing the creation of "an effec-
tive and genuine" Security Union on the legal basis of the AFSJ. The Security Union
illustrates the political momentum for European security cooperation after the terror
attacks in Brussels, Madrid, London, Copenhagen and Paris. The Security Union ad-
vanced the implementation of the EAS and drew particular attention to its cohesion,
identifying and addressing implementation gaps. Speedy and significant process has
been made on the Security Union agenda so far, primary amongst which has been the
appointment of a European Commissioner for Security specifically tasked with the im-
plementation of the EAS.

The Security Union explicitly interweaves domestic and foreign policy and the internal
and external dimension of security. This is not unsurprising considering the dis-
inctly hybrid nature of the threats addressed by the Security Union agenda (alongside
cybercrime also counter-terrorism, organized crime and exchange of information). By
significantly expanding the external dimension of security in the AFSJ, the EU is effec-
tively equating the 'Security' in 'Security and Defence' with that in 'Freedom, Security
and Justice', thereby circumventing the constitutional obstacles to moving forward on

119 These areas are identified in article 83(1) TFEU. The Treaty refers to computer crime.
120 The legal basis for this cooperation are the provisions on mutual recognition and judicial cooperation, articles
81 to 84 TFEU.
121 The establishment of an EPPO is fairly recent. It is based on article 86 TFEU and has been realized by means of
Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establish-
ment of the European Public Prosecutor’s Office (the EPPO).
122 Elaine Fahey, “The EU’s cybercrime and cyber-security rulemaking: mapping the internal and external dimen-
124 Article 67(3) TFEU.
125 COM (2016) 230 final (Brussels, April 20, 2016). A notable novelty of the Security Union is also the consistent
reporting on its implementation, which draws particular attention to implementation gaps and inconsistencies. Prog-
ness reports and a track-record of legislative efforts can be consulted at European Commission, “European
Agenda on Security – Legislative Documents,” European Commission, https://ec.europa.eu/home-affairs/what-
we-do/policies/european-agenda-security/legislative-documents_en
the CSDP. The AFSJ was transformed from an isolated domestic policy area on justice and home affairs to the legal basis for a European narrative on security in the comprehensive sense of the word. The Security Union as a political agenda thereby also signals the growing approval of European cooperation on security issues.

3.2 Substantive Cybercrime Norms

The Council of Europe Convention on Cybercrime (also termed Budapest Convention) is the main point of reference for the EU's efforts towards combating cybercrime. The Convention continues to serve as the primary source of norms the Commission continues to promote internally and externally.

The Treaty basis for minimum rules has been employed a number of times for cybersecurity legislation. A Directive on the sexual exploitation of children online has been in place for some time. The 2013 Directive on Attacks against Information Systems explicitly builds on and largely reproduces the norms and definitions in the Budapest Convention and criminalizes a sparse number of basic cyber-offences and minimum penalties. More advanced cybercrimes such as identity theft and, interestingly, attacks against information systems, are excluded. The Directive enables sanctions against natural and legal persons. The EU has with the Directive effectively bypassed the hesitance in some Member States to ratify the Convention. Further legislative progress has been made on criminal provisions on fraud and forgery in cashless media. The Commission in 2017 proposed a directive which would establish minimum rules on the fraudulent use of (non-corporeal) non-cash payment instruments, which includes virtual currencies such as bitcoin. The directive also sets out to improve the exchange of information and cooperation between criminal-justice authorities. It accounts for all initiatives that the Treaty only allows for the adoption of Directives, which prescribe minimum rules and requires subsequent adoption into national law.

132 Recital 15 Directive 2013/40/EU.
133 Included offences are illegal access to information systems, system interference, data interference and interception.
135 Article 2(c) Directive 2013/40/EU.
136 Ireland and Sweden have as of yet not ratified the Convention.
139 Article 288 TFEU.
concern of disparities between Member States and delayed implementation is therefore inevitable and further harmonization is desired.  

3.3 Law Enforcement Cooperation

Cooperation between national law enforcement authorities is currently the most effective answer to the prevalence of cross-border cybercrime in a borderless digital internal market. Effective law enforcement is also vital to the thorny question of attribution. Europol since 2013 composes of a Cybercrime Centre (EC3) specifically dedicated to the investigation of cyber offences. EC3 aims to be the focal point for the criminal investigation of cyber offences in the EU. Within EC3, the Member-State led joint cybercrime action taskforce (J-CAT) has been praised for effectively enabling joint cross-jurisdictional investigations under flexible administrative conditions.

EC3 faces challenges in the legislative and institutional conditions under which it operates. First, it has to align its operations with other institutional cybersecurity actors such as Eurojust and ENISA. Secondly and primarily, several legislative and technical obstacles formed by the patchwork of national jurisdictions continue to obstruct digital forensic opportunities. EC3 highlights the fact that investigative leads are lost because joint investigations lack timely access to communication data and other e-evidence. The 2014 Directive on European Investigative Orders (EIO Directive) regulates this issue to some extent but does not eliminate all problems. For example, a provision on e-evidence is lacking. In April 2018, the Commission put forward a proposal for an “e-evidence” regulation. Interestingly, the Council had urged the Commission to do so – a novelty in the field of criminal justice, signalling increasing willingness on the part of Member States to give in on sovereignty concerns in the face of cyber threats. Another novelty is the choice for a regulation, which is a more tangible legal instrument than a directive. In addition to the Regulation, the Commission is pushing for EU participation in the multilateral negotiations on a Protocol on e-evidence to the Budapest

141 Annegret Bendiek, “The EU as a Force for Peace in International Cyber Diplomacy,” SWP Comment No. 19, April, 2018, p. 8.
147 The legal basis for the Regulation is article 82(1) TFEU, which has not previously been used for the proposal of Regulations. See also Vanessa Franssen, “The European Commission’s e-evidence proposal: toward an EU-wide obligation for service providers to cooperate with law enforcement?” European Law Blog, October 12, 2018, https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/
Convention as well as preparing for the formal launch of a bilateral EU-US agreement on cross-border access to electronic evidence under the auspices of the Council of Europe Convention on Cybercrime.\textsuperscript{149}

4. Third Pillar: CSDP

Cyber defence is the primary component of cybersecurity to only a few Member States. The development of a cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP) is one of the strategic aims of the EU’s Cyber Security Strategy. The realization of this aim presents an institutional challenge: any initiative in the CSDP has to navigate several constitutional limitations and widespread political reluctance due to national sovereignty concerns. The ‘progressive framing’ of a CSDP which ‘might lead’ to a common defence is legally only a subcategory of the Common Foreign and Security Policy (CFSP). Consequently, the EU’s abilities in the defence domain have so far remained limited to “exhorting, facilitating, and incentivising”. The European Defence Agency (EDA) has a coordinating role. There are no standing European military forces or headquarters and NATO remains the main focal point for European defence cooperation. A full-fledged political Defence Union can only be established unanimously by the European Council. This decision has not been taken, although it has notably been called for by the European Parliament in 2016. The Commission has partly circumvented the constitutional limitations of the CSDP by progressing the Security Union based on AFSJ provisions and proposing the European Defence Fund based on internal market-related provisions. The support for the Defence Union has in recent years caused an increase of initiatives in the cyber defence domain. In turn, cybersecurity has been one of the drivers of the current political momentum for security and defence integration in the EU. At their core, however, cyber defence initiatives still primarily serve the industrial development of the European defence market.

4.1 Mutual Defence Clause

One key development for cyber defence has been the renewed interpretation of the EU ‘solidarity clause’ (article 222 TFEU). The solidarity clause is different than and additional to the ‘mutual defence clause’ (article 42(7) TEU). The latter strongly resembles and is complementary to article 5 of the NATO Treaty, which legitimizes military action on behalf of all signatories in the case of an armed attack against just one. Both the

150 Article 24(1) and article 42(1) TEU. The CFSP was very carefully introduced in the 1992 Treaty of Maastricht and gradually developed with subsequent treaty revisions. The basis for the CFSP and the CSDP is article 4(2) TFEU and the areas are regulated in Title V (articles 21-46) of the TEU. The Treaties keep foreign policy matters relatively separate from other policy areas and EU institutions and only tentatively provides for a CSDP.
152 Article 42(3) TEU and article 45 TEU.
154 Article 41(2) TEU.
mutual defence clause and article 5 of the NATO Treaty refer to national military action in the case of physical, armed attacks. The solidarity clause legitimizes action by both the Union and Member States. The latter means, following the adoption of rules and procedures to enable the operation of the solidarity clause, ‘any situation which may have a severe impact on people, the environment or property’. The solidarity clause thus includes a joint response in case of cyberattacks.

4.2 Common Defence Cooperation

A common cyber defence policy has in recent years been called for by the European Council, EU military staff, EDA, the High Representative, the European Parliament and the EU and NATO jointly. The European Council in 2014 agreed on a Cyber Defence Policy Framework, which was updated in 2018. The framework prioritizes capacity-building. It focuses on building cyber defence capacities in Member States and providing steering principles for cooperation with the private sector, as well as enhancing the protection of CSDP communication networks. Within the EDA, a plethora of smaller projects have been set up to improve cyber defense, amongst which a Collaboration Database (CoDaBa) and a Capability Development Plan (CDP). Following the 2016 Joint Framework on countering hybrid threats, several scenario-based policy discussions have taken place under the Finnish Council Presidency.

Only in December 2017, 25 Member States finally made use of the permanent structured cooperation (PESCO) Treaty provision which allows for a flexible integration under the CDSP. The establishment of PESCO is a remarkable development and, by some, seen as the most opportune pathway to promote EU defence integration. Within PESCO, Member States can initiate joint defence cooperation projects, which may then voluntarily be joined by interested Member States. There are currently 34

157 Article 3(a) of Council Decision 2014/415/EU.
159 The adoption of a Cyber Defence Policy Framework was, in fact, proposed by the EDA, the High Commissioner and the Commission jointly.
161 NATO, Cyber Defence Pledge (Warsaw, July 8, 2016).
165 Other projects by EDA include the Deployable Cyber Evidence Collection and Evaluation Capacity (DCEC), the Cyber Situation Awareness Package (CySAP), the Cyber Defence Training & Exercises Coordination Platform (CD TEXP) and the “Demand Pooling for the Cyber Defence Training and Exercise support by the private Sector” (DePoCyTE).
166 JOIN (2016) 018 final (Brussels, April 6, 2019).
167 PESCO is based on article 46(2) TEU.
PESCO projects, out of which 12 have specifically been dedicated to cyber-defence. At the same time, NATO remains the main focal point for European cyber defence cooperation in Europe.¹⁷¹ Cooperation between the EU and NATO has intensified, by introducing a Cyber Defence Pledge¹⁷² and resulting in joint projects on early-warning capabilities for headquarters and a multi-agent system for Advanced Persistent Threat detection (MASFAD).¹⁷³

4.3 Common Defence Investment

It was the Commission that proposed a European Defence Fund in June 2017. Interestingly, the legal basis for the EDF were the Treaty articles for industry and development, illustrating the close interrelationship of cyber defence and the internal market – a conclusion which is underlined by the fact that the proposal was marked a 'text with EEA relevance'.¹⁷⁴ Under the EDF, the Commission intends to allocate annual budget to joint research in defence technologies, as well as enable the joint procurement of military materials, of which the Commission estimates that it would save around 100 billion euros per year.¹⁷⁵ Under the 2021-2027 Multiannual Financial Framework, the EDF is set out to amount to EUR 500 million per year.¹⁷⁶ Within this budget, which is still being negotiated, the most recent Commission proposals include a EUR 182 million investment in cyber situational awareness and a EUR 27 million investment in AI, virtual reality and cyber technologies.¹⁷⁷ In addition, EDA has started cooperating with the European Investment Bank.¹⁷⁸ The EDF and other initiatives to stimulate investment in defence measures present a much-needed impulse to the EU’s cybersecurity defence industry. However, again, these initiatives are economic at heart. Rather than substantial legal and political defence integration, the EU’s strength lies in the regulation and stimulation of the defence industry.

¹⁷² NATO, Cyber Defence Pledge (Warsaw, July 8, 2016).
5. Fourth Pillar: CFSP

Besides the CSDP discussed above, the CFSP includes all matters of foreign policy, although foreign trade, including foreign trade agreements, is an area of exclusive competence under the Common Commercial Policy. The European Council, acting unanimously, is the primary actor in the CFSP. In tandem with the Council it identifies strategic interests, assembles common policies and takes concrete decisions. The option to adopt legislation based on the CFSP is legally excluded, making Council decisions the Union’s most tangible instrument on foreign affairs. However, foreign policy concerns have increasingly permeated other domains of Union legislation, which has led to the adoption of legislative proposals which are in effect instrumental towards the CFSP. The implementation of the CFSP is overseen by the High Representative and in practice realized by the European External Action Service (EEAS), which includes 139 European delegations in third states.

5.1 Cyber Diplomacy Toolbox

Following its declared and continuous commitment to multilateralism, the EU has devotedly participated in UNGGE talks, pushing forward the standards adopted under the Budapest Convention. Since UNGGE negotiations were halted without results in 2017, some signal a move towards ‘coalitions of the willing’, i.e. the acceptance of a more scattered approach in which willing international partners enhance cyber cooperation. Nevertheless, several Member States remain heavily invested in UNGGE talks, providing a counterweight against the “Open-Ended Working Group” initiated by Russia. Like global counterparts, the EU has also maintained bilateral cyber dialogues with the U.S., Canada, China, Japan, South Korea and others.

179 Article 3(1)(e) and Part V, Title II TFEU.
180 Article 24(1) TFEU and article 26 TFEU.
181 Article 24(1) TFEU, article 25 TFEU and article 31 TFEU.
182 Article 26 TFEU.
183 Annegret Bendiek, “The EU as a Force for Peace in International Cyber Diplomacy,” SWP Comment No. 19, April, 2018.
The EU’s approach to cybersecurity under the CFSP has in 2017 been streamlined by the adoption of the Cyber Diplomacy Toolbox. The Toolbox has the potential to function as a model for diplomatic responses to cybersecurity issues. The EU distinguishes five categories of responses: preventative, cooperative, stabilising and restrictive. These responses are complementary to the lawful responses for Member States’ self-defence based on national constitutions and the NATO legal framework.

Part of the Cyber Diplomacy Toolbox is the Council Regulation on a sanctions regime adopted in May 2019, which prescribes the freezing of funds and economic resources of any natural or legal person, entity or body responsible for (attempted) cyber-attacks with a (potentially) significant effect. The sanctions regime also codifies the principle of due diligence, by making explicit the Member State’s positive obligation to take the necessary measures to prevent the passing of natural persons involved in cyberattacks through their territories.

In the run-up to the European Parliament elections of May 2019, risks that disinformation campaigns would influence the outcome of the elections urged the creation of platforms and common standards. The Action Plan against Disinformation presents an agreement between Member States, whereas the Code of Practice against Disinformation is a joint commitment of the Commission, online platforms and other signatories. The Rapid Alert System, which was set up to coordinate the responses to disinformation in the EU election campaigns, will be evaluated in autumn 2019. A European Cooperation Network on Elections joined by the relevant national authorities will contribute to this evaluation. The establishment of cooperation the EU Internet Forum aims to further complement the cooperation between Member States and online platforms by enabling the dialogue between Home Affairs ministers, the internet industry and other stakeholders.

5.2 Cybersecurity Concerns in Foreign Trade

The cohesion of the EU’s cybersecurity approach has been enhanced by introducing cybersecurity considerations in foreign trade legislation. Within the Common Commercial Policy, the recently adopted Foreign Direct Investment (FDI) Regulation provides a first step towards EU cooperation on investment screening. It allows the Commission to issue opinions on the security or public order implications of certain investments and promotes coordination on international investments between Member States. In addition, following increased awareness of the strategic importance of

---

187 Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. The sanctions regime is based on article 215 TFEU which allows for the adoption of restrictive measures.
dual-use goods to cyber threats, the Regulation on expert controls for dual-use goods was updated in 2018.


6. Conclusion

“If current trends continue unmitigated, the EU may end up being entirely dependent on third countries for key technologies. This would leave our economy, security and society exposed and vulnerable on an unprecedented scale. [...] Importantly, it can also threaten our democracies.”

“Member States or individual companies cannot cope with this challenge alone. There is need for coordination and strategic vision.”

The political agenda of the incoming Von der Leyen Commission and the Commission’s digital department’s proposal for a Digital Leadership Package are paving the way for digital industrial development and cyber-resilience to be the key political priorities to the EU in coming years.

Without a clear constitutional basis, the EU has employed an internal market rationale and increasingly incorporated security and fundamental rights considerations to build towards its cybersecurity approach. Cybersecurity as a policy concern has quickly ascended to the top of the EU’s political agenda and managed to deepen European integration in the politically sensitive areas of security and defence. Single market harmonization and industrial policy projects are now complemented with legislative instruments to diminish the economic risks of cybercrime, a stimulus for the European defence industry and tentative steps towards formulating common foreign policy responses to cyber threats. Nevertheless, in spite of the broadening of the policy incentives to deal with cybersecurity, the locus of the EU’s approach to cybersecurity remains with the regulation and securing of the internal market.

A forward regulatory framework on all digital questions – data protection, cybersecurity, AI et cetera – is a double-edged European law sword. On the one hand, it serves to protect European citizens with the high level of data security and fundamental rights protection that the EU prides itself on. In turn, digital questions and cybersecurity in particular have substantially pushed this level of protection. On the other hand, a coherent digital and cyber security regulatory framework is an imperative requirement for the European single market to benefit from the transition to the digital age – as fragmentation obstructs cross-border economic activity – as well as for a single market for ICT and cybersecurity products to catch up on its competitiveness. Moreover, much of the EU’s geostrategic strength lies on its regulatory power and the externalization of its

norms and values. Similar to its strength in data protection cybersecurity could turn out to be success story of the next "geopolitical Commission" from 2019 to 2024.

**Dr Annegret Bendiek** is Senior Associate in the Research Division EU/Europe

**Eva Pander Maat** was an intern in the Research Division EU/Europe

© Stiftung Wissenschaft und Politik, 2019

All rights reserved.

This Working Paper reflects the author's views.

**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
7. Annex

**Table**

Cyber Security in the EU: Areas of Responsibility

<table>
<thead>
<tr>
<th></th>
<th>Single market</th>
<th>AFSJ: Area of Freedom, Security and Justice</th>
<th>CSDP: Cyber Defence</th>
<th>CFSP: Cyber Diplomacy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EU</strong></td>
<td>ENISA</td>
<td>Europol (EC3)</td>
<td>EDA</td>
<td>EEAS</td>
</tr>
<tr>
<td></td>
<td>CSIRT network</td>
<td>Eurojust</td>
<td>GSA</td>
<td>SIAC (EU INTCEN, EUMS INT)</td>
</tr>
<tr>
<td></td>
<td>CERT-EU</td>
<td>EU-LISA</td>
<td>ESDC</td>
<td>EU SITROOM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>EU Hybrid Fusion Cell</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ERCC</td>
</tr>
<tr>
<td><strong>National</strong></td>
<td>Authorities in charge of NIS</td>
<td>Executive and data-protection authorities</td>
<td>Defence, military and security agencies</td>
<td>Foreign ministries</td>
</tr>
<tr>
<td></td>
<td>National CSIRTs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>