Working Paper
SWP Working Papers are online publications within the purview of the respective Research Division. Unlike SWP Research Papers and SWP Comments they are not reviewed by the Institute.

SWP

RESEARCH DIVISION EU / EUROPE | WP NR. 02, OCTOBER 2019

The EU's Regulatory Approach to Cyber-security

Annegret Bendiek and Eva Pander Maat

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Contents

1.

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

[1] European Cybercrime Centre, *Internet Organized Crime Assessment 2017* (The Hague: European Union Agency for Law Enforcement, 2017)
[2] European Cybercrime Centre, *Internet Organized Crime Assessment 2017* (The Hague: European Union Agency for Law Enforcement, 2017)
[3] European Cybercrime Centre, *Internet Organized Crime Assessment 2018* (The Hague: European Union Agency for Law Enforcement, 2018)
[4] European Cybercrime Centre, *Internet Organized Crime Assessment 2017* (The Hague: European Union Agency for Law Enforcement, 2017)
[5] European Cybercrime Centre, *Internet Organized Crime Assessment 2018* (The Hague: European Union Agency for Law Enforcement, 2018)
[6] European Cybercrime Centre, *Internet Organized Crime Assessment 2018* (The Hague: European Union Agency for Law Enforcement, 2018)
[7] European Cybercrime Centre, *Internet Organized Crime Assessment 2017* (The Hague: European Union Agency for Law Enforcement, 2017)
[8] Annegret Bendiek and Magnus Römer, "Externalizing Europe: the global effects of European data protection." *Digital Policy, Regulation and Governance* 21, no. 1 (2019): 32-43, p. 37.

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.[9] 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).[10]The EU has broad legislative competences to regulate the single market.[11] In contrast, its competences in the AFSJ are mainly restricted to matters of law enforcement.[12] 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.[13]

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,[14] 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.[15] Cybersecurity forms an integral part of the DSM as

[9] Article 43(1) TFEU does allow for the adoption of Council Decisions. See also Ramses A. Wessel, "Cybersecurity in the European Union: Resilience through Regulation?" in *Routledge Handbook of EU Security Law and Policy* ed. Elena Conde Pérez (London/New York: Routledge, 2019).

[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.

[14] Patryk Pawlak, "The EU's Role on Shaping the Cyber Regime Complex", *European Foreign Affairs Review* 24, iss. 2 (2019): 167-186, pp. 169.

[15] Jean-Claude Juncker, "A new start for Europe: My agenda for jobs, growth, fairness and democratic change. Political guidelines for the next European Commission. Opening statement in the European Parliament plenary session" *European Commission* July 15, 2014,
https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech_en.pdf

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.[16] 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) [17] 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.[18] 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.[19] 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. [20] 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.[21] 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, [22] 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'[23] and features as a common thread through all domains of the EU's cybersecurity

[16] European Political Strategy Centre, "Towards a 'Security Union': Bolstering the EU's counter-terrorism response" *European Commission* April 20, 2016, https://ec.europa.eu/epsc/publications/strategic-notes/towards-%E2%80%98security-union%E2%80%99_en
[17] JOIN (2013) 1 final (Brussels, February 7, 2013).
[18] Robert Scott Dewar, *Cyber security in the European Union: an historical institutionalist analysis of a 21st century security concern*, PhD diss. (University of Glasgow, 2017), pp. 125.
[19] COM (85) 310 final (Milan, June 14 1985).
[20] Robert Scott Dewar, *Cyber security in the European Union: an historical institutionalist analysis of a 21st century security concern*, PhD diss. (University of Glasgow, 2017).
[21] COM (2015) 192 final (Brussels, May 6, 2015), pp. 12-13.
[22] JOIN (2013) 1 final (Brussels, February 7, 2013); SWD (2017) 295 final (Brussels, September 13, 2017); JOIN (2017) 450 final (Brussels, September 13, 2017).
[23] Annegret Bendiek, "A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience", *SWP Research Paper* No. 11, October, 2017, p. 6.

policy, as well the 2016 Global Strategy.[24] To the EU, "security begins internally".[25] 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.[26] 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.[27] 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[28] 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.[29] 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.[30] 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

[24] European External Action Service, "Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy", June, 2016 http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
[25] Annegret Bendiek, "A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience", *SWP Research Paper* No. 11, October, 2017, p. 14.
[26] Annegret Bendiek, "A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience", *SWP Research Paper* No. 11, October, 2017, p. 14.
[27] Helen Carrapico and Andre Barrinha, "The EU as a Coherent (Cyber) Security Actor?" *JCMS* 55, no. 6. (2017): 1254–1272; Annegret Bendiek, "Europe's Patchwork Approach to Cyber Defence Needs a Complete Overhaul" *Council on Foreign Relations*, August 30, 2017,
https://www.cfr.org/blog/europes-patchwork-approach-cyber-defense-needs-complete-overhaul
[28] The Charter of Fundamental Rights of the European Union.
[29] Article 19 TEU.
[30] Article 2 TEU.

law.[31] 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,[32] 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.[33] Notably, the ECJ focused on the Directive's secondary objective: that of security.[34] This focus illustrates that the suitability of article 114 as a legal basis can be questioned,[35] 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.[36] 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.[37] The ECJ's decision in the Google Spain case established the 'right to be forgotten'. [38] 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.[39] 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.[40] 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).[41]

[31] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Recitals 2 and 3.

[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.

[35] Orla Lynskey, "The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland," *Common Market Law Review* 51, (2014): 1789–1812.

[36] European Court of Justice, Joined Cases C-293/12 and C-594/12 "Digital Rights Ireland, April 8, 2014, para 71.

[37] European Court of Justice, Joined Cases C-203/15 and C-698/15 "Tele2 and Watson," December 21, 2016.

[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.

[40] McKay Cunningham, "Diminishing Sovereignty: How European Privacy Law Became International Norm", *Santa Clara Journal of International Law* 11, no. 2 (2013): 421-453, p. 440.

[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.[42] 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.[43] 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.[44] Again, these heightened standards are now codified in the GDPR.[45] 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.'[46]

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.[47] 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.

[42] Anu Bradford, "The Brussels Effect," *Nw. U. L. Rev.* 107 No. 1, (2013); Annegret Bendiek and Magnus Römer, "Externalizing Europe: the global effects of European data protection." *Digital Policy, Regulation and Governance* 21, no. 1 (2019): 32-43.

[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

[48] Ramses A. Wessel, "Cybersecurity in the European Union: Resilience through Regulation?" in *Routledge Handbook of EU Security Law and Policy* ed. Elena Conde Pérez (London/New York: Routledge, 2019).
[49] Anu Bradford, "The Brussels Effect" *Nw. U. L. Rev.* 107 No. 1, (2013).
[50] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[51] ENISA, "ENISA puts out EU ICT Industrial Policy paper for consultation," *European Agency on Cybersecurity*, July 10, 2019, https://www.enisa.europa.eu/news/enisa-news/enisa-puts-out-eu-ict-industrial-policy-paper-for-consultation

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

[52] ENISA, "Consultation Paper – EU ICT industrial policy: breaking the cycle of failure," *European Agency on Cybersecurity*, July, 2019, pp. 1-2.

[53] COM (2018) 630 final (Brussels, September 12, 2018), p. 1.

[54] COM (2015) 192 final (Brussels, May 6, 2015).

[55] Jean-Claude Juncker, "A new start for Europe: My agenda for jobs, growth, fairness and democratic change. Political guidelines for the next European Commission. Opening statement in the European Parliament plenary session," *European Commission,* July 15, 2014, https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech_en.pdf, p. 6.

[56] COM (2015) 192 final (Brussels, May 6, 2015), p. 3.

[57] Dariusz Adamski, "Lost on the Digital Platform: Europe's Legal Travails with the Digital Single Market", *Common Market Law Review* 55, (2018): 719–752.

[58] European Commission, "Shaping the Digital Single Market" *European Commission*, https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market

[59] Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC (Text with EEA relevance.).

[60] Directive 2015/2366 of the European Parliament and of the Council of 25 Nov. 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) 1093/2010, and repealing Directive 2007/64/EC, O.J. 2015, L 337/35.

[61] Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market.

[62] 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

[63] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

[64] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast).

[65] COM (2017) 0228 final (Brussels, May 10, 2017).

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'.[66] In the DSM, resilience means creating minimum standards for cybersecurity and mandatory cyber-hygiene measures for businesses and service operators.[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. [68]

2.2 Towards a Cyber-resilient Regulatory Framework

The 2016 NIS Directive[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.[70] The NIS directive prescribes security and notification requirements for operators of essential services and digital service providers.[71] Adherence to these requirements is to be supervised by the competent authorities in Member States.[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.[73] The Directive is, however, less rigid in its approach to the much broader category of digital

[66] JOIN (2013) 1 final (Brussels, February 7, 2013).
[67] Annegret Bendiek, Raphael Bossong and Matthias Schulze, "The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges" *SWP Comment* No. 47, November, 2017, p. 3.
[68] JOIN (2013) 1 final (Brussels, February 7, 2013), 12
[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.
[70] Article 1 Directive (EU) 2016/1148. A very tentative predecessor of the NIS Directive could be seen in the European Critical Infrastructure Protection Directive (Council Directive 2008/114/EC) of which the effectiveness has recently been reviewed by the Commission.
[71] Recitals 49-54 Directive (EU) 2016/1148.
[72] Recitals 19 and 59-61 Directive (EU) 2016/1148.
[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, [74] which Member States are tasked with identifying.[75] 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.[76] In addition, Member States must develop a national cyber security strategy as well as create national computer security incident response teams (CSIRTs).[77] A network of CSIRTs is created at Union level.[78] 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.[79] This is despite considerable efforts of the Commission to aid Member States in the implementation.[80]

The Cybersecurity Act was adopted in 2019 and presents a significant step forward in the EU's approach to cybersecurity.[81] The regulation finally introduced the legal basis to adopt an EU-wide cybersecurity certification scheme for ICT products.[82] Rather detailed provisions on the adoption of such a scheme and provisions that should be included are provided.[83] ENISA will play a central role and prepare a candidate certification scheme, for which an ad hoc working group is currently being assembled.[84] 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.[85] 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.[86] 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.[87] This is a missed opportunity, as voluntary approaches are expected to have a limited reach and mandatory standards have much greater potential

[74] Recital 49, for example, makes explicit that "the security requirements for digital service providers should be lighter"; recital 57 sets out that "this Directive should take a differentiated approach with respect to the level of harmonisation in relation to those two groups of entities. For operators of essential services, Member States should be able to identify the relevant operators and impose stricter requirements than those laid down in this Directive. Member States should not identify digital service providers, as this Directive should apply to all digital service providers within its scope."
[75] Recitals 19-25, article 5 Directive (EU) 2016/1148.
[76] Recital 54 Directive (EU) 2016/1148.
[77] Articles 7 and 9 Directive (EU) 2016/1148.
[78] Article 12 Directive (EU) 2016/1148.
[79] European Commission, "State-of-play of the transposition of the NIS Directive", *European Commission* https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive
[80] COM/2017/0476 final (Brussels, October 10, 2017).
[81] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
[82] Article 46 Regulation (EU) 2019/881.
[83] Articles 47-49 and article 54(1)(a)-(v) Regulation (EU) 2019/881.
[84] ENISA, "Call for expression of interest for the first ad hoc working group on cybersecurity certification," *ENISA*, August 6, 2019, https://www.enisa.europa.eu/news/enisa-news/call-for-expression-of-interest-for-the-first-ad-hoc-working-group-on-cybersecurity-certification
[85] Recital 67 Regulation (EU) 2019/881.
[86] Annegret Bendiek, Raphael Bossong and Matthias Schulze, "The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges" *SWP Comment* No. 47, November, 2017, p. 4.
[87] Recital 92 Regulation (EU) 2019/881

to be externalized to non-EU markets. [88] Furthermore, the Act renewed and expanded ENISA's now permanent mandate and increased its budget and capacity.[89]

In 2018, the Commission put forward a Proposal for a Regulation for the dissemination of terrorist content online.[90] 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. [91] 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.[92] The Proposal sets out that the Regulation aims to 'guarantee the smooth functioning of the Digital Single market',[93] but it was also presented as a legislative priority of the Security Union in the 2018 State of the Union speech by Juncker.[94] 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.[95]
The Commission has also started to formulate an EU-wide approach to the cybersecurity of 5G networks. Following its 2016 Action Plan,[96] heated debate in the European Parliament[97] and concern in the European Council[98] the Commission published a Recommendation on the cybersecurity of 5G networks.[99] 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

[88] Annegret Bendiek, Raphael Bossong and Matthias Schulze, "The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges" *SWP Comment* No. 47, November, 2017, p. 4.
[89] Recitals 18-64 and articles 9-12 Regulation (EU) 2019/881.
[90] COM (2018) 640 final (Brussels, September 12, 2018).
[91] COM (2018) 640 final (Brussels, September 12, 2018).
[92] European Parliament, "Preventing the dissemination of terrorist content online", *European Parliament Legislative train schedule: Area of justice and fundamental rights*, September, 2018, http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-preventing-the-dissemination-of-terrorist-content-online
[93] COM (2018) 640 final (Brussels, September 12, 2018).
[94] Jean-Claude Juncker, "State of the Union 2018: The Hour of European Sovereignty, Authorised version of the State of the Union Adress 2018" *European Commission*, September, 2018, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en_0.pdf
[95] SWD (2019) 1240 final (Brussels, April 3, 2019).
[96] COM (2016) 588 final (Brussels, September 14, 2016).
[97] European Parliament, Resolution 2019/2575 (RSP) (Strasbourg, March 12, 2019).
[98] Council of the European Union, "European Council conclusions of 21 and 22 March 2019," 1/19 (Brussels, March 22, 2019).
[99] COM (2019) 2335 final (Brussels, March 26, 2019).

protection",[100] 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.[101] 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.[102]

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".[103] 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.[104] Recently, the Commission declared that EUR 135 million will be made available under Horizon Europe for cybersecurity projects by citizens and SMEs.[105]

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.[106] 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.[107]

[100] Recital 20 COM (2019) 2335 final (Brussels, March 26, 2019).
[101] COM (2019) 2335 final (Brussels, March 26, 2019).
[102] Barbara Lippert, Nicolai von Ondarza and Volker Perthes, "European Strategic Autonomy: Actors, Issues, Conflicts of Interests," *SWP Research Paper* No. 04, March, 2019.
[103] European Commission, "Press release: EU budget: Commission proposes €9.2 billion investment in first ever digital programme", *European Commission*, June 6, 2018,
https://europa.eu/rapid/press-release_IP-18-4043_en.htm
[104] European Commission, "Press release: EU budget for 2021-2027: Commission welcomes provisional agreement on Horizon Europe, the future EU research and innovation programme", *European Commission*, March 20, 2019,
https://europa.eu/rapid/press-release_IP-19-1676_en.htm
[105] COM (2019) 353 final (Brussels, July 24, 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).
[107] COM (2018) 630 final (Brussels, September 12, 2018), pp. 4-5.

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. [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.[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.[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. [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'.[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.

[108] Annegret Bendiek, Raphael Bossong and Matthias Schulze, "The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges" *SWP Comment* No. 47, November, 2017, pp. 3-4.
[109] COM (2018) 630 final (Brussels, September 12, 2018), p. 4.
[110] Council Joint Action 2005/575/CFSP (Brussels, July 18, 2005).
[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=d6d644f016-EMAIL_CAMPAIGN_2019_08_22_10_54&utm_medium=email&utm_term=0_10959edeb5-d6d644f016-190421257
[112] Barbara Lippert, Nicolai von Ondarza and Volker Perthes, "European Strategic Autonomy: Actors, Issues, Conflicts of Interests," *SWP Research Paper* No. 04, March, 2019; Ulrike Franke and Tara Varma, "Independence Play: Europe's Pursuit of Strategic Autonomy", *European Council on Foreign Relations*, July, 2019.

3. Second Pillar: The Area of Freedom, Security and Justice (AFSJ)

> "*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*."[113]

Cybercrime is an economic risk to the EU.[114] Cybersecurity is a measure to avert this risk and increase investors' and consumers' trust in the internal market.[115] Drastically reducing cybercrime is the second policy aim in the CSS and has been an objective since 2005.[116] The EU's action on cybercrime legally falls within the Area of Freedom, Security and Justice (AFSJ).[117] The AFSJ is joined by most Member States[118] and provides no basis for the harmonization of criminal law, merely for the approximation of national

[113] European Cybercrime Centre, *Internet Organized Crime Assessment 2018* (The Hague: European Union Agency for Law Enforcement, 2018)

[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.

[115] Under the challenge "Security" for a Single European Information Space, the Commission listed ""making internet safer from fraudsters, harmful content and technology failures to increase trust amongst investors and consumers". See COM (2005) 229 (Brussels, June 1 2005), p. 5, also quoted in Robert Scott Dewar, *Cyber security in the European Union: an historical institutionalist analysis of a 21st century security concern*, PhD diss. (University of Glasgow, 2017), p. 152.

[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 Lichtenstein).

law by prescribing minimum rules on certain areas of serious crime, including cybercrime.[119] Consequently, the centre of gravity of integration in the AFSJ lies with judicial and law enforcement matters,[120] although recent proposals do include issues of procedural criminal law. The establishment of Europol and EC3, Eurojust, OLAF and, since recently, [121] EPPO have helped facilitate this cooperation. Europol in particular has matured into an important point of coordination for law enforcement in the EU and has functioned as the platform for several cooperative initiatives on cybercrime.[122]

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.[123] In 2016, the Commission followed up on the EAS by announcing the creation of "an effective and genuine" Security Union on the legal basis of the AFSJ.[124] 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 advanced the implementation of the EAS and drew particular attention to its cohesion, identifying and addressing implementation gaps.[125] 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 implementation of the EAS.

The Security Union explicitly interweaves domestic and foreign policy and the internal and external dimension of security.[126] This is not unsurprising considering the distinctly 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 effectively 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 establishment 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 dimensions of EU security," *European Journal of Risk Regulation* 5, no. 1 (2014): 46-60.
[123] COM (2015) 185 final (Strasbourg, April 28, 2015).
[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. Progress reports and a trackrecord 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
[126] COM (2015) 185 final (Strasbourg, April 28, 2015), p. 4; James Sperling, and Mark Webber, "The European Union, security governance and collective securitization," *West European politics* 42, no. 2 (2019): 228–260.

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.[127] The Security Union as a political agenda thereby also signals the growing approval of European cooperation on security issues.[128]

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.[129]

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.[130] The 2013 Directive on Attacks against Information Systems[131] explicitly builds on and largely reproduces the norms and definitions in the Budapest Convention[132] and criminalizes a sparse number of basic cyber-offences[133] and minimum penalties.[134] More advanced cybercrimes such as identity theft and, interestingly, attacks against information systems, are excluded. The Directive enables sanctions against natural and legal persons.[135] The EU has with the Directive effectively bypassed the hesitance in some Member States to ratify the Convention.[136] 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 a on the fraudulent use of ((non-)corporeal) non-cash payment instruments, which includes virtual currencies such as bitcoin.[137] The directive also sets out to improve the exchange of information and cooperation between criminal-justice authorities.[138] 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.[139] The

[127] Ester Herlin-Karnell, *The Constitutional Structure of Europe's Area of 'Freedom, Security and Justice'and the Right to Justification* (Bloomsbury Publishing: 2019), p. 4; Hendrik Hegemann and Ulrich Schneckener, "Politicising European security: from technocratic to contentious politics?" *European Security* 28 no. 2 (2019): 133-152, p. 140.

[128] Annegret Bendiek, "A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience", *SWP Research Paper* No. 11, October, 2017, pp. 16-17.

[129] Patryk Pawlak, "The EU's Role on Shaping the Cyber Regime Complex", European Foreign Affairs Review 24, iss. 2 (2019): 167-186.

[130] Directive 2011/93/EU replacing Council Framework decision 2004/68/JHA.

[131] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[132] Recital 15 Directive 2013/40/EU.

[133] Included offences are illegal access to information systems, system interference, data interference and interception.

[134] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[135] Article 2(c) Directive 2013/40/EU.

[136] Ireland and Sweden have as of yet not ratified the Convention.

[137] COM (2017) 0489 final - 2017/0226 (COD) (Brussels, September 13, 2017).

[138] Recital 24-27 and article 15 COM (2017) 0489 final - 2017/0226 (COD) (Brussels, September 13, 2017).

[139] Article 288 TFEU.

concern of disparities between Member States and delayed implementation is therefore inevitable and further harmonization is desired.[140]

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.[141] 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.[142]

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.[143] 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.[144] The 2014 Directive on European Investigative Orders (EIO Directive) [145] regulates this issue to some extent but does not eliminate all problems.[146] For example, a provision on e-evidence is lacking. In April 2018, the Commission put forward a proposal for an "e-evidence" regulation.[147] 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.[148] 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

[140] Annegret Bendiek, Raphael Bossong and Matthias Schulze, "The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges" *SWP Comment* No. 47, November, 2017, p. 5.
[141] Annegret Bendiek, "The EU as a Force for Peace in International Cyber Diplomacy," *SWP Comment* No. 19, April, 2018, p. 8.
[142] George Christou, "The collective securitisation of cyberspace in the European Union," *West European Politics* 42, no. 2 (2019): 278-301, pp. 292-293; George Christou, "The challenges of cybercrime governance in the European Union," *European Politics and Society* 19, no. 3 (2018): 355-375; Tuesday Reitano, Troels Oerting and Marcena Hunter, "Innovations in international cooperation to counter cybercrime: The joint cybercrime action taskforce." *The European Review of Organised Crime* 2, no. 2 (2015): 142-154.
[143] Annegret Bendiek, Raphael Bossong and Matthias Schulze, "The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges" *SWP Comment* No. 47, November, 2017, p. 3.
[144] IOCTA 2017, 13
[145] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.
[146] George Christou, "The challenges of cybercrime governance in the European Union," *European Politics and Society* 19, no. 3 (2018): 355-375.
[147] COM (2018) 225 final (Brussels, April 17, 2018).
[148] 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.[149]

[149] European Commission, "Factsheet: Questions and answers: mandate for the second additional protocol to the Budapest Convention" *European Commission*, February 5, 2019, https://europa.eu/rapid/press-release_MEMO-19-865_en.htm

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).[150] Consequently, the EU's abilities in the defence domain have so far remained limited to "exhorting, facilitating, and incentivising".[151] The European Defence Agency (EDA) has a coordinating role.[152] There are no standing European military forces or headquarters and NATO remains the main focal point for European defence cooperation.[153] A full-fledged political Defence Union can only be established unanimously by the European Council.[154] This decision has not been taken, although it has notably been called for by the European Parliament in 2016.[155] 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.[156] 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 CDSP 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 onlytentatively provides for a CSDP.
[151] Sven Biscop, "Oratio pro pesco," *Egmont Paper* No. 91, January, 2017, p. 3.
[152] Article 42(3) TEU and article 45 TEU.
[153] Annegret Bendiek, "A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience", *SWP Research Paper* No. 11, October, 2017, p. 6. See also article 41(2) TEU.
[154] Article 41(2) TEU.
[155] Resolution 2016/2067 (INI), European Parliament (Strasbourg, 23 November 2016).
[156] Annegret Bendiek, "A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience", *SWP Research Paper* No. 11, October, 2017.

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'.[157] 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,[158] EU military staff, EDA, the High Representative,[159] the European Parliament[160] and the EU and NATO jointly.[161] The European Council in 2014 agreed on a Cyber Defence Policy Framework, [162] which was updated in 2018.[163] 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. [164] 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).[165] Following the 2016 Joint Framework on countering hybrid threats,[166] 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.[167] The establishment of PESCO is a remarkable development[168] and, by some, seen as the most opportune pathway to promote EU defence integration.[169] Within PESCO, Member States can initiate joint defence cooperation projects, which may then voluntarily be joined by interested Member States.[170] There are currently 34

[157] Article 3(a) of Council Decision 2014/415/EU.
[158] Council of the European Union, "EU Cyber Defence Policy Framework", 15585/14 (Brussels, November 18, 2014).
[159] The adoption of a Cyber Defence Policy Framework was, in fact, proposed by the EDA, the High Commissioner and the Commission jointly.
[160] European Parliament, Resolution 2016/2067 (INI) (Strasbourg, November 23, 2016).
[161] NATO, Cyber Defence Pledge (Warsaw, July 8, 2016).
[162] Council of the European Union, "EU Cyber Defence Policy Framework", 15585/14 (Brussels, November 18, 2014).
[163] Council of the European Union, "EU Cyber Defence Policy Framework (2018 update)", 14413/18 (Brussels, November 19, 2018).
[164] Council of the European Union, "EU Cyber Defence Policy Framework", 15585/14 (Brussels, November 18, 2014).
[165] Other projects by EDA include the Deployable Cyber Evidence Collection and Evaluation Capacity (DCEC^2), 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.
[168] Steven Blockmans, "T*he EU's modular approach to defence integration: An inclusive, ambitious and legally binding PESCO*?" *Common Market Law Review* 55, (2018): 1785–1826; Editorial Comments, "A stronger Common Foreign and Security Policy for a self-reliant Union?*" Common Market Law Review* 55, (2018): 1675–1684.
[169] Nicole Koehnig and Marie Walter-Franke, "France and Germany: Spearheading a European Security and Defence Union?" *Policy Paper Jacques Delors Institut* No. 202, July, 2017.
[170] Council Decision 2017/2315 (Brussels, December 8, 2017).

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 Pledge[172] 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.

[171] Annegret Bendiek, "A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience", *SWP Research Paper* No. 11, October, 2017, p. 6. See also article 41(2) TEU.
[172] NATO, Cyber Defence Pledge (Warsaw, July 8, 2016).
[173] Annegret Bendiek, "A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience", *SWP Research Paper* No. 11, October, 2017, p. 20.
[174] Articles 173(3), 182(4), 183 and 188(2) TFEU. Editorial Comments, "A stronger Common Foreign and Security Policy for a self-reliant Union?*" Common Market Law Review* 55, (2018): 1675–1684.
[175] European Commission, "Factsheet: The European Defence Action Plan – FAQs," *European Commission*, November 30, 2016, https://europa.eu/rapid/press-release_MEMO-16-4101_en.htm
[176] Annegret Bendiek, "A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience", *SWP Research Paper* No. 11, October, 2017, p. 18.
[177] European Commission, "Press Release: European Defence Fund," *European Commission*, March 19, 2019, https://ec.europa.eu/commission/news/european-defence-fund-2019-mar-19_en
[178] European Defence Agency, "Press Release: European Defence Agency and European Investment Bank Sign Cooperation Agreement," *European Defence Agency*, February 28, 2018, https://www.eda.europa.eu/info-hub/press-centre/latest-press-releases/2018/02/28/european-defence-agency-and-european-investment-bank-sign-cooperation-agreement>

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.[179] 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.[180] The option to adopt legislation based on the CFSP is legally excluded, making Council decisions the Union's most tangible instrument on foreign affairs.[181] 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.[182]

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.[183] 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.[184] Nevertheless, several Member States remain heavily invested in UNGGE talks, providing a counterweight against the "Open-Ended Working Group" initiated by Russia.[185] 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 22(1), article 24(1) TEU and article 26 TEU.
[181] Article 24(1) TEU, article 25 TEU and article 31 TEU.
[182] Article 26 TEU.
[183] Annegret Bendiek, "The EU as a Force for Peace in International Cyber Diplomacy," *SWP Comment* No. 19, April, 2018.
[184] Patryk Pawlak, "The EU's Role on Shaping the Cyber Regime Complex", European Foreign Affairs Review 24, iss. 2 (2019): 167-186.
[185] The OEWG will report back to the UN General Assembly in 2020, the UNGGE's agenda is planned for the period 2019-2021. See Resolution adopted by the General Assembly on 5 December 2018 [on the report of the First Committee (A/73/505)], United Nations General Assembly,
https://undocs.org/en/A/RES/73/27;
Resolution adopted by the General Assembly on 22 December 2018 [on the report of the First Committee (A/73/505)], United Nations General Assembly,
https://undocs.org/en/A/RES/73/266

The EU's approach to cybersecurity under the CFSP has in 2017 been streamlined by the adoption of the Cyber Diplomacy Toolbox.[186] 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.[187] 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.[188]

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,[189] whereas the Code of Practice against Disinformation is a joint commitment of the Commission, online platforms and other signatories.[190] 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[191] 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.[192] In addition, following increased awareness of the strategic importance of

[186] Council of the European Union, "Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")," 10474/17 (Brussels, June 19, 2017).
[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.
[188] Article 4 Council Regulation (EU) 2019/796.
[189] JOIN (2018) 36 final (Brussels, December 5, 2018).
[190] COM (2018) 236 final (Brussels, April 26, 2018).
[191] Regulation 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union.
[192] European Commission, "Press release: EU foreign investments screening regulation enters into force," *European Commission*, April 10, 2019,

dual-use goods to cyber threats,[193] the Regulation on expert controls for dual-use goods was updated in 2018.[194]

https://europa.eu/rapid/press-release_IP-19-2088_en.htm

[193] SWD (2017) 295 final (Brussels, September 13, 2017), p. 45; JOIN (2017) 450 final (Brussels, September 13, 2017), pp. 10, 13, 17.

[194] Commission Delegated Regulation (EU) 2018/1922 of 10 October 2018 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items

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.*"[195]

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

[195] 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=d6d644f016-EMAIL_CAMPAIGN_2019_08_22_10_54&utm_medium=email&utm_term=0_10959edeb5-d6d644f016-190421257

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.

7. Annex

Table

Cyber Security in the EU: Areas of Responsibility

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

EC3: European Cybercrime Centre, *CSIRT:* Computer Security Incident Response Team, *CERT:* Computer Emergency Response Team, *EDA:* European Defence Agency, *ESDC:* European Security and Defence College, *EEAS:* European External Action Service, *ENISA:* European Union Agency for Network and Information Security, *ERCC:* Emergency Response Coordination Centre, *EU INTCEN:* European Union Intelligence and Situation Centre, *EU-LISA:* European Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice, *EU SITROOM:* Europe-an Union Situation Room, *EUMS INT:* European Union Military Staff, Intelligence Directorate Mission, *GSA:* European Global Navigation Satellite Systems Agency, *NIS:* Network and Information Security, *SIAC:* Single Intelligence Analysis Capacity

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

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

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