Heibrock, Marlien:

The European Union´s Approach to Cybersecurity Exploring and Explaining Variation in the EU´s Regulatory and Capacity-Building Approach to Cybersecurity

Masterarbeit, Wintersemester 2025

Gutachter*in: Rittberger, Berthold

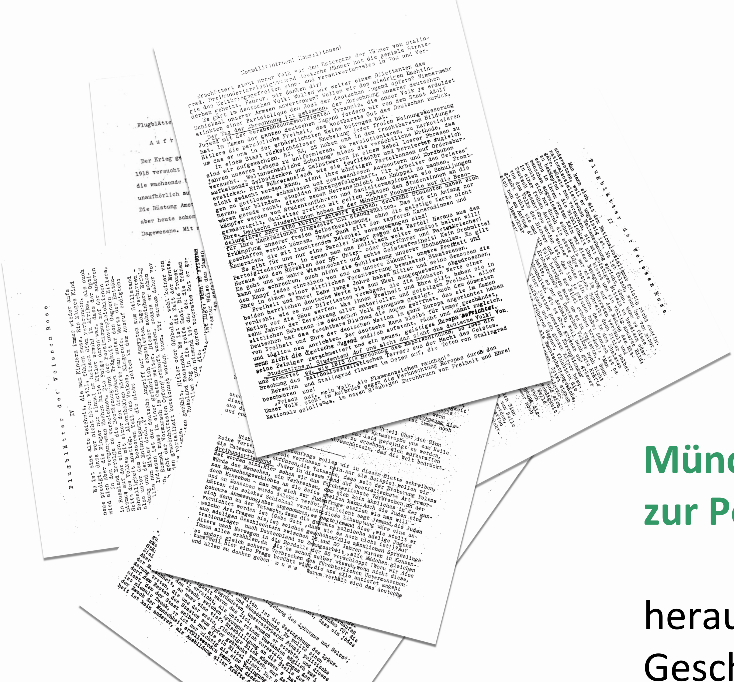
Sozialwissenschaftliche Fakultät
Geschwister-Scholl-Institut für Politikwissenschaft
Politikwissenschaft

Ludwig-Maximilians-Universität München

https://doi.org/10.5282/ubm/epub.125306

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

GESCHWISTER-SCHOLL-INSTITUT
FÜR POLITIKWISSENSCHAFT



Münchener Beiträge
zur Politikwissenschaft

herausgegeben vom
Geschwister-Scholl-Institut
für Politikwissenschaft

2025

Marlien Heibrock

The European Union's Approach to Cybersecurity. Exploring and Explaining Variation in the EU's Regulatory and Capacity-Building Approach to Cybersecurity.

Masterarbeit bei
Prof. Dr. Berthold Rittberger
2025

Dedication

I would like to dedicate my master thesis to my parents.
I am grateful for their endless support throughout my academic journey.

Abstract

The EU's activity in policy areas that are associated with core state power areas has been observed by several scholars. Policy areas such as security that conventionally fall within the realm of the state are also addressed by the EU. Cybersecurity as a digital security domain has so far not been explored from the perspective of core state power integration in a comprehensive way. The EU's cybersecurity landscape indicates variation *within* the instruments of core state power integration instruments. Differentiating between regulation and capacity-building offers a starting point in exploring the EU's role in cybersecurity. But considering the role of hard and soft law as well as the role of new EU bodies such as agencies and networks as well as direct and indirect capacity-building initiatives point towards different ways how the EU responds to demands for cybersecurity integration. How can this variation be explained? As the master thesis claims the role of EU actors in decision-making concerning regulation and capacity-building and the way cybersecurity dimensions are linked to EU competences can provide answers to this question. Understanding cybersecurity as one of the EU's integration efforts allows to assess the different forms of these integration steps and the implications of the EU's sectoral approach to cybersecurity. Understanding the EU's role in cybersecurity is of relevance when considering the cross-border nature of cybersecurity and the increasing geopolitical relevance of cyberspace.

Keywords: Cybersecurity; core state power integration; EU security; regulation; capacity-building; hard law; soft law; agencies; networks.

Table of contents

Abbreviations

CEPOL	The European Union Agency for Law Enforcement
CERT-EU	Computer Emergency Response Team for the European Union
CFSP	Common Foreign and Security Police
Commission	European Commission
Council	European Council
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incidence Response Team
ECA	European Court of Auditors
ECI	European Critical Infrastructure
ECCC	European Cybersecurity Competence Centre
ECJ	European Court of Justice
EC3	European Cybercrime Center
EDA	European Defence Agency
EDF	European Defence Fund
EP	European Parliament
EU-CyCLONe	European Cyber Crises Liaison Organization Network
ICT	Information and Communications Technology
JHA	Justice and Home Affairs
PESCO	Permanent Structured Cooperation
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

List of tables and figures

1. Introduction

“Virtual attacks threatening critical infrastructure, government institutions and personal data form one of the key challenges to security policy in the 21st century.” (Bendiek 2012, 5). Cyber-attacks have become more common and sophisticated (Odermatt 2018). The EU’s Member States and institutions are increasingly targets of cyber-attacks (Balser & Krüger 2024; European Commission 2009; European Parliament 2021; Odermatt 2018). The large-scale cyber-attack on Estonia in 2007 (Barrinha & Carrapico 2016), the Russian state-sponsored hacking operations targeting the German Bundestag in 2017 (Odermatt 2018) and the Social Democratic Party of Germany in 2023 (Balser & Krüger 2024) as well as the French election campaign in 2017 (Odermatt 2018), cyber-attacks on the European Commission (Odermatt 2018) and most recently the suspected sabotage over undersea cables in the Baltic Sea (Sytas et al. 2024) illustrate the scope and (geo)political relevance of cyber-attacks in the EU.

As a consequence, the EU has developed several cybersecurity strategies over the years. Cybersecurity “commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure” (European Commission 2013b, 3). The aim is “to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein” (ibid.) by developing “technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access.” (Dunn Cavelty 2014, 702).

Cybersecurity is a multifaceted, cross-border phenomenon that covers occurrences and risks of different nature (Carrapico & Barrinha 2017; European Commission 2013b; Odermatt 2018). As the EU faces an increase in cyber-attacks (European Commission 2009; European Parliament 2021), cybersecurity “has become a top priority for the EU” (Dunn Cavelty & Smeets 2023, 1330). The EU’s activities encompass “the protection of critical information systems and infrastructures from cyber-attacks, the prevention and investigation of cybercrime, and cyber defence.” (Carrapico & Farrand 2020, 1111).

Considering the borderless nature of cyber risks and threats “an effective national response […] require[s] EU-level involvement” (European Commission 2013b, 17). The EU seeks to “position itself as an important addition to member states’ efforts” (Shepherd 2022, 154) in cybersecurity. The master thesis focuses “policy-making activities in European security” (Kruck & Weiss 2023, 2). In particular the master thesis is interested in cybersecurity, a new security field that is primarily driven by technological progress but that is also usually considered to remain a national responsibility. Even though security is one of the core functions of the state (Kruck & Weiss 2023; Majone 1997), the EU became active in security policy fields such as cybersecurity which "is now central to the EU's integration efforts" (Carrapico & Farrand 2020, 1111).

The EU's activity in the area of cybersecurity represents a case of core state power integration. Conventionally, European (cyber)security is thought of to reside only in the 'positive state' (Kruck & Weiss 2023, Majone 1997). However, a European cybersecurity landscape has evolved which now encompasses a wide range of approaches. How does the EU approach a policy area that touches upon core state powers? Most prominently are regulatory and capacity-building approaches. But as will be demonstrated variation within each approach exists. Soft and hard rules are part of the EU's regulatory approach and new institutional actors such as agencies and networks as well as direct and indirect initiatives form part of the EU's approaches to cybersecurity. The master thesis is interested in exploring and explaining the variation in the EU's approach to cybersecurity. Thus, the underlying research question to the master thesis is: *How can the variation in the EU's regulatory and capacity-building approach to cybersecurity be explained?*

Answers to this question should help to shed light on how the EU approaches cybersecurity, a cross-border phenomenon that necessitates cooperation while also touching upon core constitutive features of the state. This is of relevance considering the increase of cyber-attacks targeted at the EU and the (geo)political relevance of cyberspace. The master thesis aims to contribute to the core state power integration and EU (cyber)security literature. For answering the research question the master thesis draws on to the 'core state power integration' theoretical framework by Genschel & Jachtenfuchs (2014). It further seeks to expand certain theoretical aspects of the framework in order to account for variation *within* the EU's regulatory and capacity building approaches. Congruence analysis is employed to assess the relevance of the theories contained in the expanded theoretical framework and a comparative case study of selected regulatory and capacity-building approaches in the area of EU cybersecurity is conducted.

The master thesis proceeds as follows. First, a state of the art situates the research question into the broader context and reflects on the boundaries of the research. In order to gain an overview of the different approaches, a mapping of the EU's cybersecurity landscape follows in a second step. The third part introduces the expanded theoretical framework from which expectations regarding the variation in the EU's approach to cybersecurity are formulated. Next, the method and case selection is presented. The comparative case studies follow. The final chapter summarizes and discusses the main findings, elaborates on implications and gives an outlook for future research.

2. State of the art: Core state power integration and EU cybersecurity

The master thesis places the research question into the context of core state power integration (Genschel & Jachtenfuchs 2014; 2016). Starting point of this research branch is the observation that the EU is increasingly active in policy fields that usually constitute core state power features of states. Thereby the EU moves beyond market regulation and uses regulation and capacity-building for integrating "new, initially exempt policy areas." (Genschel & Jachtenfuchs 2014, 5). The European integration of core state powers proceeds for example in military security (Weiss 2014; Mérand & Angers 2014; Menon 2014), fiscal and monetary policy (Genschel & Jachtenfuchs 2014; 2018), and public administration (Trondal 2014).

So far, the EU's cybersecurity landscape has not been researched as a case of core state power integration. Studies in the area of EU cybersecurity only marginally touch upon core state power integration. Sivan-Sevilla (2023) for example demonstrates with regard to cybersecurity certification the link between market integration and core state power integration. Dunn-Cavelty & Smeets (2023) inquire into ENISA's role in cybersecurity governance in the context of the 'regulatory security state' (Kruck & Weiss 2023) and point towards limits of European cybersecurity integration. The master thesis aims to fil this research gap by providing a comprehensive account of the EU's cybersecurity landscape and the different instruments of core state power integration.

Therefore, it aims to expand the theoretical framework provided by Genschel & Jachtenfuchs (2014). Exploring and explaining variation in the EU's approach to cybersecurity requires to gain detailed knowledge of the regulatory and capacity-building approaches. The master thesis suggests differentiating between hard and soft law (Abbott & Snidal 2000) in the EU's regulatory approach. It therefore acknowledges that EU core state power integration as in the case of cybersecurity proceeds by both legally-binding and non-legally binding acts (Terpan & Saurugger 2020).

When differentiating between capacity-building approaches, the role of agencies and networks as well as direct and indirect capacity-building initiatives can be made. Thereby the master thesis seeks to account for the rise of *de novo* bodies (Bickerton et al. 2016) in "policy areas that constitute core functions of the nation-state" (Egeberg & Trondal 2017, 676).

European (core state power) integration is assumed to increasingly take place in new institutional structures that lay “outside the Commission hierarchy” (Kelemen & Tarrant 2011, 929). Therefore, the master thesis also aims to speak to the agencification literature (Busuioc & Groenleer 2014; Kaunert et al. 2013; Levi-Faur 2011, Wonka & Rittberger 2010; Rittberger et al. 2024) and to connect this strand of literature to the theoretical framework of core state power integration. Further emphasis is put on the role supranational actors and EU Member States can assume in decision-making concerning core state power integration. For the specific case of cybersecurity, it additionally becomes crucial to consider how cyber sub-issues are linked to the different EU areas of competence.

Beside advancing the core state power integration theoretical framework, the master thesis aims to contribute to the general debate evolving around EU cybersecurity governance (Barrinha & Carrapico 2016; Carrapico & Farrand 2018; 2020; 2024; Farrand & Carrapico 2021; 2022). It aims to provide answers to the question *how* cybersecurity is governed in the EU by focusing on the various regulatory and capacity-building approaches. By considering the wide range of the EU’s cybersecurity landscape the master thesis tries to draw a comprehensive picture of the different cybersecurity dimensions while pointing towards the extent and limits of core state power integration as well as to the potentials and limits. Gaining a better understanding of the EU’s approach to cybersecurity is crucial at times where cyberspace is increasingly of geopolitical interest and part of the EU’s quest for ‘digital-sovereignty’ (Carrapico & Farrand 2024).

3. Mapping the EU’s cybersecurity landscape

The EU’s cybersecurity landscape encompasses a wide range of initiatives that evolved over time. As will be shown, cybersecurity has different, over-lapping dimensions ranging from network and information security, critical infrastructure protection to cybercrime, cyberdefence and cyberdiplomacy. The following sections trace the EU’s approach to the different dimensions of cybersecurity. Table 1 and 2 summarize selected regulatory and capacity-building instruments.

3.1. Network and information security

“Network and information security can be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions.“ (European Commission 2001b, 3). The first initiatives regarding network and information security go back to the late 1990s and early 2000s (Christou 2016; Porcedda 2023). In its first communications on network and information security the Commission presented policy measures in order to ensure a safe information society (European Commission 2001a; 2001b). The focus lay on network and information security, data protection and how to enhance security as resilience (Christou 2016; European Commission 2001a; 2001b; Porcedda 2023). The communications for example included the proposal to set up a European warning and information system and to provide support for market orientated standardization and certification (European Commission 2001b).

In 2002, a framework decision on attacks against information systems was proposed by the Council (Council 2002) and adopted in 2005 (Council 2005). The Council decision required Member States to take the necessary measures to secure network and information security. It further required that the illegal access to information systems shall be punishable under criminal law. For better coordination in the area of network and information security, Member States shall establish a point of contact for the exchange of information on offences related to attacks against information systems.

A European Commission green paper on critical infrastructure protection stressed the necessity to involve a broad number of stakeholders for the effective protection of critical infrastructure (Christou 2016; European Commission 2005). Further in 2006, a communication by the Commission outlined an EU strategy for a secure information society to tackle key challenges in network and information security by multi-stakeholder dialogues and building partnerships (European Commission 2006a).

Another communication by the Commission in the same year (European Commission 2006b) contained the aim to ensure the resilience of security and information technology against threats and to reduce vulnerabilities (Christou 2016). Therefore, the Communication "called for the designation and identification of critical infrastructure and measures to protect them" (Shepherd 2022, 149) and the establishment of a critical infrastructure warning information network (Christou 2016; Shepherd 2022). The outlined program "was reflective of hands-off meta-governance through the establishment of various information sharing and coordinative platforms.“ (Christou 2016, 123). Additionally, a Council Directive (Council 2008a) "set out more concrete procedures, mechanisms and platforms for identifying and designating European Critical Infrastructure (ECI) and facilitating reporting, coordination and protection of ECI in these sectors" (Christou 2016, 123).

The European Council report on the implementation of the European security strategy stressed the political dimension of attacks on IT systems (Council 2008a; Porcedda 2023). The report followed after the cyber-attacks against Estonia took place in 2007 (Porcedda 2023). Another communication on the protection from large-scale cyber-attacks (European Commission 2009) emphasized security as resilience and put forward an action plan on how to address key challenges in cybersecurity (Christou 2016; Shepherd 2020). The plan consisted of actions for preparedness, prevention, detection, response, mitigation and recovery (European Commission 2009).

The directive on a common regulatory framework for electronic communications networks and services (European Parliament and Council 2009) made it mandatory for telecommunication operators to report cyber-incidents to the national regulatory authority (Christou 2016; Shepherd 2022). This represents a move away from a voluntary approach (Shepherd 2022). In 2010, a communication of the commission on a 'Digital Agenda for Europe' (European Commission 2010a) followed that entailed actions "to address prevention, detection and response in relation to the challenges presented by network and information security." (Christou 2016, 122).

The European cyber-security strategy from 2013 (Commission 2013) set out different objectives with regard to network and information security, cybercrime and law enforcement in order to pursue coherence in the field of cybersecurity (Christou 2016; Carrapico & Barrinha 2017; Porcedda 2023). With regard to network and information security the communication highlighted the need to identify vulnerabilities of network and information systems to achieve cyber resilience. In addition, the economic safeguarding of the digital single market and the development of industrial and technical resources were addressed in the strategy (Brandão & Camisão 2022; Christou 2016; Porcedda 2023). More generally, the strategy called for optimizing coordination and coherence between the national and EU level across cybersecurity areas.

Subsequently, in 2013 the EP and the Council proposed a directive concerning measures to ensure a high common level of network and information security across the Union (European Parliament & the Council 2013a). The proposal became a formal directive in 2016 (European Parliament & the Council 2016) and represents a "key component underlying the EU's cybersecurity strategy" (Dunn Cavelty-Smeets 2023, 1338). The NIS-Directive is assumed to be "the most optimal option for incentivising governments and businesses to adopt practices that would lead to a more effective security of resilience“ (Christou 2016, 132) through different obligations such as developing and preparing capabilities among Member States, creating IT-security requirements and reporting cyber incidents (Christou 2016; Kipker 2023; Shepherd 2020). Dunn-Cavelty and Smeets (2023) show that the directive required national cybersecurity capacity building activities such as the establishment of a national CSIRTs and the performance of cyberexercises. The directive needed to be transposed into national law: Providers of essential services in critical infrastructure protection and digital service providers are obliged to take adequate IT-security measures and to report any significant cyber incidents to national authorities (Kipker 2023).

In 2017 a new cybersecurity strategy was formulated (European Commission 2017a). Herein contained are different key actions to ensure and improve cyber resilience. Such actions included strengthening ENISAs role, creating effective EU cyber deterrence by enhancing public-private partnerships and improving Member States investigative capabilities. A joint communication from 2020 on the 'EU's Cybersecurity Strategy for the Digital Decade' (European Commission 2020a) attributes new importance to cybersecurity "as an essential international concern underpinning crucial national economic and security interests at a time of geopolitical shifts" (Porcedda 2023, 51). Furthermore, the EU called for technological sovereignty in matters of cybersecurity (Farrand & Carrapico 2022; Porcedda 2023). The Cybersecurity Strategy from 2020 relies on regulation, investment and policies "to adopt measures leveraging incentives, obligations and benchmarks" (Porcedda 2023, 51) in the different areas of cybersecurity and EU law making. The strategy set out different objectives to adapt to new geopolitical challenges in cyberspace. For example, the strategy explores ways to provide an ultra-secure communication infrastructure and internet connectivity.

In 2020, a proposal for a directive on the resilience of critical entities (European Commission 2020b) identified weaknesses in Member State's cyber resilience and suggested to strengthen the obligation for Member States to adopt a cybersecurity strategy, risk management and reporting obligations (Shepherd 2022). Another proposal for a directive (which became the NIS2 directive in 2023) concerning measures for a high common level of cybersecurity across the Union in 2020 (European Commission 2020c) reiterates the importance of reinforcing cyber resilience and proposes measures for adapting to the new cybersecurity landscape. The NIS2-Directive entered into force in 2023 (European Parliament & Council 2022a). It lays out "measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market" (European Parliament & Council 2022a, 2) by formulating obligations for Member States with regard to establishing strategies and competent authorities for cooperation and cyber crisis management. A directive on the resilience of critical entities (European Parliament and Council 2022b) followed that requires Member States to carry out risk assessments and identify critical entities for the sectors of for example energy, transport, financial market infrastructure and health (European Commission

2023b). The identified critical entities have to take measures to enhance their resilience (European Commission 2023b).

In 2023, the Institutional Cybersecurity Regulation (European Parliament & Council 2023) was approved which "obliges all Union entities to have their own internal cybersecurity risk-management measures" (Carrapico & Farrand 2024, 7). Furthermore, the regulation established an inter-institutional cybersecurity board which "should have an exclusive role in monitoring and supporting the implementation of this Regulation by the Union entities and in supervising the implementation of general priorities and objectives of, and providing strategic direction to, CERT-EU." (European Parliament & Council 2023, 4).

The 2023 proposed Cyber Solidarity Act[1] (European Commission 2023a) "aims to strengthen capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks." (European Commission 2024b). It includes a European cybersecurity alert system (called European Cybersecurity Shield) which is composed of security operation centers across the EU, and "a comprehensive Cybersecurity Emergency Mechanism to improve the EU's cyber resilience." (European Commission 2024b). The alert system is funded directly by the Digital Europe Programme (Carrapico & Farrand 2024; European Commission 2024b).

The recently adopted EU Cyber Resilience Act (European Parliament & Council 2024, see also Council 2024) aims at ensuring "that hardware and software products made available in the EU are rendered cyber-secure" (Carrapico & Farrand 2024, 6). The new regulation is considered to "give the Commission considerable powers, under the heading of market surveillance and enforcement, including deeming products as non-compliant with the Regulation and as presenting a significant cybersecurity risk on an ENISA assessment." (Carrapico & Farrand 2024, 6).

ENISA fulfils several tasks with regard to network and information security. The agency was established in 2004 (European Parliament & Council 2004). "ENISA's creation was based in the idea that there was a need for greater levels of coherence and coordination in the EU's approach to cybersecurity […]." (Farrand & Carrapico 2021, 30). Its mandate was extended three times (European Parliament & Council 2008; 2011a; 2013b). The agency's mandate became permanent in 2019 (European Parliament & Council 2019). It must be noted that the

[1] A provisional agreement on the "Cybersecurity Solidarity Act" was reached between the Council presidency and the European Parliament's negotiators on 20.03.2024 (https://www.consilium.europa.eu/en/press/press-releases/2024/03/06/cyber-solidarity-package-council-and-parliament-strike-deals-to-strengthen-cyber-security-capacities-in-the-eu/, last access 13.11.2024).

regulation from 2019 renamed ENISA into the European Union Agency for Cybersecurity. Under the current legislation the agency should contribute to the following tasks: Development and implementation of Union policy and law, capacity-building, operational cooperation at Union level, market, cybersecurity certification and standardization, knowledge and information dissemination, awareness-raising and education, research and innovation and international cooperation (Article 5-12 of Regulation 2019/881).

The agency's role and tasks evolved over time (Dunn Cavelty & Smeets 2023). In its initial phase and based on its founding regulation (European Parliament and Council 2004), the agency was tasked to conduct risk analysis, provide advice, facilitate cooperation, contribute to awareness raising and to develop international norms and standards (see also: Dunn Cavelty & Smeets 2023; Kipker 2023; Shepherd 2022). The founding regulation set out four objectives: Enhancing the capability of Member States to prevent, address and to respond to network and information security problems, providing assistance and advice to the Commission and Member States, developing expertise, to foster cooperation among the public-private sector and assisting the European Commission in preparing legislation in the field of network and information security (European Parliament & Council 2004, 4; see also: Dunn Cavelty & Smeets 2023). In 2009 ENISA's role was enhanced by the Framework Directive on Electronic Communications (European Parliament & Council 2009) which gave the agency a central role in cyber-incident reporting (Shepherd 2022). ENISA was further tasked to organize and run cyber incident exercises (European Parliament & Council 2004).

In 2012, ENISA's work was complemented by CERT-EU (also called Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies) that is in charge of the security of information networks of EU institutions and cooperates with national CERTs (Kipker 2023; Porcedda 2023). As an inter-institutional provider CERT-EU protects the information and communication technology infrastructure of all EU institutions and bodies and further coordinates responses to cyber incidents (Carrapico & Farrand 2024; see also CERT-EU 2024; European Union 2024). The team helps to prevent, detect, mitigate and respond to cyberattacks (CERT-EU 2024; European Union 2024). In the context of Russia's war against Ukraine, CERT-EU indicated an increase in cyberattacks on EU institutions (Carrapico & Farrand 2024; CERT-EU 2023).

On Member State level CSIRTs are tasks to monitor incidents at national level, provide early warning, response to incidents and provide risk and incident analysis and situational awareness (European Parliament & the Council 2016, 18). CERT-EU and national CSIRTs are embedded in the CSIRT-network. The network should contribute to the exchange of information, help to implement a coordinated response to an incident and assist the coordinated disclosure of vulnerabilities (CSIRTs Network 2024).

With the NIS directive in 2016, ENISA was assigned to assist Member States with its implementation (Christou 2016; Dunn Cavelty & Smeets 2023; Kipker 2023). Further, ENISA became member of the NIS-Cooperation Group and the secretariat of the above mentioned CSIRT network which facilitated the strategic cooperation and exchange of information between Member States (Dunn Cavelty & Smeets 2023; European Parliament & Council 2004; Kipker 2023). The NIS-Cooperation Group was established for the NIS-Directive implementation and should contribute to achieve a high common level of security for network and information systems in the EU (European Commission 2024a).

The Cybersecurity Act of 2019 (European Parliament & Council 2019) established a European cybersecurity certification framework that aims to improve the functioning of the internal market by increasing the level of cybersecurity and by harmonizing the digital single market for ICT products, services and processes (European Union 2024). In this context ENISA "was designated a key role in setting up and maintaining the certification framework by preparing the technical ground for specific certification schemes" (Dunn Cavelty & Smeets 2023, 1340). Moreover, ENISA was "mandated to increase operational cooperation at the EU level" (Dunn Cavelty & Smeets 2023, 1340) by helping Member States to handle cybersecurity incidents (European Parliament & Council 2019). With the Cybersecurity Act of 2019 ENISA's operational and budgetary resources were strengthened (Kipker 2023; Porcedda 2023; Shepherd 2022). The legislative act also stresses the "transnational dimension" (Shepherd 2022, 150) of cybersecurity whereby ENISA should also contribute to cooperation with international organizations and third countries.

The EU Cybersecurity Strategy from 2020 reiterates ENISA's role in capacity-building, exchange of knowledge and cooperation (Dunn Cavelty & Smeets 2023; European Commission 2020a). The NIS2-Directive added further tasks to the agency such as the establishment and maintenance of a vulnerability register of ICT products and services (European Parliament & Council 2022a). Further, the agency was mandated to carry out security risk assessment of critical ICT services, systems and product supply chains (Dunn Cavelty & Smeets 2023; European Parliament & Council 2022a).

In order "to support the coordinated management of large-scale cybersecurity incidents" (European Parliament & Council 2022a, 25) the directive established the EU-CyCLONe. It serves as a cooperation network for national authorities that are in charge of cyber crisis management (ENISA 2024b). ENISA provides the secretariat and helps to "support the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information." (European Parliament & Council 2022a, 25).

Another an important element in the 2020 EU Cybersecurity Strategy (European Commission 2020) represents the establishment the ECCC. Proposed in 2018 (European Commission 2018) and established in 2021 European Parliament & Council 2021a) the agency "should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives" (European Parliament & Council 2021a, 3) such as in relation to Horizon Europe or the Digital Europe Programme. The aim is to coordinate financial support in the area of cybersecurity research and development. Therefore, the agency should help to strengthen the EU's autonomy and competitiveness in cybersecurity by "retaining and developing the Union's research, academic, societal, technological and industrial cybersecurity capacities and capabilities" (European Parliament & Council 2021a, 9).

Further, it should for instance also collaborate with ENISA, promote cybersecurity resilience and provide recommendations for research and innovation. The ECCC cooperates with the 'Network of National Coordination Centers' that function as points of contact at national level to support the agency in fulfilling its mission and objectives (ECCC 2024b). As regards the financing of the agency, both the EU and Member States commit to contributing to the agency (ECCC 2024). The co-financing approach was agreed upon by the EP and the Council during the negations on the adaption of the agencies' regulation (ibid.). However, individual Member State contributions remain voluntary (ECCC 2024a; European Parliament & Council 2021a).

3.2. Cybercrime

While securing network and information systems against cyber-attacks is an important component of the EU cybersecurity landscape, malicious online activities represent an additional threat to the EU which necessitates law enforcement and cooperation. Therefore, the legal dimension of cybercrime will be explored. Generally, cybercrime "refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target." (European Commission 2013b, 3). Offences comprise traditional offences such as fraud or identify-theft, content-related offences and offences unique to computers and information systems (ibid.).

Concrete EU initiatives regarding cybercrime can be traced back to the late 1990s (Shepherd 2022). In 1996 the Commission issued a communication on illegal and harmful content on the internet (Commission 1996) in which it called for reinforced policy cooperation and certain minimum common standards in member state legislation (Shepherd 2022). On an international level, most notably is the EU's support for and the promotion of the 2001 Council of Europe Convention on Cybercrime which is also known as the Budapest Convention (Council of Europe 2001; Shepherd 2022). The convention outlines the following categories of cybercrime: Offences against confidentiality, integrity, and availability of computer data and systems, computer-related offences and offences related to infringement of copyright and related rights (Shepherd 2022). The Budapest Convention "is the only binding international agreement on cybercrime" (Shepherd 2022, 155) and "provides the framework for the EU's cyber-diplomacy efforts" (ibid.). Therefore, the Budapest Convention mainly represents the external dimension of cybercrime (Christou 2016). However, the EU's initial legal approach built on the Convention (Christou 2016; Porcedda 2023).

In 2001 the EU started to address cybercrime more concretely (Christou 2016; Shepherd 2022). A communication on combatting computer related crime (European Commission 2001a) introduced common incriminations, sanctions and EU enforcement mechanisms (Christou 2016; Shepherd 2022). Further it called for improved cooperation of law enforcement authorities and the creation of cybercrime units at the national level (Shepherd 2022). More legal instruments related to fraud and counterfeiting of non-cash means of payment and copyright followed in the same year (Council 2001; European Parliament and Council 2001; Shepherd 2022).

In 2004 a Council Framework Decision addressed the issue sexual exploitation of children and child pornography (Council 2004) by setting "minimal requirements in terms of approximation of legislation across member states" (Christou 2016, 93) and improving judicial cooperation and coordination. However, the framework decision was deemed inadequate due to problems in prosecuting offenders and consequently revised and replaced by a new directive in 2011 (Christou 2016). The new directive (European Parliament and Council 2011b) moved beyond minimal legislation by expanding the scope and substance of criminal law, "cross-jurisdictional investigations, proceedings, and cases, and the prevention of offences" (Christou 2016, 98f.). The directive further established rules concerning sanctions for criminal offences (European Parliament and Council 2011b).

A Council Framework Decision from 2005 (Council 2005) established a "more robust legal layer or environment for prosecution" (Christou 2005, 93) of general cybercrime cases by rule approximation in criminal law across Member States. In 2007 the Commission issued a communication on a general policy on the fight against cybercrime (Commission 2007) that aimed to improve strategic operational cooperation and coordination among law enforcement authorities across the EU, cooperation with third countries, international collaboration, judicial training related to cybercrime issues and public-private dialogues (Christou 2016; Shepherd 2023). Again, the communication emphasized the need for harmonization of national legislation. In 2008 two Council Conclusions on cybercrime followed. The first one (Council 2008b) concerned the setting up of alter platforms for reporting offences noted on the internet in order to improve the sharing between Member States and the EU (Shepherd 2023). The second one (Council 2008c) reinforced and set out measures for providing training and information exchange, using joint investigations, strengthening public-private partnerships and cooperation with third countries (Shepherd 2023).

The 2009 Stockholm Programme echoes these initiatives and further calls for improved judicial cooperation among Member States (Council 2009). Tackling and reducing cybercrime is also one key priority of the already mentioned 2013 EU Cybersecurity Strategy (Christou 2016). The NIS-Directive emphasizes that reducing cybercrime is only possible by enhancing cyber resilience (European Parliament & Council 2013, 10; Porcedda 2023). In 2017 the European Parliament passed a resolution on the fight against cybercrime in which it called for prevention, enhancing responsibility and liability of service providers, strengthening police and judicial cooperation, enhancing capacity-building at European level and improving cooperation with third countries (European Parliament 2017).

Cybercrime has also an operational dimension in the EU (Christou 2016). The European Law Enforcement Agency (Europol) became a central role as a resource and cooperation platform in cybercrime (Christou 2016). Europol provides data, identifies offenders and offences, facilitates the exchange of information and supports the coordination of Member States' operational activities (Busuioc & Groenleer 2013; Christou 2016). The Draft Council Conclusions from 2008 (Council 2008b) initiated the set-up of national alert platforms and of a European alert platform for reporting offences noted on the Internet in order to improve the sharing of information between Member States and the EU (Shepherd 2023). As a "point of convergence of national platforms" (Council 2008b, p. 9), Europol was assigned a coordinating role in cybercrime (see also Busuioc & Groenleer 2013). In its Stockholm Programme the Council further calls onto Europol to step up its "strategic analysis of cybercrime" (Council 2009, 47; see also Shepherd 2022).

In 2010, cybersecurity was formalized into a distinct policy domain with the Commission's Internal Security Strategy (European Commission 2010b; Carrapico & Farrand 2020). With regard to cybercrime and the role of Europol Carrapico and Farrand (2020) observe: "The Internal Security Strategy incorporated the reinforcement of existing agencies such as Europol with expanded competences in the field of cybercrime through a European Cybercrime Centre (EC3) […]." (1116). The creation of a center dedicated to cybercrime within Europol has already been proposed in the Draft Council Conclusions on implementing a concerted strategy to combat cybercrime in 2010 (Council 2010, 7f.; Shepherd 2022). In 2012, the Commission proposes the establishment of the EC3 within Europol (Commission 2012; Shepherd 2022). According to the communication EC3's tasks are focusing on cybercrimes committed by organized criminal groups, cybercrimes causing serious harm to their victims, and cybercrime affecting critical infrastructure and information systems (European Commission 2012, 4). Furthermore, EC3 should function as the European cybercrime information focal point, pool expertise to support Member States' capacity-building, provide support to member state cybercrime investigations and become the collective voice of European cybercrime investigators in law enforcement and the judiciary (European Commission 2012, 4f.).

The sub-unit became operational in 2013 and provided Europol with "an additional resource to fight cybercrime" (Christou 2018, 363). EC3 "is seen as a central node in fighting cybercrime"(Christou 2016, 88) that facilitates cooperation and coordination. In its operational activity EC3 focuses on cyber-dependent crime (e.g. the usage of botnets or ransomware), child sexual exploitation, payment fraud and tackling criminality on the Dark Web and alternative platforms (Christou 2016; Europol 2024a). EC3 provides "operational, strategic, analytical and forensic support to Member States' investigations" (Europol 2024a) for each of the cybercrime types. Furthermore, the EC3 supports training and capacity-building for relevant Member State authorities, engages public and private stakeholders and conducts prevention and awareness campaigns (Europol 2024a; Shepherd 2022). Generally, EC3's role concerns enhancing law enforcement capabilities and to support Member States operationally (Christou 2018).

In order to further facilitate coordination and cooperation in cybercrime between relevant actors and agencies, new institutional structures have been created (Christou 2016; 2018). EC3 also "developed working relationships" (Shepherd 2022, 158) with other agencies such as ENISA, Eurojust, CEPOL, EEAS and EDA (Christou 2016; Shepherd 2022). In particular, Eurojust, the EU's judicial cooperation agency, "has posted personnel at EC3 and contributes to Europol's investigations." (Porcedda 2023, 59). Since 2014, EC3 also "hosts and supports the

Joint Cybercrime Action Taskforce (J-CAT) which is comprised of cyber liaison officers from various EU Member States, non-EU law enforcement partners and EC3." (Europol 2024b).

J-CAT was established as an EU taskforce in Member State initiative (Reitano et al. 2015). It is a permanent operational team that works on high-profile cases for cybercrime investigations (Europol 2024b; Shepherd 2022). EC3 provides the secretariat for J-CAT, operational and technical support and coordinates its operations (Christou 2018). With these new "governance arrangements within EC3" (Christou 2018, 356) additional operational capabilities in the field of cybercrime were installed that facilitate cross-border investigations and exchange of information (Christou 2018). Further, setting up the taskforce "in one physical location" (Reitano et al. 2015, 144) helped to overcome previous deficits in cooperation and law enforcement. In the area of cybercrime, a taskforce allows for flexibility and quick reaction (Christou 2018). Therefore, J-CAT "has its own ad hoc procedures in place" (Christou 2018, 366) to deal with urgent cases independent of formal meetings with Europol and EC3. Its structure further allows J-CAT to act as a proxy for Europol/EC3 in cooperation efforts with non-EU states and foreign law enforcement agencies (Christou 2018; Reitano et al. 2015). The taskforce was able to successfully conclude different cybercrime operations (Reitano et al. 2015).

In 2016 the Council called yet for further institutional structures in the area of cybercrime by concluding "that existing exchange between judicial authorities and experts in the field of cybercrime and investigations in cyberspace should be formalised and enhanced under the European Judicial Cybercrime Network supported by Eurojust […]." (Council 2016a, 2). The network "gathers judicial prosecutors and practitioners at European level thereby helping cross-national investigations." (Porcedda 2023, 59; see also Eurojust 2024). It therefore "facilitates and enhances cooperation between competent judicial authorities" (Eurojust 2024; see also Council 2016b) in the process of investigating and prosecuting cybercrime. The European Judicial Cybercrime Network (EJCN) is located within the European Union Agency for Criminal Justice Cooperation (Eurojust).

Eurojust participates in the ECJN Board, hosts meetings of the network, supports the exchange of information and "consults the EJCN about the development of policy work and other stakeholder activities to ensure a strong interaction between Eurojust's expertise in international judicial cooperation and the operational and subject matter expertise of the EJCN members." (Eurojust 2024). Apart from hosting the network, Eurojust also pursues further cybercrime related projects and initiatives such as the publication of the Cybercrime Judicial Monitor (Eurojust 2021; 2024). With regard to developing skills and knowledge in the area of cybercrime, the CEPOL additionally hosts a specialized training center for law enforcement officials: The Cybercrime Academy (CEPOL 2019; CEPOL 2021).

These new institutional structures “[…] have been created to tackle the issue of cybercrime in terms of […] facilitating coordination among stakeholders within and between member states – and the operational aspects of cybercrime cooperation – from investigation to prosecution.” (Christou 2016, 116). In particular, EC3 is tasked to ensure that operational activities correspond with relevant EU policies and to coordinate with related agencies such as Eurojust and CEPOL (Christou 2016).

3.3. Cyber defence

In comparison with the other sub-issue areas, the EU’s approach to cyber defence is far less developed and evolved only in recent years (Deschaux-Dutard 2020; Shepherd 2022). But as cyber defence has grown in importance, some notable initiatives were developed by the EU (Shepherd 2022). In the EU context cyber defence is about developing cyber self-protection and not to develop offensive cyber capabilities (Odermatt 2018; Shepherd 2022).

The different EU Cyber Security Strategies also encompass cyber defence. The 2013 Cyber Security Strategy mentions with regard to cyber defence: “To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyberdefence capability development should concentrate on detection, response and recovery from sophisticated cyber threats.“ (European Commission 2013b, 11). The Cybersecurity Strategy from 2017 emphasizes cyber-resilience as being essential in CSDP mission (European Commission 2017a) and the Strategy from 2020 calls for “ensuring that cybersecurity and cyber defence are further integrated into the wider security and defence agenda.” (European Commission 2020, 18). Both strategies consider the possibility to invoke the EU Solidarity Clause or Mutual Defence Clause (Article 42 TFEU) in case the EU needs to respond to a particular serious cyber incident or attack (European Commission 2017; 2020).

In its 2017 Communication on cybersecurity, the Commission proposes that “cyber defence projects or technologies developed by undertakings could benefit from European Defence Fund financing when it comes to both the research and development phase.” (Commission 2017a, 10). The Commission further proposes cyber defence to be included within the framework of the Permanent Structured Cooperation (PESCO). Since then, several projects related to cyberdefence have been initiated by different EU Member States (PESCO 2024).

The European Council Conclusions in 2013 called for an EU cyberdefence policy framework (Council 2013) which then followed in 2014 (Council 2014). The Cyberdefence Policy Framework considers cyberspace as "the fifth domain of warfare" (Council 2014, 2). The framework stresses the EU's ambition to support the development of Member States' cyber defence capabilities and to enhance the protection of CSDP communication networks used by EU entities (Shepherd 2022). The Cyberdefence Policy Framework further seeks to improve training and education possibilities and to enhance cooperation between related agencies and the private sector (Shepherd 2022; Porcedda 2023). Enhancing cooperation with NATO is also part of the EU's strategy in cyber defence (EDA 2013).

Within the context of the 2014 EU Cyberdefence Framework, cyber defence was integrated into EDA's mandate (Council 2014). The EDA supports the EU Member States in improving their defence capabilities, facilitates collaboration for Ministries of Defence, fosters cooperation and synergies between the public and private sector, offers education and training courses and assesses cyber challenges in other defence domains such as air, space, maritime and land (EDA 2021). The EDA also leads a network of cyber defence teams from EU Member States. The military CERT-network was established to enhance the level of cooperation in the cyber domain at EU level (EDA 2023). The military CERTs also participate in cyberdefence exercises with the EDA.

The EU Cyber Defence Policy Framework was updated in 2018 (Council 2018a). The new policy framework sets out priorities with regard to research and technology and the civilian-military cooperation (Council 2018a). It further proposes cyberdefence to be included in crisis management (Council 2018a, Shepherd 2022). In 2023, the Council adopted conclusions on the EU Policy on Cyber Defence (Council 2023a) which echoes the ambitions of the previous policy framework. If further stresses the need to secure the "EU defence ecosystem" (Council 2023a, 10) by encouraging Member States to develop own capabilities to conduct cyber operations and promoting the use of standards for civilian cybersecurity and cyber defence uses. In addition, the council calls for recommendations to develop tools for secure communication in the cyber defence domain (Council 2023a).

A more recent communication from the Commission emphasizes that the "EU needs to take on more responsibility for its own security" (European Commission 2022b, 1) and to "increase investments in full-spectrum cyber defence capabilities, including active defence capabilities" (ibid.) by ensuring "its technological and digital sovereignty in the cyber field." (ibid.). Further the EU sees itself as a coordinator within the defence community: The Communication proposes to establish the EU Cyber Defence Coordination Centre (European Commission 2022b, 3).

In addition, the Commission calls for enhanced civilian-military collaboration, plans to enhance mutual assistance between Member States and to enhance cyber resilience of the Member States's military infrastructures in CSDP missions. With regard to the last point the Communication mentions that the High Representative and the Commission "will assist Member States with the development of non-legally binding recommendations for the defence community, inspired by the Directive on measures for a high common level of cybersecurity across the Union (NIS2), as defence is excluded from the scope of the Directive." (European Commission 2022, 9).

Furthermore, the Communication focuses on EU efforts to develop cyber defence capabilities by supporting the further development of military capabilities e.g. through the EDF, enhancing research efforts in key technologies for cyber defence and increasing the number of EU cyber defence workforce by the help of new initiatives such as the proposed Cyber Skills Academy (European Commission 2022b). The EDF in particular allows to finance projects of military research and development in e.g. cyberdefence through the EU budget (Hoeffler 2023; see also Commission 2022). One notable cyberdefence-related project financed by the EDF is the 'EUCINF project' that develops a cyber and information warfare toolbox (EDF 2022; EUCINF 2024).

3.4. Cyberdiplomacy

Cybersecurity is also an issue in international diplomacy as tensions between global powers increase (Shepherd 2022). On the international stage the EU aims at enhancing international cooperation through the UN, by capacity-building in third states and by shaping international norms in cyberspace (Shepherd 2022, 167; see also Carrapico & Farrand 2024; Porcedda 2023). The 2013 Cybersecurity Strategy sought to mainstream cyber issues into the EU's Common Foreign and Security Policy (CFSP) (Commission 2013; Shepherd 2022).

The Council Conclusions on Cyberdiplomacy emphasized the external dimension on the EU's approach to cybersecurity by promoting the protection of human rights in cyberspace, supporting norms of behavior and the application of international law in cyberspace and maintaining engagement with international organizations (Council 2015; see also Council 2018b). In its diplomatic efforts in cybersecurity, the EU also stresses the importance of external cyber capacity building in form of cooperation with third countries (Council 2018b). An example here are the recent Cyber Dialogues between the EU and Ukraine (Commission 2024). The EU also provides funding for cyberdiplomacy related projects such as the ‘EU Cyber Direct’ initiative. The project is “focused on policy support, research, outreach and capacity building in the field of cyber diplomacy.” (EU Cyber Direct 2024).

In 2017, the Council introduced the ‘Cyberdiplomacy-Toolbox’ which provides a framework for the EU’s diplomatic response to malicious cyber activities (Council 2017; see also Council 2023b; Moret & Pawlak 2017). The initiative involves objectives such as cyber capacity-building in third countries, cyber dialogues between the EU and non-EU states and the establishment of regional partnerships in cybersecurity matters (Carrapico & Farrand 2024). A joint European diplomatic response “should […] influence the behavior of potential aggressors in a long term.” (Council 2017, 5). In this regard the EU considers restrictive measures as suitable (Council 2017). The 2019 Council Decision “allows for restrictive measures to be applied in response to cyber-attacks” (Council 2019, 14). The “use of cyber sanctions add crucial foreign policy elements“ (Shepherd 2022, 171) to the EU’s cybersecurity approach. Taken together, cyberdiplomacy is mainly pursued through soft law, cooperation with third states, external cyber capacity-building and the projection of EU core values in cyberspace onto the international stage.

Integration instrument: Regulation	**Hard/soft law?**	**Content**
Communication: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (2001a).	Soft law	The communication contains legislative proposals for criminal law harmonization, indirect capacity-building proposals such as setting-up specialised units at national level, training and cooperation.
Communication: Network and Information Security -Proposal for a European Policy Approach (2001b).	Soft law	A proposal of a European policy approach on member state and EU level that contains awareness raising, a European warning and information system, technology support, support for market orientated standardisation and certification, a legal framework and international co-operation.
Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.	Hard law	Member states shall take the necessary measures to secure network and information security. Illegal access to information systems shall be punishable under criminal law. Member states shall establish a point of contact for the exchange of information on offences related to attacks against information systems.
Communication from the Commission on a Programme for Critical Infrastructure Protection (2006).	Soft law	The communication lays out a plan to identify and reduce vulnerabilities of member states' critical infrastructure.
Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.	Hard law	The directive establishes a procedure for the identification and designation of European critical infrastructures and a common approach to the assessment of the need to improve the protection of such infrastructures. Member states shall take the necessary measures to comply with the directive.
Communication: Critical Information Infrastructure Protection. Protecting Europe from Large Scale Cyber-Attacks and Disruptions- Enhancing Preparedness, Security and Resilience (2009).	Soft law	The communication calls for better cooperation and coordination across Europe and sets out an action plan on how to tackle challenges posed by large scale cyber-attacks (including preparedness, prevention, detection, response, mitigation, recovery, international cooperation and implementing criteria for the ICT sector).
Directive 2009/140/EC of the European Parliament and of the Council.	Hard law	The directive made it mandatory for telecommunications operators to report cyber-incidents to the national regulatory authority.

Communication: Cybersecurity Strategy of the European Union -An Open, Safe and Secure Cyberspace (2013).	Soft law	The Cybersecurity Strategy contains different, comprehensive measures in relation to the cybersecurity sub-areas.
Directive (EU) 2016/1148 of concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).	Hard law	The Directive lays down measures and obligations to achieve a high common level of security of network and information systems within to Union to improve the functioning of the internal market.
Communication: Resilience, Deterrence and Defence - Building strong cybersecurity for the EU (2017).	Soft law	The new strategy laid out key actions to strengthen cyber resilience, to create effective EU Cyber Deterrence and to strengthen international cooperation on cybersecurity.
Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade (2020).	Soft law	The Communication stresses the geopolitical dimension of cybersecurity. The strategy set outs different objectives that aim at improving the security of information networks and digital infrastructure.
Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).	Hard law	The Directive lays down cybersecurity risk-management measures and obligations for Member States to adopt national cybersecurity strategies, to establish cyber crisis management authorities and CIRTs.
Regulation 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (2023).	Hard law	The Regulation obliges all Union entities to have their own internal cybersecurity risk-management measures.
Regulation -Cyber Resilience Act (2024).	Hard law	The Regulation sets out requirements for products with digital elements with a view to ensure that products are safe before placed on the market. The law introduces EU-wide cybersecurity requirements for the design, development, production and making available on the market.
Communication on illegal and harmful content on the internet (1996).	Soft law	The communication presents certain policy options to reduce illegal and harmful content on the Internet that include e.g. enhancing cooperation between member states, the need for a common European Framework for liability of access providers and host service providers.

Council of Europe Convention on Cybercrime -Budapest Convention (2001).	Hard law	The Budapest Convention is the only binding international agreement on cybercrime. It contains sections on measures to be taken at the national level (regarding criminal law) and on international cooperation (e.g. transborder access to computer data).
Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.	Hard law	The Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children. Further, it introduces provisions to strengthen the provision of those crimes and the protection of the victims thereof.
Communication: Towards a general policy on the fight against cybercrime (2007).	Soft law	The Communication sets out certain objectives such as improving and facilitating coordination and cooperation between cybercrime units, other authorities and experts in the EU, developing an EU Policy Framework on the fight against cybercrime with Member States and relevant stakeholders, strengthening operational law enforcement cooperation and EU-level training, and harmonisation of national legislation.
Draft Council conclusions on setting up national alert platforms and a European alert platform for reporting offences noted on the Internet (2008).	Soft law	The Draft Council conclusions invite Member States to set up a national alert platform for the purpose of centralising alerts on offences notes on the internet and invites Europol to establish a European platform which should function as a point of convergence of national platforms.
EU Cyber Defence Policy Framework (2014).	Soft law	The Cyber Defence Policy Framework supports the development of cyber defence capabilities of EU Member States. Priorities are: Supporting the development of Member States cyber defence capabilities related to CSDP by the help of the Capability Development Plan, enhancing the protection of CSDP communication networks used by EU entities and the promotion of civil-military cooperation and synergies with wider EU cyber policies.

Joint Communication: EU Policy on Cyber Defence (2022).	Soft law	The communication proposes a new strategy containing: Strengthening common situational awareness and coordination within defence community, enhancing coordination with civilian communities, enhancing the cyber resilience of the defence ecosystem, ensuring EU cyber defence interoperability and coherence of standards, develop cyber defence capabilities, enhancing research efforts in key technologies for cyber defence, increasing the number of EU cyber defence workforce, and strengthening EU-NATO cooperation and cyber-dialogues.
Council Conclusions on Cyberdiplomacy (2015).	Soft law	The Council Conclusions on Cyberdiplomacy stress the importance to promote and protect human rights and fundamental freedoms in cyberspace.
Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (2017).	Soft law	The "Cyberdiplomacy Toolbox" contains restrictive measures for a joint EU diplomatic response to malicious cyber activities.
Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.	Hard law	The Council Decision includes economic sanctions as a response to cyber-attacks with a significant effect which constitutes an external threat to the Union or its Member States.
Council Conclusions on the EU Policy on Cyber Defence (2023).	Soft law	The Council Conclusions stresses the role of the EU in cyber defence and sets out different objectives regarding securing the EU defence ecosystem, investing in cyber defence capabilities and cooperation with international partners.

Table 1. *Summary of selected EU regulatory instruments.*

Integration instrument: Capacity-building	**Type**	**Aim/target**
ENISA -The European Union Agency for Cybersecurity	New agency	The agency primarily supports the built-up of national capacities in cybersecurity. But also engages in direct capacity-building through training, exercises and awareness-raising.
Computer-Emergency-Response Team (CERT-EU)	Direct capacity-building	An inter-institutional provider that contributes to the security of the ICT infrastructure of EU institutions, bodies and agencies. The team helps to prevent, detect, mitigate and respond to cyberattacks, and by acting as the cybersecurity information exchange and incident response coordination hub.
CSIRT-network	Network (operational cooperation between member states)	The network is composed of national CSIRTs and CERT-EU. It should contribute the exchange of information, to implement a coordinated response to an incident and to help the coordinated disclosure of vulnerabilities.
National Liaison Officers Network (ENISA)	Network	The National Liaison Offices Network facilitates the exchange of information between ENISA and the Member States and supports ENISA in disseminating its activities.
NIS-Cooperation group	Network (for member state coordination)	The group was established for the NIS implementation. It should contribute to achieve a high common level of security for network and information systems in the EU. It facilitates the cooperation and exchange of information among EU Member States.
European Cybersecurity Certification Framework (see Cybersecurity Act)	Indirect capacity-building	A European Cybersecurity Certification Framework aims at harmonizing the digital single market for ICT products, services and processes. ENISA is involved in developing cybersecurity certification schemes.
European Cybersecurity Competence Centre (ECCC)	Agency	The agency makes strategic investment decisions and pools resources from the EU and its Member States, and indirectly the industry to improve and strengthen technology and industrial cybersecurity capacities. The agency coordinates funding.

National Coordination Centres related to ECCC	Network (coordination with national centres)	The National Coordination Centres function as points of contact at national level to support the Competence Centre in fulfilling its mission and objectives.
European Cyber Crises Liaison Organization Network (EU-CyCLONe)	Network (cooperation with member states' authorities)	A cooperation network for Member States national authorities that is in charge of cyber crisis management. ENISA supports the network operationally. It was established under the NIS-Directive.
European Cybercrime Centre (EC3/Europol)	Agency -task expansion	Europol's tasks were extended by establishment of the European Cybercrime Centre. EC3 provides operational, strategic, analytical and forensic support to Member States' investigations.
Cybercrime Action Taskforce (J-CAT)	Network organization	The taskforce is a permanent operational team (located at Europol/EC3) that works on high-profile cases for cybercrime investigations.
European Judicial Cybercrime Network (Eurojust)	Network (cooperation between judicial authorities)	The network facilitates and enhances cooperation between competent judicial authorities.
Cybercrime Academy (CEPOL)	Direct EU capacity-building	CEPOL hosts a specialized training center for law enforcement officials.
European Defence Agency	Agency -task expansion	The EDA supports the EU member states in improving their defence capabilities and facilitates collaboration for Ministries of Defence.
Military CERT-Network	Network	The network was established to enhance the level of cooperation in the cyber domain at EU level. The military CERTs also participate in Cyber Defence exercises with the EDA.
PESCO projects related to cyberdefence	Direct EU capacity-building	Several member states participate in different PESCO projects that are related to cyberdefence.
European Defence Fund	Indirect capacity-building	The EDF incentives and supports defence research projects and development such as in cyberdefence (see for example the 'EUCINF' project).

Table 2. *Summary of selected EU capacity-building instruments.*

4. Variation in the EU's approach to Cybersecurity

By mapping the EU cybersecurity landscape, variation in the approach to cybersecurity across the different sub-areas that encompass network and information security, cybercrime, cyberdefence and cyberdiplomacy can be observed. Generally, the EU approaches cybersecurity by regulation and capacity-building. However, on closer inspection variation inside these instruments can be observed as well (see figure 1). Regulation can take form of binding and non-binding rules (hard vs. soft law). Capacity-building may be direct (on EU-level) or indirect (on national level). Further, capacity-building may take form of new actors i.e. through the creation of agencies or networks. Regarding agencies we find further variation: Either new agencies are established, or the tasks of pre-existing agencies are expanded.

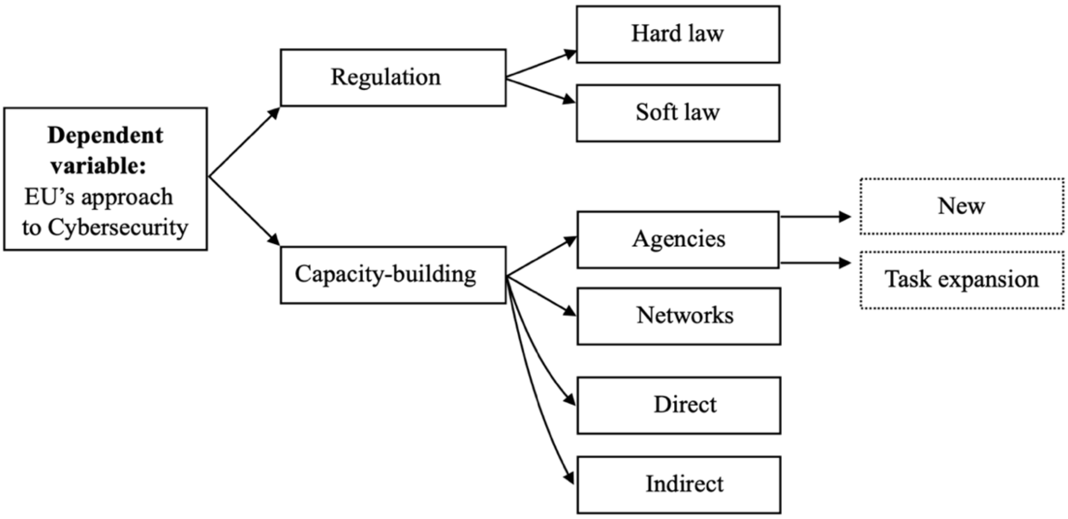


Figure 1. *Variation of the dependent variable.*

How can we account for this cross-sectoral variation in the EU's approach to cybersecurity? The core state power integration literature (Genschel & Jachtenfuchs 2014) provides a theoretical framework that helps to explain different patterns of integration in policy areas that relate to core state functions. EU Cybersecurity can be described as a case of core state power integration. Usually, core state power integration is described to proceed by regulation and capacity-building (Genschel & Jachtenfuchs 2014). Less attention has so far been directed to the variation within both approaches. Why is the EU's approach to cybersecurity composed of various instruments? The following section elaborates on the theoretical framework. The core state power integration framework should serve as a starting point. But as will be shown, the master thesis seeks to extent the theoretical framework in order to account for variation within each approach to cybersecurity.

5. Theoretical framework: Integration of core state powers by regulation and capacity-building

The EU has expanded the scope of its regulatory activities to new policy areas previously assumed to reside only in the realm of the sovereign Member States (Genschel & Jachtenfuchs 2014; 2016). By moving beyond market integration, the EU proceeded to the integration of core state powers (Genschel & Jachtenfuchs 2014). Genschel & Jachtenfuchs (2014) indicate that "EU institutions are more deeply involved in regulating and exercising core state powers." (8). By core state powers, the authors refer to constitutive features of the state such as coercive force, public finance and public administration (Genschel & Jachtenfuchs 2014). Further key functions of the sovereign state include "money, and fiscal affairs, defence and foreign policy, migration, citizenship and internal security." (Genschel & Jachtenfuchs 2016, 43).

The EU's activity in the area of cybersecurity can be regarded as an instance of integration of core state powers. Though the state has different roles in cybersecurity e.g. as a security guarantor and legislator (Dunn Cavelty & Egloff 2019), security governance is increasingly dispersed between governments and international organizations (Krahmann 2003). The fragmentation of political power can occur in the form of delegating authority upwards to the supranational level (Dunn Cavelty & Egloff 2019, 42; see also Krahmann 2003). Cybersecurity represents no exception here as the EU became active in this specific security policy field that is conventionally thought of to reside in the realm of the nation state (Dunn Cavelty & Egloff 2019; Dunn Cavelty & Smeets 2023; Kruck & Weiss 2023).

According to Genschel & Jachtenfuchs (2014) the integration of core state powers proceeds by regulation and capacity building. EU institutions "gradually enlarge their scope of regulatory activities in order to include new, initially exempt policy areas" (Genschel & Jachtenfuchs 2014, 5) and create "resources for exercising core state powers" (Genschel & Jachtenfuchs 2014, 6). Therefore, the authors differentiate between regulation (of national core state powers) and capacity-building (for European core state powers) as instruments of integration.

Integration by regulation implies the creation of "common rules, hard or soft, for the exercise of national core state powers" (Genschel & Jachtenfuchs 2014, 11). Here the EU "constrains the use national actors […] make of national core state powers" (Genschel & Jachtenfuchs 2014, 11). Integration by capacity-building implies the creation of EU resources or common capabilities for the supranational exercise of core state powers (Genschel & Jachtenfuchs 2014). In the case of capacity-building, the EU "creates new European actors and assigns new powers to them, which are exercised in parallel to, in competition to, or even instead of corresponding national powers." (Genschel & Jachtenfuchs 2014, 11). Though, not being mutually exclusive, both instruments of integration have different implications. By regulation, the EU "gains regulatory control over their [the Member State's] core powers" (Genschel & Jachtenfuchs 2014, 11), whereas capacity-building "pushes the EU on a path towards state building" (Genschel & Jachtenfuchs 2014, 11; see also Kelemen & McNamara 2022; Kruck & Weiss 2023).

The authors identify two demand conditions that determine the instrument of integration: Policy externalities and economies of scale (Genschel & Jachtenfuchs 2014). Policy externalities create the demand for integration by regulation. "Policy externalities arise when the domestic exercise of core state powers negatively or positively affects actors in other member states." (Genschel & Jachtenfuchs 2014, 12). "External effects create incentives for international coordination, which, in turn, induce actors to call for common European regulatory frameworks facilitating such coordination." (Genschel & Jachtenfuchs 2014, 13).

Economies of scale create the demand for integration by capacity-building. "Economies of scale exist when it is cheaper in terms of economic, administrative or political unit costs to consolidate core state powers at the European level rather than exercise them disjointedly at the national level." (Genschel & Jachtenfuchs 2014, 12f.). Instead of building separate national capacities, joint gains from European capacity-building can be derived (Genschel & Jachtenfuchs 2014). In this regard the authors mention the consolidation of defence capabilities at EU level, fiscal risk pooling or the centralization of information exchange as examples of European capacity-building (Genschel & Jachtenfuchs, 13).

Beside these demand conditions, supply conditions govern the mode of integration (Genschel & Jachtenfuchs 2014). Supply conditions depend on the "actors able and willing to bring it about, i.e. actors who control decisions concerning EU regulation and capacity building *and* have an interest in using this control for extending EU regulation and capacity." (Genschel & Jachtenfuchs 2014, 14). The authors differentiate between modes of stealth or publicity. Non-majoritarian actors such as the Commission or the ECJ pursue integration by stealth because "more integration tends to increase their authority, resources and prestige, and thus serves their institutional self-interest" (Genschel & Jachtenfuchs 2014, 14). In contrast, majoritarian actors such as the EP and the Council pursue integration by publicity as they have the power to supply EU regulation and capacity building (Genschel & Jachtenfuchs 2014). The integration of core state powers requires both demand and supply: There needs to be a demand for collective problem solving and the supply of actors to bring about the necessary institutional changes (Genschel & Jachtenfuchs 2014, 16).

6. Accounting for variation in the EU's approach to core state power integration

The theoretical framework by Genschel & Jachtenfuchs (2014) helps to understand through which instruments core state power integration can proceed. But how can we explain variation within both types of core state power integration instruments and across cybersecurity sub-sectors? Building on the core state power integration framework and with reference to supra-nationalism and liberal intergovernmentalism but also by elucidating further conditions that can account for variation in the EU's approach to cybersecurity integration, the master thesis seeks to expand the theoretical framework of core state power integration. The following sections focus on the different instruments of core state power integration and possible explanations for the identified variation within each instrument.

6.1. Variation in the EU's regulatory approach: Hard law and soft law

6.1.1. Demand for regulation in cybersecurity

Externalities create demand for regulation. "Policy externalities arise when the domestic exercise of core state powers negatively or positively affects actors in other member states." (Genschel & Jachtenfuchs 2014, 12). External effects can be either negative or positive. In the case of cybersecurity negative externalities mostly emanate from inadequate security standards, incoherent national legal frameworks and a lack of coordination e.g. in reaction to cyber-attacks. The interconnectedness of cyberspace may reinforce negative externalities (Bauer & van Eeten 2009).

In order to reduce negative externalities, the creation of a common European regulatory framework that facilitates such coordination is necessary (Genschel & Jachtenfuchs 2014). Due to the cross-border nature of cybersecurity, the EU is well positioned to assume the role of a policy coordinator. By realizing that certain common interests cannot be attained on a national level, the transfer of policy competences to supranational institutions and the creation of supra-national rules becomes viable (Haas 1961; Sweet & Sandholtz 1997).

The demand for regulation can also arise as a reaction to external shocks or events Schimmelfennig 2018) as certain security issues become salient. In the case of cybersecurity mainly changes in technology, the increase of cyber-attack and geopolitical tensions can create demand for cooperation. External shocks or events may lay open vulnerabilities and dependencies on part of the EU. A response to new exogenous interdependencies (Schimmelfennig et al. 2015) may reflect the EU's digital independence and sovereignty discourse (Carrapico & Farrand 2020; 2024; Farrand & Carrapico 2022). Cybersecurity integration is assumed to be increasingly underpinned by a security logic (Farrand & Carrapico 2022; Sivan-Sevilla 2021).

The demand for regulation can also arise due to endogenous interdependence as the integration within one policy area may lead to the integration of functionally related policy areas following neo-functionalist theory (Niemann et al. 2019; Sandholtz & Sweet 2012). This process of functional 'spill-over' (Haas 1961) is achieved when it "becomes evident that initial policy objectives cannot be adequately attained without such an extension." (Sweet & Sandholtz 1997, 301). The effect of spill-over into functionally related policy domains can be expected in the case of cybersecurity as this policy area encompasses different dimensions that overlap. To effectively address certain cyber issues, expanding the regulatory approach from one policy field to another related policy field is likely to be observed for example in network and information system security and cybercrime. Both areas are functionally related as network and information systems are often targets of cybercriminal activities *and* tools through which cyber criminals operate. Functional spill-over into related policy fields can lead to certain path-dependencies (Hooghe & Marks 2019; Sivan-Sevilla 2021) that narrow down the option of how (cyber) policy issues are approached by regulation i.e. either by soft or hard law.

It can be acknowledged that different demand conditions exist in the area of cybersecurity. The EU can reduce externalities, react to external shocks/events by facilitating coordination and creating common regulatory frameworks or by linking functionally related policy domains. The instrument of regulation can assume two forms. Scholarly literature differentiates between hard and soft law (Cappellina et al. 2022; Saurugger & Terpan 2020; Terpan 2015). Hard law encompasses legally binding acts such as regulations or directives and soft law encompasses non-binding acts like communications, recommendations, guidelines, and strategies (Saurugger & Terpan 2020). Accordingly, the main distinguishing feature is the legal binding force. In practice, hard and soft law can coexist in a policy field (Trubek & Trubek 2007). What can account for the choice between hard and soft law? The question directs attention to the supply conditions of EU core state power integration as "(d)emand for integration does not automatically generate its own supply." (Genschel & Jachtenfuchs 2014, 14).

6.1.2. The supply conditions for the choice between hard and soft law in cybersecurity

The supply conditions for regulation depend on the "actors willing and able to bring it about" (Genschel & Jachtenfuchs 2014, 14). Here in particular actors are meant that "control decisions concerning EU regulation […] *and* have an interest in using this control for extending EU regulation." (Genschel & Jachtenfuchs 2014, 14). EU actors as 'suppliers of integration' have different preferences when it comes to the choice between hard and soft law. Consider supranational actors such as the Commission, the ECJ[2] and the EP first. Generally, these EU actors favor more integration as it "tends to increase their authority, resources and prestige, and thus serves their institutional self-interest." (Genschel & Jachtenfuchs 2014, 14; see also Kelemen & Tarrant 2011). The Commission has the right of initiative to propose legislation, the ECJ enforces EU law, and the EP has a co-legislation role. Consequently, these actors always prefer hard law acts over soft law acts as a way to extend EU integration.

Underlying these assumptions is supranationalism as theory of EU integration. Supranationalism regards the Commission and the ECJ "at the heart of the expansive dynamism of European integration." (Sandholtz & Sweet 2012, 23). Due to its supranational agency, the Commission can act as legislative agenda-setter and as a political entrepreneur (Kaunert et al. 2013; Sandholtz & Sweet 2012). The Commission can support and mobilize certain policy objectives or link new issues (such as cybersecurity) to existing EU competences (Sivan-Sevilla 2021).

Consider EU Member States next. In contrast to supranational actors, "the willingness of national governments [to supply integration] is more contingent and cannot be taken for granted." (Genschel & Jachtenfuchs 2014, 15). The agreement to binding legal obligations on the supranational level has to be viewed more differentiated from the perspective of EU Member States. The adoption of hard law acts can reduce transaction costs and strengthen the credibility of commitments (Abbott & Snidal 2000). Therefore, hard law acts can facilitate the operation within a legal framework (Abbott & Snidal 2000). Legally binding acts further contribute to assuring compliance with rules among actors (Börzel 2021). However, adopting hard law entails costs for Member States. Hard law restrict actors' behavior and their sovereignty (Abbott & Snidal 2000). A violation of EU law incurs further costs for Member States as hard law acts are subject to enforcement by the ECJ (Abbott & Snidal 2000).

[2] Due to the novelty of cybersecurity as an EU policy field, Bendiek & Maat (2019) note that there are no specific ECJ rulings on cybersecurity yet. The role and influence of the ECJ on cybersecurity polices can therefore not be assessed in this master thesis. The focus primarily lays on the Commission as a supranational and non-majoritarian actor.

Sovereignty concerns can play a crucial role here as Member States may be reluctant to delegate authority to the supranational level and give up sovereignty. Concerns for national security can "act as brake on European integration." (Kaunert et al. 2013, 277). Therefore, Member States may not commit to hard legal acts and limit their autonomy due to sovereignty reasons. Sovereignty costs "are especially high in areas to national security" (Abbott & Snidal 2000, 440) but should be less pertinent in case that legal acts have to be transposed into national law (Abbott & Snidal 2000). Other forms of costs regard those that arise in cases of non-compliance (Börzel 2021). If actors expect the legal costs in case of non-compliance too high, the adoption of hard law acts is unlikely.

Considering the costs that can arise from hard law acts for Member States, the adoption of soft law instruments may serve as an alternative. Softer legislation is often easier to achieve "especially […] when actors are states that are jealous of their autonomy and when the issues at hand challenge state sovereignty." (Abbott & Snidal 2000, 423). The adoption of soft law instruments can thus limit sovereignty costs. Soft law further allows Member States to deal with uncertainties in complex issue areas and to facilitate compromise and cooperation. Asymmetries of interdependence that give rise to divergent preferences of EU Member States towards integration (Moravcsik & Schimmelfennig 2019) can hinder finding ways to agree on legally binding acts. As an alternative, soft law instruments can help Member States to "adapt their commitments to their particular situations rather than trying to accommodate divergent national circumstances" (Abbott & Snidal 2000, 445). Soft law can also be considered a "stepping-stone towards hard law" (Abbott & Snidal 2000, 456). Learning processes of the consequences of an agreement based on soft instruments may lower the "perceived costs of subsequent moves to harder legalization." (Abbott & Snidal 2000, 435). Therefore, initial soft law approaches in policy areas may pave the way for legally binding acts.

Underlying the assumptions for the legal choices of EU Member States is the EU integration theory of liberal intergovernmentalism. Liberal intergovernmentalism regards states as the critical actors in EU integration that "seek to achieve goals primarily through intergovernmental negotiation and bargaining" (Moravcsik & Schimmelfennig 2019, 65) and less through the delegation to the supranational level due to sovereignty concerns.

The variation in the EU's regulatory approach to cybersecurity can on the one hand be explained by demand conditions (externalities and exogenous/endogenous interdependence) and on the other hand by supply conditions (supranational actors vs. Member States) on the other hand. The demand side indicates several reasons for cooperation through legal frameworks in cybersecurity on EU level. However, the supply side mainly drives the choice of legal instruments. Supranational actors prefer hard law acts while Member States through the Council rather resort to soft law acts.

6.1.3. Areas of EU competence as scope conditions for the EU's regulatory approach

The choice of EU actors to propose hard law or soft law acts is assumed to be shaped by the specific area of EU competence. As the EU treaties "do not provide the EU with an explicit cybersecurity competence" (Delinavelli 2023) cybersecurity sub-issues are linked to existing EU competences (see also Bendiek & Maat 2019). The area of EU competence is considered to influence the extent to which actors can control decisions concerning EU regulation and use this control for extending EU regulation. It is therefore necessary to differentiate between the different types and areas of EU competences as laid down in the treaties while also considering the respective decision-making rules.

The Treaty on the Functioning of the European Union (TFEU) differentiates between three types of competences: Exclusive competences, shared competences and supporting competences (Article 2 TFEU). The EU has for example *exclusive competences* in specific aspects of the internal market and in monetary policies (Article 3 TFEU). The EU and its Member States can adopt legally binding acts in areas of *shared competences* such as the internal market, energy, freedom, security and justice and research, technological development and space (Article 4 TFEU). The EU has only *supporting competences* (Article 6 TFEU) for example in the area of industry. Most decisions in the EU's areas of competences fall under the ordinary legislative procedure and legal acts are adopted under qualified majority voting (Article 294 TFEU).

The EU's common foreign and security policy (CFSP) is "defined and implemented by the European Council and by the Council of the European Union" (European Union 2022). The CFSP represents an intergovernmental policy area. The Commission and the EP have only limited participation in the decision-making procedure and are excluded from any legislation activity (European Union 2022). Most decisions in the area of CFSP are taken by unanimity. Decision in the area of the EU's Common Foreign and Defence Policy (CSDP) are taken by the Council also by unanimity (Articles 42-46 TEU)[3].

Considering the different areas of EU competence, it can be expected that the Commission proposes hard law acts in the area of the single market where the EU has advanced the

[3] See also: https://eur-lex.europa.eu/EN/legal-content/glossary/common-security-and-defence-policy-csdp.html, accessed 28.11.2024.

most. Therefore, the Commission primarily seeks cybersecurity integration by linking cyber-issues to the area of the single market (Bendiek & Maat 2019; Farrand & Carrapico 2022, Sivan-Sevilla 2021). In areas of shared and supporting competences both hard and soft law can become viable options depending on the Member States' assessment of the costs of hard law and consideration of soft law as an alternative. Cybersecurity issues can be linked to areas of shared competences such as freedom, security and justice, research or technological development or as well to areas of supporting competences such as industry. Due to functional demand conditions EU Member States can be willing to agree to hard law acts in these policy areas. In areas of shared competences, the Council and the EP can control decisions concerning the extension of EU regulation through the ordinary legislative procedure. However, even in certain areas of shared competence (e.g. JHA) intergovernmental cooperation still persists (Lavenex & Wallace; Lavenex 2020; Maricut 2017; Roos 2017) and soft law acts are preferred over hard legal acts.

In intergovernmental policy areas such as the CFSP and CSDP, the adoption of soft law acts is expected due to the Member State's role in these domains and the predominance of sovereignty concerns. In these areas EU Member States are assumed to influence policies and to retain control on intergovernmental level (Sivan-Sevilla 2021). Here Member States through the Council retain control over decisions concerning the extension of regulation. In the area of CFSP and CSDP, Member States are assumed to use their control by limiting cooperation to the intergovernmental level and by only adopting non-legally binding decisions.

In general, supranational actors and Member States have different preferences what regards the choice between soft or hard law. Whereas supranational actors prefer hard law acts, the preference of Member States is more contingent. Member States are assumed -depending primarily on the area of EU competence- to either opt for hard or soft law. In the case of cybersecurity, the extent to which cyber-issues can be linked to shared competences can determine the legal choice. In these areas hard law can become a viable option as sovereignty costs are less pertinent and EU actors control decisions for extending EU regulation. In intergovernmental areas where sovereignty costs are high, the adoption of soft law is expected.

Though EU cybersecurity is generally representing a case of core state power integration, sovereignty costs vary across cybersecurity dimensions. The dimensions of cybersecurity comprise network and information security, critical infrastructure protection, cybercrime, cyberdefence and cyberdiplomacy. Member States should be less willing to give up sovereignty in areas of cyberdefence as this area immediately affects the core state powers of national Member States. The functional demand for cooperation in cyberdefence might however induce

Member States to adopt soft law acts such as frameworks or strategies. Member States should be less concerned with integrating network and information security or critical infrastructure protection as the functional demand conditions (for example when considering the cross-border nature of cybersecurity) should outweigh sovereignty costs. An agreement to hard law acts can be expected here. Having shed light on the demand conditions and supply options for hard and soft law, the next section elaborates on the various forms of capacity-building. As identified through the mapping of the cybersecurity landscape, capacity-building can result in the creation of agencies or networks, and it can be direct or indirect.

6.2. Variation in the EU's capacity-building approach

6.2.1. Demand for capacity-building in cybersecurity

Economies of scale create demand for capacity-building. "Economies of scale exist when it is cheaper in terms of economic, administrative or political unit costs to consolidate core state powers at the European level rather than exercise them disjointedly at the national level." (Genschel & Jachtenfuchs 2014, 12f.). Creating capacities on EU level instead of on the national level can create joint gains in terms of better coordination and efficiency (Genschel & Jachtenfuchs 2014). With regard to cybersecurity, building capacities on EU level is reasonable when considering its cross-border nature. The consolidation of European capacities to strengthen cyber resilience to react to cyber threats in a coordinative way can be more efficient.

Exogenous shocks/events such as cyber-attacks or shifts in geopolitics can also create the demand for capacity-building when vulnerabilities and dependencies of the EU become salient. As already mentioned, a response to exogenous interdependencies may reflect the EU's digital independence and sovereignty discourse. Developing capacities on EU-level represents an integral step in the EU efforts to regain (digital) autonomy. Demand for capacity-building can also arise due to endogenous interdependencies. The creation of capacities in one policy area may give rise to create further capacities in functionally related policy areas. Due to the interconnectedness of cyberspace, the building of capacities in functionally related domains is necessary to assure a comprehensive approach to cybersecurity.

Generally, the demand for capacity-building may also depend on pre-existing capacities on member state level. It is less efficient to duplicate already existing national capacities on EU level. It may be easier to build on already existing capacities than to build new ones. Therefore, past decisions to create capacities on the national level can condition capacity-building on EU level (see for example Thatcher 2011). Though there exist functional demands for capacity-building in cybersecurity on EU level, the extent and form of capacity-building is determined through different supply conditions.

6.2.2. Supply conditions for capacity-building (agencies and networks) in cybersecurity

In order to account for variation in capacity-building, attention is again directed to the supply side of core state power integration. Thereby the focus lays on the actors that are willing and able to proceed in core state power integration. More precisely those actors "who control decisions concerning […] capacity building *and* have an interest in using this control for extending […] capacity" (Genschel & Jachtenfuchs 2014, 14) are meant here. Capacity-building relates to the creation of EU resources for exercising core state powers. Such resources "are found primarily in […] EU agencies." (Trondal 2014, 167). EU agencies represent an example of new European actors (Bickerton et al., 2015; Genschel & Jachtenfuchs 2016). Agencies are "EU level public authorities with a legal personality and a certain degree of organizational and financial autonomy that are created by acts of secondary legislation in order to perform clearly specified tasks" (Kelemen 2005, 175). EU agencies help to deal with complex policy domains by providing expertise (Majone 1997).

Non-majoritarian institutions such as EU agencies "supply the Commission with relevant organizational capacities, particularly at the implementation stage of the decision-making cycle." (Trondal 2014, 167). EU agencies are considered as a valuable source for the Commission in preparing its decisions (Ruffing 2022). Institutionally, agencies are assumed to be closely related to the EU administrative apparatus and contribute to the centralization of regulatory functions on EU level (Egeberg et al. 2015; Egeberg & Trondal 2017). Therefore, agencies can help the Commission to expand its role and organizational resources in policy fields (Egeberg & Trondal 2011; Kelemen 2012 & Majone 2012; Thatcher 2011).

For supranational actors, namely the Commission and the EP, "the idea of establishing autonomous European agencies was an attractive second-best means through which to expand the EU's regulatory capacity" (Kelemen & Majone 2012, 226) especially under consideration that Member State governments are reluctant to expand the competences of the Commission. The delegation of authority to autonomous bodies outside the structure of the Commission (Kelemen & Majone 2012) allows Member States to pursue integration without further supranationalism i.e. the further transfer of decision-making power to the EU (Bickerton et al. 2015; Puetter 2012). Though Member State governments are generally assumed to be more hesitant to delegate certain tasks to the supranational level as delegation constrains their sovereignty (Abbott

& Snidal 2000; Moravcsik 1998, 67), the delegation to agencies can be seen as way of EU Member States to resist "any significant expansion" (Kelemen & Tarrant 2011, 929) of the Commission's power.

From an intergovernmentalism point of view, agencies "are set up to implement or monitor the implementation of policies agreed upon by national governments." (Egeberg & Trondal 2017, 676). Agencies can be seen as an attempt of Member States to credibly commit to long-term policy objectives (Christensen & Nielsen 2010; Kelemen & Majone 2012; Majone 1997; Wonka & Rittberger 2010) and to deal with uncertainties (Abbott & Snidal 2000). The delegation of certain tasks to agencies remains a decision of national governments and head of states. Therefore, the role and tasks of agencies are considered to be more limited. Especially in areas related to national security where sovereignty costs are high, delegation is more moderate (Abbott & Snidal 2000). In areas where sovereignty costs are low e.g. areas that necessitate technical coordination (Abbott & Snidal 2000), delegation from the national level to agencies is more likely.

Member States are expected to only delegate authority to administrative bodies that are subject to direct and indirect control (Abbott & Snidal 2000). Therefore, governments "insist on keeping EU agencies under their control" (Egeberg & Trondal 2017, 676; see also Bickerton et al. 2015) and limit their autonomy with regard to important issues (Abbott & Snidal 2000). In contrast, the delegation to agencies on the national level allows states to retain control and it incurs lower sovereignty costs (Abbott & Snidal 2000).

It can be summarized that supranational actors can expand their capacities by creating agencies while for Member States the creation of agencies can be seen as a way to avoid further supernationalism. However, Member States demand "considerable intergovernmental oversight of the agencies" (Kelemen & Majone 2012, 227). While functional demands (e.g. dealing with complex policy issues) drive the establishment of agencies in the first place, the actual design of such bodies is determined by considerations of the different actors on EU-level.

The delegation to agencies can be viewed from a principal-agent and competence-control theoretical viewpoint (Abbott et al. 2020; Biermann & Rittberger 2020; Rittberger et al. 2024; Ruffing et al. 2023). Inherent to the decision to create capacities in form of agencies is the granting of authority to the supranational level by indirect governance and delegation. Principals (European Commission, Council and EP) grant authority to an agent (EU agencies) to fulfill certain tasks. While there are functional motivations to grant certain competences and independence to agencies (Kelemen 2005; Kelemen & Majone 2012), principals -though having different preferences and interests- limit the independence of the agent by installing control mechanisms (Vos 2014; 2018).

The Commission and the EP[4] favor more independent agencies while Member States through the Council want to keep agencies under (intergovernmental) control (Kelemen & Majone 2012; Rittberger et al. 2024). Member States assure oversight of agencies "through the creation of management boards that were to be dominated by appointees of member state governments." (Kelemen & Majone 2012, 227). Based on this theoretical conception, capacity-building in form of agencies depends on the actor's willingness to grant competences and independence to them. Therefore, EU actors have to balance competence and control. The actual design of agencies is thus politically motivated and "the result of political compromise involving EU law-makers in the Council of Ministers, the European Parliament, and the European Commission." (Kelemen & Majone 2012, 226). EU actors can further either decide to create new agencies or to expand the tasks of (already existing) agencies.

The task expansion of agencies is also described by the process of 'layering' (Dunn-Cavelty & Smeets 2023; Kruck & Weiss 2023; Mahoney & Streeck 2010; Streeck & Thelen 2005). Layering implies gradual institutional change through "amendments, additions, or revisions to an existing set of institutions.“ (Streeck & Thelen 2005, 24). EU actors can decide whether to work within existing institutions and to gradually change these or to create new ones (Mahoney & Streeck 2010).

The focus now has been on the creation of agencies for building capacities. What we can also observe is the creation of networks (alongside agencies). Networks can be defined "as semi-stable informal clusters of interdependent actors, who have or take a specific interest or stake in solving a certain policy problem and who dispose of resources required for shaping and implementing the policy, and who are willing to mobilize and pool these resources.“ (Justaert & Keukeleire 2012, 437). Networks "are characterised by their feasibility, speed and expertise with regard to improving the capacity to resolve problems or tackle threats.“ (Christou 2018, 358). In contrast to agencies, networks are a form of informal governance. Networks can act "autonomously through spontaneous coordination of relevant actors“ (Christiansen et al. 2003, 6) and work "through informal relations which take place outside both the official structures and the semi-official arenas […].“ (ibid).

[4] The European Parliament conducts parliamentary oversight (legislative supervision and monitoring of the decisions and actions of agencies) for stronger accountability of agencies (Font & Pérez Durán 2016; see also Kelemen & Majone 2012).

Whilst representing an instance of indirect and informal governance (Biermann & Rittberger 2020; Christiansen et al. 2003; Justaert & Keukelerei 2012), networks function as an intermediary between domestic agencies, national actors, EU agencies and the EU-level (Biermann & Rittberger 2020; Abbott et al. 2020). Networks are a form of orchestration that allow governors to either (re)establish control or to enhance competence (Biermann & Rittberger 2020; Blauberger & Rittberger 2015). The relationship between agencies and networks can be either competitive or co-operative (Levi-Faur 2011). However, there are indications of a co-existence of agencies and networks which point towards the combination of delegation and orchestration (Biermann & Rittberger 2020).

Networks are useful in policy domains where the EU lacks operational capacities (Thatcher 2011; Blauberger & Rittberger 2015). As operational capacities here are understood for example the deployment of experts and equipment for "preventing, discouraging, deterring and responding to malicious cyber activities" (Backman 2023, 94; see also Commission 2021a). In the context of the EU, networks thereby can enhance operational coordination between the EU and Member State level (Backman 2023). Networks are also assumed to contribute to enhancing implementing capacities on the national level in order to assure the application of EU regulation (Blauberger & Rittberger 2015). By adding a network to an existing agency, networks are primarily expected to enhance competence. The establishment of networks can also be considered as an effort to harmonize the fragmented institutional landscape through agencies (Thatcher 2011). Furthermore, networks can represent an alternative choice to the delegation to agencies when political commitment is weak, and resources are limited (Levi-Faur 2011). Control can be enhanced by adding an agency to an established network (Biermann & Rittberger 2020). This combination allows to formalize the governance structures.

6.2.3. Areas of EU competence as scope conditions for the EU's capacity-building

Depending under which area of EU competence certain cybersecurity issues fall, different expectations regarding the choice between agencies and networks as forms of capacity-building can be derived. By referring back to the different areas of EU competence it can be expected that new agencies are created in areas where the Commission enjoys considerable competences such as related to the single market. Hereby the Commission will link cyber-issues to the single market. In this area, Member States through the Council can agree to establish an agency but they make sure to keep control over such bodies through e.g. member state representation in the agencies' board. It must be noted that in certain areas of shared competence, despite the communitarization of certain policy areas (such as JHA), intergovernmental decision-making arrangements and cooperation still persist (Lavenex & Wallace; Lavenex 2020; Maricut 2017; Roos 2017).

In intergovernmental areas that directly affect core state powers and incur sovereignty costs, it can be expected that Member States rather agree on expanding the tasks to deal with certain cyber-issues given functional demands for capacity-building. In cybersecurity sovereignty costs should be highest when issues relate to defence or external dimensions such as diplomacy. As Member States retain control over capacity-building decisions in these policy domains, extensive delegation to agencies is unlikely as Member States are reluctant to give up sovereignty.

Networks as a more informal mode of governance, can help to enhance operational and implementation capacities and coherence between policy fields. EU actors or agencies can be seen as a potential orchestrator of a network. In areas where cyber-issues are linked to shared competences networks can be expected to be added along existing agencies to enhance operational and implementation capacities. For Member States looser network structures can function as an alternative to (further) delegation in intergovernmental policy areas to facilitate operational cooperation in cyber specific domains.

In general, functional demands for European capacity-building exist but Member State's preferences for control and the different EU areas of competence influence the choice and extent to which capacities can be built on EU level. Agencies contribute to more centralization whereas networks represent a more flexible and informal way to enhance capacities. More generally, capacity-building can assume direct or indirect forms. In the following both types of capacity-building are explored and contextualized against the theoretical background.

6.3. Variation in capacity-building: Direct and indirect forms of capacity-building

EU capacity-building can be either direct or indirect. It can occur at EU-level directly when the building of capacities empowers the EU to either directly respond to cyber-issues or by creating resources on EU-level in the long-term. For example, direct capacity-building approaches can contribute to improving operational activities to prevent or deter cyberattacks, by providing training and skills to EU officials in cyber-related fields or by funding EU-level projects on cybersecurity.

Indirect capacity-building relates to supporting the built-up of national capacities (see for example Genschel & Jachtenfuchs 2023). When differentiating between the instruments of integration regulation and capacity-building, it must be noted that regulation often functions “to stimulate, steer and shape the creation and exercise of national capacities.” (Genschel & Jachtenfuchs 2023, 1456). Regulation and capacity-building “are often complementary rather than mutually exclusive instruments of rule.” (Genschel & Jachtenfuchs 2023, 1449; see also Genschel & Jachtenfuchs 2014). Regulation thus often aims at building capacities on national level that indirectly contribute to the overall capacities of the EU. For example, rules that aim at harmonizing security standards of digital products contribute to the overall level of cybersecurity in the EU. Other indirect capacity-building approaches (through regulation) can include the setting-up of information points and liaison offices on national-level or incentives for investment in cyber technologies.

Based on the theoretical considerations outlined before, it can be assumed that supranational actors prefer direct capacity-building over indirect capacity-building as it extends EU-level resources. Direct capacity-building approaches on EU level are rather limited due to the Member States predominance in security related matters. The Commission will resort to indirect capacity-building proposals by incentivizing the built-up of capacities for “the exercise of national core state powers” (Genschel & Jachtenfuchs 2014, 11) when tapping into intergovernmental areas of competence as in the case of (cyber)defence. In this case, Member States are expected to be more willing to support initiatives aiming at enhancing national capacities, rather than pooling resources on EU-level. Indirect capacity-building approaches are also expected in cases where cyber issues are linked to shared competences as the EU has to rely on the capacities of Member States in security matters (Genschel & Jachtenfuchs 2023).

The extended analytical framework aims to shed light on how to account for variation in the EU’s regulatory and capacity-building approach in cybersecurity. Table 3 summarizes the theoretical framework. It acknowledges the core state power instruments but further elaborates on the specific form each instrument can take by considering the role of EU actors in decisions concerning regulation and capacity-building.

Core state power instruments	**Regulation** - Soft law - Hard law	**Capacity-building** - Agency (*new* or *task expansion*) - Networks - Direct/indirect capacity-building
Demand for core state power integration	- Externalities - Exogenous interdependence (exogenous shocks/events). - Endogenous interdependence (functional spill-over).	- Economies of scale - Exogenous interdependence (exogenous shocks/events). - Endogenous interdependence (functional spill-over and presence of prior capacities).
Supply for core state power integration	Actors controlling decisions concerning EU regulation: - Supranational actors (European Commission, European Parliament, ECJ) prefer hard law acts. - Member States through the Council (mostly) prefer soft law acts over hard law acts.	Actors controlling decisions concerning EU capacity-building: - Supranational actors opt for creating new agencies. - Member States (through the Council) agree to establishing agencies while retaining control over them or by deciding to expand tasks of existing agencies. - Member States (through the Council) establish networks alongside agencies to enhance competence and as an alternative to delegation. - Supranational actors propose measures for both direct and indirect capacity-building.
Scope condition	Areas of EU competence (shared or intergovernmental).	

Table 3. *Summary of theoretical framework.*

Underlying to the theoretical considerations outlined under the supply and demand conditions for the instruments of core state power integration are different EU integration theories namely neo-functionalism/supranationalism and liberal intergovernmentalism. Whereas the demand side for core state power integration is primarily driven by neo-functionalism/supranationalism, the supply side is characterized by both supranationalism and liberal intergovernmentalism.

The demand side indicates several reasons for (expanding) cybersecurity integration and cooperation on EU-level. However, the demand for (cyber)security does not automatically generate its own supply. The supply side in particular stresses the importance of EU actors and their ability and willingness to control decisions concerning the extension of EU regulation and capacity-building. The general claim here is that supranational actors push towards core state power (i.e. cybersecurity) integration while Member States are assumed to be more hesitant to pursue such integration steps and rather prefer intergovernmental cooperation. The actual choice of integration instruments is further shaped by the EU areas of competence. Based on the extended theoretical framework and considering the areas of EU competence, certain theoretical expectations were derived.

Regarding variation in regulation (soft vs. hard law) it is expected that supranational actors (Commission and EP) will propose and support hard law acts on cybersecurity issues in areas of shared competence. Member States (through the European Council and Council) are expected to support hard law acts in areas of shared competences. However, Member States are expected to prefer and to adopt soft law acts in intergovernmental policy areas such as the CFSP and CSDP when linked to cyber-issues.

Capacity-building approaches are reflected in the creation of agencies or networks and may take form or direct or indirect initiatives. Supranational actors are expected to propose and support the creation of agencies in areas of shared competence that are linked to cyber-issues. Member States are expected to support the creation of agencies in areas of shared competence whilst demanding considerable control over them. However, in intergovernmental policy areas, Member States are expected to only agree to expand the tasks of pre-existing agencies that can be related to cyber-issues. Supranational actors or Member States are expected to establish networks to enhance competence while for Member States networks can also serve as an alternative to (further) delegation in intergovernmental policy areas that can be related to cyber-issues. Supranational actors are expected to enhance direct capacity-building on EU-level while incentivizing the build-up of national cyber-related capacities by indirect (regulatory) approaches. But in how far can these different theoretical considerations and expectation explain the variation in the EU's approach to cybersecurity. The following section will present the empirical strategy to assess how the theoretical expectations correspond to empirical observations.

7. Research Design and methodology

In order to assess the relevance and relative strength of the theoretical framework that seeks to explain variation in the EU's approach to cybersecurity, congruence analysis is employed (Blatter & Blume 2008; Blatter & Haverland 2012; Blatter et al. 2018). Congruence analysis "focuses on drawing inferences from the (non-)congruence of concrete observations with specified [expectations] from abstract theories to the relevance or relative strength of these theories for explaining/understanding the case(s) under study." (Blatter & Blume 2008, 325). The case study approach allows to gain a more comprehensive understanding of the EU's approach to cybersecurity.

While congruence analysis mainly builds on the rivalry between theories, it is also open to the question whether theories can be seen as complementary or interrelated (Blatter et al. 2018). Underlying to the theoretical framework presented here are different EU integration theories. While acknowledging a certain rivalry between the theoretical expectations stemming from supranationalism (emphasis on supranational actors) on the one hand and liberal intergovernmentalism (emphasis on EU Member States) on the other hand, a combination of both theories to explain variation in the EU's approach to cybersecurity is explored as well. Considering this, employing congruence analysis should further help me to assess explanations for the extent of core state power integration in the case of EU cybersecurity while also pointing to the limits of (cyber)security integration by evaluating and comparing the strength of the theories.

The research design is Y-orientated and focuses on explaining a specific outcome (Blatter et al. 2018; Ganghof 2019). The specific outcome of interest is the variation in the EU's regulatory and capacity-building approach to cybersecurity (Y). For each outlined explanatory approach, the independent variable (X) was identified, and theoretical expectations were formulated accordingly. It is argued that the role of EU actors in decision-making regarding core state power integration is crucial for explaining variance in the regulatory and capacity-building approach to cybersecurity. Supranational actors are generally assumed to drive core state power integration while non-majoritarian actors such as the Council opt for intergovernmental cooperation rather than for further integration in core state power policy areas. The outlined theoretical expectations are assumed to apply under consideration of the different areas of EU competence.

Congruence analysis attempts to draw inferences from the concrete to the abstract: "'Concrete' is defined as the (non-)congruence between predications deduced from theories and empirical observations within one or few cases, whereas 'abstract' refers to the concepts which are the elements of a theory […]." (Blatter & Blume 2008, 341). Theories "provide coherent interpretative frameworks for the understanding and explanation of events and outcomes within a (scientific) discourse." (ibid.). Generalization in the context of congruence analysis is described as "drawing conclusions from these empirical findings for the relative strength or relevance of a theory within a broader set of theories […]." (Blatter & Blume 2008, 342).

Congruence analysis employs interpretative techniques to draw conclusions about the capability of an abstract concept to explain a specific case (Blatter & Blume 2008). The concepts are given their meaning through embedding them into the wider theoretical framework. Interpretation techniques then allow to link and contrast empirical observations with abstract concepts. For the analysis, an expanded theoretical framework (see appendix) was used which encompasses the definition of the relevant concepts, the theoretical backgrounds and expectations under consideration of the demand and supply side as well as the various instruments of core state power integration.

7.1. Case selection

The universe of cases encompasses all core state power integration instruments. In the EU cybersecurity is approached by regulation and capacity-building. Each core state power instrument assumes different forms. As the research interest lays in explaining variation in each of the core state power instruments, a small-n comparative case study between the different forms of regulation (hard/soft law) and capacity-building (agencies/networks and direct/indirect) is conducted. The selection of cases follows the most similar case study design (Seawright & Gerring 2008). Here the cases are selected according to differences only in the outcome (Y) and the independent variable(s) of interest (X). The chosen pair of cases should only differ in this regard but should otherwise be comparable across background conditions (Leuffen 2007; Seawright & Gerring 2008). Underlying to the most similar case design is the logic that the presence or absence of X is what causes variation on Y (Seawright & Gerring 2008).

Based on the theoretical framework, variation of the EU's approach to cybersecurity is assumed to be influenced by the extent to which supranational actors *or* actors on intergovernmental level control decisions concerning regulation and capacity-building and the willingness to use this control for extending and limiting core state power i.e. cybersecurity integration. Every case within each pair of case comparisons is based on one instrument (regulation or capacity-building). Each case is selected out of a possible number of cases per instrument.

The case pairs for comparison differ with regard to the dependent variable (regulation: hard/soft law, capacity building: agency/network; direct/indirect) and the independent variables (supranational actors vs. EU actors on intergovernmental level). Apart from these central differences, the case pairs for comparison should be as similar as possible. Even though cybersecurity sub-areas are "distinct in their focus, these areas all work together towards the protection of the EU's digital infrastructure and residents." (Carrapico & Farrand 2024). As argued before there are several functional demand conditions for cybersecurity integration. The following table summarizes the selection of cases for comparison.

Regulation	**Hard law:** *Cyber Resilience Act*	**Soft law:** *Council Conclusions on the EU Policy on Cyber Defence*
Capacity-building	**Agency** • New: *ENISA* • Task expansion: Europol/*EC3*	**Network:** *European Judicial Cybercrime Network* (Eurojust)
Capacity-building	**Direct:** *CERT-EU*	**Indirect:** *European Defence Fund*

Table 4. *Case selection.*

The first pair of comparison regards the EU's regulatory approach that can either take the form of hard law (regulation or directive) or soft law. The Cyber-Resilience Act (European Parliament & the Council 2024) was selected as a case of hard law (here regulation) and the Council Conclusions on the EU Policy on Cyber Defence (Council of the European Union 2023a) as a case of soft law. The Cyber-Resilience Act sets a minimal level of cyber security for digital products and enhances cybersecurity standards and the Council Conclusions on the EU Policy on Cyber Defence calls for initiatives to secure the EU defence ecosystem. Though addressing different dimensions of cybersecurity, the general emphasis on both regulatory approaches lays on securing technologies and communication systems. Beside the difference in outcome (hard and soft law), both regulatory approaches vary to which extent supranational actors or Member States through the Council can control regulatory decisions. Whereas the Cyber-Resilience Act was subject to the ordinary legislative procedure, the EU Policy on Cyber Defence was decided on intergovernmental level.

The second pair of comparison regards the EU's capacity-building approach which comprises the creation of agencies (or its task expansion) and networks. The European Union Agency for Cybersecurity (known as ENISA) was selected as an agency and Europol with its European Cybercrime Centre (EC3) was selected for a case of agency task expansion. As a network the EJCN which is located at Eurojust was selected. These three capacity-building approaches were selected based on differences in the outcome of interest (agency, agency task expansion or network) and the extent to which supranational actors or Member States can assume a role in these new institutional structures. Whereas the selected agencies (ENISA, Europol/EC3 and Eurojust) now all fall under areas of shared competences, there are indications that in the area of Justice and Home Affairs (JHA) where Europol and Eurojust are located in, both supranational and intergovernmental decision-making modes exist, and the European Council retains a central position in this policy area (Lavenex & Wallace 2005; Maricut 2016; Roos 2017). This leads to the assumption that primarily intergovernmental operational cooperation is preferred in cyber-issues related to JHA (see also Lavenex 2020). More generally the selected agencies and the network are considered comparable as the dimensions of cybersecurity (network and information security and cybercrime) are functionally related. For a direct capacity-building initiative CERT-EU and as an indirect capacity-building initiative the European Defence Fund (EDF)[5] was selected. Both approaches contribute to enhancing EU capacities with regard to dimensions of cybersecurity. However, both approaches differ with regard to the extent to which supranational actors and Member States can partake in capacity-building decisions. Whereas CERT-EU is based on an interinstitutional arrangement for direct EU capacity-building, the EDF (regulation) indirectly supports the creation of cyber capacities.

In the following, the cases are compared and assessed with regard to the congruence of the theories in explaining variation in the EU's approach to cybersecurity. Thereby, both the demand and supply side of the regulatory and capacity-building approaches are explored. I rely on primary sources such as legal texts, press releases from the EU, and secondary literature on the different core state power integration instruments and on the specific cases.

8. Analysis

8.1. Variation in regulation: Approaching cybersecurity by hard law and soft law

8.1.1. Enhancing cybersecurity standards for digital products: The Cyber Resilience Act

"The lack of appropriate cybersecurity in products with digital elements in the Union is due to regulatory and market failures" (Chiara 2022, 256). Market failures "in providing optimal cybersecurity standards" (ibid.) arise due to information asymmetries and negative externalities. On the one hand consumers cannot sufficiently assess the level of cybersecurity of digital products, and on the other hand the cybersecurity market generally is characterized by sup-optimal investment levels and under consumption (Bauer & van Eeten 2009; Chiara 2022; Jardine et al. 2022). Negative externalities arise as "a significant portion of the cost of a cyber attack is borne by others in the network environment." (Jardine et al. 2022, 1). In the context of the EU, regulatory failures emanate from fragmented legal frameworks that only partially address problems

[5] The EDF further exemplifies the link between regulation and (indirect) capacity-building as will be demonstrated.

of cybersecurity provision (Chiara 2022). The recently adopted Cyber Resilience Act can be considered a way to correct these market and regulatory failures through the adoption of harmonised cybersecurity rules (ibid.).

Already in the 2021 State of the European Union Address, president of the European Commission Ursula von der Leyen called for a Cyber Resilience Act (European Commission 2021b). The Cyber Resilience Act was then proposed by the European Commission in 2022 (European Commission 2022a) and, after approval by the EP and Council (European Commission 2023c; Council 2024; European Parliament 2024) entered into force on 10 December 2024 and is directly applicable across the EU (European Parliament & Council 2024). Compliance with the new rules are required from 2027 onwards (BSI 2024; Schmittner et al. 2024).

The regulation considers cyberattacks has having "a critical impact not only on the Union's economy, but also on democracy as well as consumer safety and health." (European Parliament & Council 2024, 1). The aim of the regulation "is to ensure that hardware and software products made available in the EU are rendered cyber-secure, through measures aimed at guaranteeing cybersecurity through a products entire life-cycle" (Carrapico & Farrand 2024, 152). The regulation contains "mandatory requirements for manufactures of products with digital elements" (Chiara 2022, 257). Thereby, software and hardware products will bear the 'CE marking' to indicate compliance with the requirements (Council 2024; European Parliament & Council 2024, 9; see also Schmittner et al. 2024).

The Cyber Resilience Act is further assumed to overcome the fragmented (between the national and EU level) and sectoral (across products) legal frameworks "in relation to cybersecurity requirements for products with digital elements" (Chiara 2022, 256) by ensuring coherence through the new cybersecurity framework (ibid.). The horizontal scope of the regulation encompasses "comprehensive cybersecurity requirements for all products with digital elements" (European Parliament 2024, 2). The new act also complements existing legal frameworks such as the NIS(2)-Directive and the Cybersecurity Act (Chiara 2022).

The Cyber Resilience Act is based on Article 114 TFEU and relates to the functioning of the internal market (see also Carrapico & Farrand 2024; Chiara 2022). The regulation is considered to "give the Commission considerable powers, under the headings of market surveillance and enforcement, including deeming products as non-compliant with the Regulation and as presenting a significant cybersecurity risk based on ENISA assessment." (Carrapico & Farrand 2024, 152). Under the Cyber Resilience Act, the Commission can adopt implementing acts to apply Union-level restrictions (Carrapico & Farrand 2024; Chiara 2022). Under Article

45 of the Cyber Resilience Act (European Parliament & Council 2024, 55) even the withdrawal of non-compliant products from the market is possible.

The regulatory approach is reflective of a market logic (Carrapico & Farrand 2020; Christou 2016; Farrand & Carrapico 2022). Over the years the EU aimed at strengthening cyber security by protecting the economy and society in the Member States and within the EU as a whole (Kipker 2023). Thereby the EU moved from a hands-off approach to a more regulatory hands-on approach (Christou 2016; Porcedda 2023). The EU Commission connects the area of cybersecurity with the protection of the (digital) single market (Kipker 2023; Brandão & Camisão 2022). The 'market-security nexus' (Brandão & Camisão 2022) is evident in several soft and hard law acts that concern EU cybersecurity including the Cyber Resilience Act.

The Commission can enhance its role in (cyber)security-related matters by strategically linking the single market with (cyber)security (Brandão & Camisão 2022). Falling under the area of shared competences (Article 4 TFEU), the Cyber Resilience Act was subject to the ordinary legislative procedure. Support for legally binding acts on part of the EU Member States through the Council cannot be taken for granted. In general, the expectation was that Member States prefer soft law acts over hard law acts. However, the Cyber Resilience Act found quick political agreement between the Commission, the European Parliament and the Council (European Commission 2023c; European Parliament 2023). In 2022, the Council even explicitly called upon the Commission "to propose EU common cybersecurity requirements for connected devices and associated processes and services through the Cyber Resilience Act" (Council 2022, 6).

By referring back to the demand side for regulation, functional reasons for the adoption of the Cyber Resilience Act have clearly outweighed possible sovereignty and legal costs that could be associated with (cyber)security integration. By "establishing uniform cybersecurity standards across domains and markets" (Schmitter et al. 2024, 396) to safeguard digital assets against cyber threats, the regulation reduces transaction costs and contributes to a harmonised market for digital products (see also Sivan-Sevilla 2021). Coherent with the expectation that the Commission approaches cyber security by a market logic, the Cyber Resilience Act is reflective of such approach as it primarily concerns the security of digital products in the single market. Member States showed no opposition to the regulatory approach and did not, contrary to the expectation, opt for a softer approach.

8.1.2. The limits of core state power integration: Council Conclusions on EU Cyber Defence

As cyber-attacks against critical infrastructure are also a component of hybrid warfare and occur in conflicts (Shepherd 2022), the EU started to address cyber defence in its cyber security strategies. Cyber defence is now considered an essential part in the EU's cyber security strategy and was integrated into the CSDP (Christou 2016; Ortiz Hernández 2024). The EU's activity in cyber defence is mainly a reaction to external events such as cyber-attacks on EU Member States (e.g. on Estonia in 2007) and the emergence of hybrid warfare (Carrapico & Farrand 2024; European Commission 2016; 2023; Farrand & Carrapico 2022; Ortiz Hernández 2024; Shepherd 2022). But also, the realization that "cyber defence is a critical element in securing systems and infrastructures against cyber-attacks" (Christou 2016, 119) indicates that a comprehensive cybersecurity approach even extends to the CSDP: Cybersecurity integration in one area spills into functionally related ones. Cybersecurity is not only addressed by a sole market-centered integration logic but by a "security-market relationship" (Liebetrau 2024, 719) where emphasis is increasingly put on security politics.

However, "advancing cyberdefence within the EU has not been easy" (Shepherd 2022, 162) due to "member states' reluctance to provide the EU with a strong role in the areas of foreign, security, and especially defence policy" (ibid.) and divergent perceptions regarding certain cyber defence issues (Deschaux-Dutard 2020; Ortiz Hernández 2024). Cyberdefence is politically sensitive, concerns core state powers and thus raises sovereignty concerns among Member States (Deschaux-Dutard 2020; Shepherd 2022).

The development of a cyberdefence policy and capabilities falls under the CSDP where intergovernmentalism is the "ruling principle" (Deschaux-Dutard 2022, 120) and decisions are taken by unanimity. Intergovernmental policy areas are reflective of "the unwillingness of Member States to give to the EU a central role in a core sovereign competence" (Odermatt 2018, 19). Therefore, EU Member States are expected to only agree on adopting soft law acts in the area of cyber defence. Under Article 24 TEU, the EU can adopt strategies for "a common European defence also in cyberspace." (Ortiz Hernández 2024, 57).

The Council Conclusions on the EU Policy on Cyber Defence (Council 2023a) are illustrative of such soft approach to cyber defence which can be integrated in the EU's general strategies towards cyber defence that evolved over time as a reaction to exogenous and endogenous interdependencies. Adopted in 2023, the Council conclusions stress that the war in Ukraine "had provided a new strategic context and confirmed the need for the EU [and] its

Member States […]" (Council 2023a, 2) "to further strengthen their resilience to cyber threats and enhance its common cyber security and cyber defence against malicious behavior and acts of aggression in cyberspace" (Council 2023c).

The conclusions further "emphasise the importance of investing substantially, both individually and collaboratively, in enhanced resilience and in the deployment of full-spectrum defensive cyber defence capabilities" (Council 2023c) by the help of cooperative frameworks and financial incentives (Council 2024a, 2023c). Other central points of the document include strengthening cooperation and coordination within the EU and the public-private sector, securing the EU defence ecosystem by developing own cyber defence capabilities and reducing strategic dependencies across Member States' capabilities and supply-chains, investing in interoperable cyber defence capabilities and building partnerships on cyber defence policies (Council 2023a; 2023c).

However, the Council Conclusions, with regard to Article 4(2) TEU, note that national security and the cyber domain "remains a sole responsibility of each Member State" (Council 2023a, 3). The Member States decide on their own to "define their goals and actions to implement the EU's objectives." (Ortiz Hernández 2024, 60). What is more, Member States still own the assets deployed in CSDP missions and not the EU itself (Deschaux-Dutard 2020; Shepherd 2022). This demonstrates that at the operational and strategic level of cyberdefence primarily the Member States remain responsible (ibid.). The limits to core state power integration become visible in the case of cyber defence as the Council Conclusions on the EU Policy on Cyber Defence encourage Member States to develop their own cyber defence capabilities and "proactive defensive measures to protect, detect, defend and deter against cyberattacks." (Council 2023a, 10). Further, the Council Conclusions consider the development of "non-legally binding voluntary recommendations inspired by NIS2 to increase cybersecurity in the defence community […]" (Council 2023a, 10) and to "explore […] whether specific voluntary standards for defence systems could be required" (Council 2023a, 11).

Also, with regard to investment in cyber defence capabilities, the Council "encourages Member States to increase their investments" (Council 2023a, 13) and to develop "voluntary commitments for the further development of national cyber defence capabilities" (ibid.). In the final section of the document the Council "invites Member States to voluntarily state their ambition and actions with regards to cyber defence […] and make full use of non-legally binding voluntary recommendations and commitments to step up their national […] cyber defence efforts aiming to maximize the impact at the EU level." (Council 2023a, 18). These are some examples that demonstrate the intergovernmental and voluntary character of the outlined objectives related to the EU Policy on Cyber Defence. Congruent with the expectation that EU Member States prefer soft law instruments and maintain intergovernmental arrangements in the area of the CSDP due to sovereignty concerns, cyber defence integration in the EU remains limited to voluntary commitments.

8.1.3. Comparison of the two regulatory approaches

The variation in the EU's regulatory approach in the form of hard law acts and soft law acts is strongly shaped by the supply side which emphasized the role of EU actors in controlling decisions concerning regulation. Whereas supranational actors such as the Commission favor core state power integration through hard law, EU Member States are assumed to only agree to non-legally binding acts due to sovereignty concerns. As exemplified by the case studies, the choice between hard and soft law acts is influenced by the way cyber-issues are connected to EU areas of competence which in turn determine the extent of decision-making powers of EU actors.

Even though in both cases demand for core state power integration exists, the choice of the regulatory instrument (hard or soft rules) is shaped by the policy area under which the specific cyber-sub area falls. Cyber defence "is a critical element in securing systems and infrastructures against cyber-attacks" (Christou 2016, 119) but both cybersecurity dimensions are governed by different mandates. Whereas cyber defence falls under an intergovernmental policy area, network and information security falls under a shared competence area which made, as in the case of the Cyber Resilience Act, the adoption of a hard legal act possible.

Cyber defence integration remains limited due to the predominance of non-legally binding recommendations. It therefore becomes crucial to consider to what extent the sub-issue areas of cybersecurity actually affect the very core state powers of EU Member States: Cybersecurity integration steps that concern the harmonization of the internal market affect Member State's core state powers less than those concerning (cyber) defence. The EU started to approach network and information security by linking measures in this area to the single market (European Commission 2001b; see also Bendiek & Maat 2019; Farrand & Carrapico 2022). The sub-area of network and information security is primarily driven by an economic logic (Christou 2016; Porcedda 2023; Sivan-Sevilla 2021). Over time the EU moved from a hands-off approach to a more regulatory hands-on approach by creating a common legal framework (Christou 2016; see also Fahey 2014). Soft law has increasingly been replaced by hard law acts in the area of network and information security (Odermatt 2018).

Over time a certain path decency towards the adoption of hard law acts in the area of network and information security and the digital single market developed. Sub-issue areas of cybersecurity that are connected to the single market are more integrated than the cyber defence area which is based on intergovernmental and voluntary cooperation despite a heightened security awareness due to external cyber threats. In general, the variation within the EU's regulatory approach to cybersecurity can mainly be attributed to the different mandates under which cyber sub-areas fall and the extent to which core state powers are affected by the EU's steps towards cybersecurity integration.

By referring back to the theoretical framework it can be concluded that both theories namely supranationalism and liberal intergovernmentalism are relevant in explaining variation within the EU's regulatory approach to cybersecurity. However, as the cybersecurity dimensions fall under different areas of competence, the strength of each theory differs. Whereas supranationalism helps to explain cybersecurity integration by hard law in the area of the single market, intergovernmentalism can provide explanations for the adoption of soft law acts in the area of cyber defence. The Commission has been active in pushing forward cybersecurity integration by a market logic whereas the Member States keep intergovernmental cooperation in the area of cyber defence through the Council. The following section moves on to the EU's different capacity building approaches.

8.2. Variation in capacity-building: New agencies, task expansions and networks

8.2.1. New resources for core state power integration: The European Union Agency for Cybersecurity

Agencies provide the EU resources for exercising core state powers. The European Union Agency for Cybersecurity (ENISA) was established based on the idea to create a point of reference for advice and expertise on cybersecurity on EU level (European Parliament & Council 2004; 2019). ENISA is tasked to reduce fragmentation of the internal market, to contribute to Member State law approximation and to help Member States with the implementation of Union policies related to cybersecurity (European Parliament & Council 2019). From the demand side perspective, the creation of ENISA helped to consolidate security of information and communication technology at EU level. Due to the cross-border nature of cybersecurity and the interconnectedness of societies through network and communication technologies, the creation of European point of reference allows for better coordination and efficiency to respond to cyber threats.

The agency was established by a secondary law act of the European Parliament and the Council (European Parliament & Council 2004; 2013b; 2019). The regulation of ENISA is based on Art. 114 TFEU (with reference to Art. 26 TFEU) which concerns the proper functioning of the single market (European Parliament & Council 2019; Kipker 2023). The regulation of ENISA explicitly states that network and information systems and electronic communication networks are an essential part of the EU's economic growth and "the cornerstone for achieving the digital single market." (European Parliament & Council 2019, 1). Cybersecurity is again approached by a market logic.

The regulation further provides an overview of the agency's structure and organization (see also ENISA 2024a). The agency consists of a management board (ensures that the agency carries out its tasks as laid out by the regulation), an executive board (prepares decisions), an executive director (responsible for managing the agency), a national liaison officers network (facilitates exchange of information between the agency and EU Member States) and an advisory group (draws up work programs, helps to achieve strategic objectives and communicates with stakeholders).

How can the role of ENISA be contextualized against the background of the Commission and the Member States? ENISA should function as the "centre of expertise on cybersecurity" (European Parliament & Council 2019, 34). The agency is tasked to enhance cybersecurity expertise which "is based on a technical risk management perspective in cybersecurity" (Dunn Cavelty & Smeets 2023, 1344). As cybersecurity, a digital security domain, represents a policy field characterized by technological change (Kruck & Weiss 2023), the need for expertise is demanded. The European Commission "as a comparatively small public administration" (Christiansen et al. 2003, 2) requires technical expertise which it cannot find "in-house and [does] not want to rely on from national governments.“ (Christiansen et al. 2003, 2).

In particular, ENISA provides the Commission with relevant resources by offering policy suggestions. The Regulation explicitly mentions that "ENISA should assist the Commission by means of advice, opinions and analyses regarding all Union matters related to policy and law development, updates and reviews in the field of cybersecurity and sector-specific aspects thereof in order to enhance the relevance of Union policies and laws with a cybersecurity dimension and to enable consistency in the implementation of those policies and laws at national level." (European Parliament & Council 2019, 18). Therefore, the Commission can expand its role in a digital security policy domain by relying on ENISA's expertise for the formulation of policies.

For Member States the creation of ENISA can on the one hand be seen as a way to resist any further expansion of the Commission's power and on the other hand as a way to credibly commit to policies and long-term objectives with regard to cybersecurity. ENISA is assigned the mandate to achieve a high common level of cybersecurity on EU level by actively supporting the Member States (Article 3 of Regulation 2019/881). The objectives are confined to assist the Member States in developing and implementing Union policies related to cybersecurity (Article 4 of Regulation 2019/881). ENISA can therefore be characterized as a policy implementation agency (Rittberger et al. 2023). The agency is further tasked to support capacity-building and preparedness of the Member States as well as to promote cooperation and coordination among Member States (Article 4 of Regulation 2019/881). Considering this, ENISA is primarily mandated to regulate, coordinate, and certify the built-up of national capabilities for network and information security (Genschel & Jachtenfuchs 2023). ENISA "does not provide insights into political or strategic questions and stays far away from national security questions." (Dunn Cavelty & Smeets 2023, 1344).

The actual design of agencies can be seen as a compromise between the European Commission, the European Parliament and the Council. Under consideration of the theoretical framework, it was argued that EU actors grant a certain degree of independence and competences to agencies whilst establishing mechanisms to keep agencies under control. In order to carry out their tasks effectively without political interference, agencies need a certain degree of independence (Ruffing et al. 2023; see also Vos 2014).

The founding regulation of an agency provides independence over decision-making processes (e.g. over policy or managerial decisions) and to decision-makers (e.g. independence of agency head and management board) (Ruffing et al. 2023). In this context, the scholarly literature speaks of formal independence[6] as the point of reference for assessing the level of independence is the legal basis of the agency (Rittberger et al. 2024; Ruffing et al. 2023). As a relational concept (Vos 2014), independence must be clarified with regard to the question: From whom should agencies be independent? As the legal basis of the agency is decided by its principals, the independence from the agencies' EU principals, namely the Commission, the EP and the Commission, is primarily meant here. For exploring the agencies' independence, two studies that measure different levels of agency independence over time are considered (Ruffing et al. 2023, Rittberger et al. 2024; see also appendix).

[6] Assessing the *de facto* independence of the agency is beyond the scope of this master thesis and therefore not further explored.

In comparison to other EU agencies, ENISA has a relatively low general level of independence (Ruffing et al. 2023; see also appendix). Even though, the agency evolved over time with a "gradual expansion of its mandate, budget, and operational capacity under subsequent revisions to legislation […]" (Farrand & Carrapico 2021, 30; see also Dunn-Cavelty & Smeets 2023; Ruffing et al. 2023), the general independence level of ENISA remained rather stable. An "incremental process of competence accretion" (Ruffing et al. 2023, 4) does not automatically result in more agency independence in the case of ENISA.

To what extent can ENISA influence decisions? The general level of independence regarding decision-making is rather low for ENISA. Since 2004 when ENISA was founded, the level remained stable until 2019. The general decision-making level of independence increased with the adoption of the Cybersecurity Act in 2019 which enhanced ENISA's role. However, what regards the independence over making policy decisions, ENISA has a very low score that remained unchanged. This corresponds to the outlined mandate of ENISA which is confined to providing expertise and helping with policy implementation. The agency is not mandated to independently decide over policy decisions. Therefore, principals opt for higher controls of the decision-making capacities (Rittberger et al. 2024). In contrast, the level of managerial decision-making independence which concerns the agency's internal organization, recruitment of staff and resources is relatively high. However, the independence level decreased a bit after the adoption of the Cybersecurity Act in 2019. ENISA can act relatively independently from other EU actors when it comes to the general management of the agency.

Moving from independence over decision-making processes to independence of the decision-makers, a relatively high level of independence can be observed. Considering ENISA's role as an implementation agency, principals grant the agency a relatively high level of decision-maker independence that allows the agency to "detect potential implementation problems" (Rittberger et al. 2024, 13). When further differentiating between the agency head and the management board, one can overserve a general decrease in the agency head's independence and an increase in the management board's independence over time due to revisions of the agency's regulation. Despite a still relatively high level of independence, the agency head of ENISA is less independent than the management board. It can be concluded that the agency head can act less independently and is subject to more requirements and obligations while the management board now exhibits a relatively high level of independence.

The design of agencies reflects the balance between independence and control. Principals design "mechanisms that encourage and respect agencies' autonomy but at the same time allow for keeping them under control and holding them accountable for what they do" (Vos

2014, 33). The scholarly literature differentiates between *ex ante* control mechanisms that are determined by the legal boundaries set in the founding regulations of agencies, ongoing (direct) control mechanisms that allow principals to steer and influence the actions of the agencies and *ex post* mechanisms (e.g. the retrospective evaluation of agencies' actions) that aim at ensuring accountability (Vos 2014).

As legislators the European Parliament and the Council are involved in establishing *ex ante* control mechanisms. Such mechanisms find for instance expression in the scope of the agency's' actions and powers and finances (Vos 2014). By referring back to ENISA's regulation, it can be summarized that its mandate mainly evolves around providing expertise and helping Member States with the implementation of policies related to cybersecurity and capacity-building. While acknowledging that cybersecurity as a case of core state power integration significantly proceeded in the EU, ENISA's scope of actions and powers do not interfere with political, strategic or national security issues (Dunn Cavelty & Smeets 2023). By limiting ENISA's scope of actions and powers, principals can *ex ante* ensure control.

More generally, the allocation and approval of the budget for EU agencies can also be considered a form of *ex ante* control (Vos 2014). Principals, namely the Commission who is responsible for the allocation of the EU budget and the European Parliament together with the Council who adopt the budget, are involved in limiting or expanding the financial resources for agencies. Even though ENISA's budget is rather low when compared to other EU agencies, its budget increased over the years (Migliorati 2020) and now amounts to 25 million euro (ENISA 2024c). However, for 2025 the EU did not propose a higher budget for ENISA (Tagesspiegel 2024).

Direct control mechanisms contribute to reducing the agency's autonomy and makes it more dependent of the controlling principals (Vos 2014). Such direct form of control is primarily exerted through the principals' involvement in the organizational structure of an agency. The organizational structure reflects the hybrid character of agencies: Representatives from the Commission and from all Member States sit in the agency management boards (Vos 2014). This direct form of control allows principals to steer and influence the actions of the agencies (ibid.). In the case of ENISA, the management board "should establish the general direction of ENISA's operations and ensure that it carries out its tasks in accordance with [the] Regulation." (European Parliament & Council 2019, 23). Further tasks of the management board are the adoption of the work program and the establishment of the budget.

The presence of Member State representatives in the agencies' management board is assumed to reflect "the Member States' concern that the integrity of their own powers be maintained […]" (Vos 2014, 20), particular in security domains. More generally, the hybrid organizational structure demonstrates "that without Member States acceptance, it is impossible for the EU to develop or carry out regulatory policies.“ (Vos 2014, 29). This is however not to neglect the role of the Commission. The presence of representatives from the Commission in the management boards enables the Commission to "make its voice heard at board meetings." (Egeberg & Trondal 2011, 876).

ENISA's regulation contains no specific direct control mechanisms on part of the EP. However, the current regulation of 2019 (European Parliament & Council 2019) mentions that ENISA should regularly inform the EP about its activities and that the agency has to submit an annual report and a budget report to the EP. Furthermore, the EP can invite the Executive Director on request to report on his or her duties (Regulation 2019/881 Article 36). Prior to his or her appointment, the selected candidate for executive director should be invited to make a statement before the relevant committee of the EP and answer questions. In this context, it should however be mentioned that it is the Commission who proposes a list of candidates for the position of the executive director. The selected candidate is then appointed by the management board (Regulation 2019/881 Article 36). Therefore, the EP is not directly involved in the appointment of the agency head. Instead of possessing direct control mechanisms the role of the EP is to ensure accountability of the agency. Apart from these mechanisms that are based on ENISA's regulation, the EP possesses general accountability mechanisms such as legislative oversight of agencies through written questions (Font & Pérez Durán 2016).

Considering the evolution, structure and mandate of ENISA, it can be summarized that the delegation to ENISA for the exercise of core state powers, is a compromise between the EU principals over granting independence, installing control mechanisms and limiting the scope of agency tasks. Congruent with the expectation that the Commission has further resources at hand for core state power integration and that Member States opt for control mechanisms in the agency's design, it has to be mentioned that ENISA remains an implementation agency which "mainly regulates, coordinates, and certifies the build-up of national network and information security capabilities by the member states" (Genschel & Jachtenfuchs 2023, 1449). This indicates that the EU still depends on Member State's capabilities in (cyber) security matters. The next section proceeds to shed light on how and to what extent the EU can build capacities in the area of cybercrime.

8.2.2. Expanding Europol's tasks: The European Cyber Crime Centre (EC3)

Cybercrime represents one of the most important threats to EU security and stability (Farrand & Carrapico 2021). It has a damaging impact on citizens, governments, businesses in Europe and consequently on economic growth (Christou 2016). The impact of cybercrime can have repercussions on all sectors of societal activity (ibid.). An increase of cybercrime activities is assumed to be the result of new "risks associated with proliferation of new technologies […] the increased technological dependency of Europe […], and the facilitation access to cyber-crime products and services as part of a thriving illegal economy" (Carrapico & Farrand 2021, 25). These external events lay open and create new vulnerabilities and opportunities for criminal activity (ibid.). More generally, demands for cybercrime integration also arise endogenously when considering that cybercrime is part of the wider cybersecurity framework and often overlaps with other dimensions of cybersecurity such as network and information security.

For the EU, reducing and countering cybercrime remains a top political priority (Christou 2016). Considering its global and cross-border nature of cybercrime threats and embeddedness in the wider cybersecurity framework, cooperation between EU Member States and on EU-level is necessary (European Commission 2013a). In order to improve law enforcement and judicial cooperation in cybercrime (Christou 2016) capacity-building efforts are pursued on EU-level. The creation of a central node can help to combat cybercrime, enables the "centralization of information exchanges" (Genschel & Jachtenfuchs 2014, 13) as in the case of Europol and facilitates pooling expertise for cybercrime on EU-level. The EU's capacity-building approach to cybercrime resulted in a task expansion of Europol with the establishment of EC3. This particular institutional choice was shaped by the supply side of core state power integration by capacity-building.

The mandate of Europol is based on Article 88 TFEU and falls under JHA. With the adoption of the Lisbon Treaty, the EU gained specific competence in criminal law which made it possible to advance in cybercrime (Porcedda 2023). The area is now subject the ordinary legislative procedure (see Arts. 82-83 TFEU). Legal instruments in the area of cybercrime are based on Articles 82 and 83 of the TFEU (Carrapico & Barrinha 2017; Carrapico & Farrand 2024; Farrand & Carrapico 2021; 2022).

The policy area of JHA which touches upon core state powers and national sovereignty "could only become communitarized by assuring a central role for the European Council and the Council." (Maricut 2016, 552; see also Busuioc & Groenleer 2013; Roos 2017). Though the Lisbon Treaty introduced supranational elements of the community method such as qualified majority voting and an enhanced role of the EP (also vis-à-vis agencies) some intergovernmental features such as the European Council's presence in agenda-setting, the centrality of the Council in decision-making and the requirement for consensus in the Council on crucial decisions persist in JHA (Lavenex 2020; Maricut 2016). Therefore, JHA is described as a "hybrid policy area" (ibid.) where both supranational and intergovernmental decision-making coexist. This hybridity is reflected in Europol's design.

Europol has become more autonomous from the Member States in terms of funding and staffing which at the same time reduced its autonomy from the Commission and the EP (Busuioc & Groenleer 2013). Though Europol is built on secondary law, the agency has intergovernmental elements in its governance structure and Member States through the Council retain control mechanisms (Busuioc & Groenleer 2013; Lavenex & Wallace 2005; Roos 2017). The agency evolved through a gradual power expansion with regard to different areas of crime (Busuioc & Groenleer 2013; Lavenex & Wallace 2005). Regarding the level of independence, it can be observed that moving JHA to supranational decision-making did not increase Europol's overall independence, it even decreased after the Lisbon Treaty (Ruffing et al. 2023; see also appendix).

Considering the hybridity of the JHA policy area, the expectation was that Member States prefer intergovernmental coordination rather than pursuing further (core state power) integration to tackle cyber issues (see also Lavenex 2020). However, in order to respond to functional demands to address cybercrime, a task expansion of an existing agency (namely Europol) represented a viable option to enhance capacities while maintaining some level of intergovernmental control. The result was the creation of the EC3.

By building on institutional structures, namely Europol, an expansion of actions in cybercrime was achieved by adding the EC3 as a sub-unit. EC3 became permanently embedded in the formal EU agency environment (Christou 2018). With regard to EC3, Europol's regulation mentions that Europol should develop expertise in cybercrime by the help of EC3 (European Parliament & Council 2016b). EC3 falls within the scope of Europol's competence to prevent and combat cybercrime (ibid.). Proposed by the Commission (European Commission 2012) EC3 was set up by Europol.

Established in 2013 (European Commission 2013a), EC3 "is seen as a central node in fighting cybercrime through pooling expertise and information, supporting criminal investigations, promoting EU-wide solutions, and raising awareness of cybercrime issues across the Union." (Christou 2016, 88; see also European Commission 2012). EC3 facilitates coordination within and between member states on cybercrime cases and provides support in operational tasks by facilitating cybercrime cooperation “from investigation to prosecution.” (Christou 2016, 116). In particular EC3 helps to coordinate Member State investigations in cybercrime “in the areas of child sexual abuse, payment fraud, botnets and intrusion.” (Christou 2016, 111). It thereby contributes to “more effective operational coherence” (Christou 2016, 106). To fulfil its tasks EC3 coordinates and collaborates with other relevant EU agencies in the field such as Eurojust. Further tasks are providing training, outreach, strategic analysis as well as technical and digital forensic support (Christou 2016, 112; Europol 2024a.).

“In terms of organizational structure EC3 is […] fully embedded within Europol.” (Europol 2013, 24). On the operational level, EC3 works in three teams: An expertise and stakeholder management team, a document and digital forensic team and an operational team that supports investigations (Europol 2024a). Over the years EC3 was able to support several notable operations in the field of cybercrime (see for example Europol 2023). Furthermore, a program board was established which, among EC3 personnel, includes e.g. representatives from the Commission, the Council, ENISA, CERT-EU, CEPOL, Eurojust and Interpol (Europol 2013). Programme Board meetings allow to bring together relevant actors in cybercrime and cybersecurity for coordination (ibid.). EC3 is financed through Europol’s budget (Europol 2013). The budget of Europol increased drastically over the years and Europol ranks among the agencies with highest budget (Migliorati 2020). For 2023, the budget for Europol was around 200 million Euro (Europol 2023).

By connecting cybercrime with the area of JHA (instead of approaching cybercrime by a sole market logic as in the case of network and information security) the view is reflected that technology abuse can have impacts on different areas of society (Farrand & Carrapico 2021). The link between cybercrime and JHA also allowed the Commission to “reinforce its competence in internal security” (Farrand & Carrapico 2021, 28) by stressing the EU’s role as being “best positioned to support Member States’ coordination in Justice and Home Affairs.“ (ibid.).

The establishment of EC3 allows Member States through the Council to maintain their control mechanisms as the sub-unit is embedded within Europol. Especially under consideration that cybercrime falls into a policy area which is still characterized by intergovernmental structures and in comparison, to network and information security more affects core state power integration and sovereignty concerns of Member States, a task expansion by building a dedicated cybercrime unit seemed the best option. This however did not let Member State’s sovereignty concerns unaffected as Carrapico and Farrand (2018) note: “Whereas the Commission and the Parliament supported a mandatory exchange of information between national competent authorities and EC3, the Council voted to make that exchange voluntary, or alternatively in the form of a summary, as a way to protect member state sovereignty." (152).

In order to respond to functional demands in cybercrime, a task expansion of Europol by embedding EC3 in its general structure allowed the EU to expand its role in JHA and cybercrime as well as Member States to retain control in a policy area that is characterized by strong intergovernmental features which is coherent with the theoretical expectations. However, it also has to be acknowledged that the EC3 supports operational coordination in cybercrime upon request by member states rather than performing operational tasks itself (see Backman 2023). Though the EC3 provides the EU with general capacities, its role remains primarily coordinative with regard to operational tasks.

8.2.3. Improving judicial cooperation in cybercrime: The Judicial Cybercrime Network

The need to complement police cooperation at the EU level through Europol with the coordination of legal proceedings among national authorities led to the creation of Eurojust, the European Union Agency for Criminal Justice Cooperation (Busuioc & Groenleer 2013). Supporting cybercrime investigations by the help of Europol and EC3 in particular also necessitates legal assistance for EU-wide judicial cooperation in cybercrime cases. Endogenous interdependencies developed within the area of cybercrime which in turn created demand for building capacities to enable legal assistance in cybercrime cases. Falling within the scope of Eurojust, cybercrime investigations started to be supported by a network. In 2016, the Council created ECJN (Council 2016b), "which gathers judicial prosecutors and practitioners at European level thereby helping cross-national investigations." (Porcedda 2023, 59). The decision to establish a network for assisting cybercrime investigations was shaped by the supply side of capacity-building.

The network is located within Eurojust. The agency's mandate is based on Article 85 TFEU and also falls under JHA. Just like Europol, Eurojust started as an intergovernmental arrangement (Busuioc & Groenleer 2013). With the adoption of the Lisbon Treaty "the Community method has been made the central legislative mode for developing and reinforcing the mandate of Eurojust […]" (Öberg 2021, 4). The delegation of powers to the supranational level from the Member States are "significant as they determine the mode, operation, design, budget and structure of those agencies." (ibid.).

Being part of the EU's integration efforts in JHA, Eurojust fulfils tasks that closely relate to core state powers and national sovereignty. Its role is confined to assist national judges and prosecutors in cross-border cases thereby providing mutual legal assistance and helping to "improve the coordination of cross-border investigations and prosecutions among the competent authorities of the members and to support them in their cooperation (Busuioc & Groenleer 2013). The overall independence level of Eurojust remained relatively stable over the years and increased with its new regulation in 2018 (Ruffing et al. 2023). Among the other here examined agencies, Eurojust has the highest overall level of independence which corresponds to its operational and coordinative role. Its budget increased over years (Migliorati 2022) and now amounts to around 60 million Euro (Eurojust 2023).

However, as already indicated in the case of Europol/EC3, intergovernmental features also persist in the design of Eurojust (Busuioc & Groenleer 2013; Öberg 2021). This becomes further obvious when considering that the establishment of the ECJN was a Member State initiative (Council 2016b). Establishing a network beside the official agency structure allows Member States to balance functional demands for judicial cross-border cooperation in cybercrime with intergovernmental control. The network provides the necessary tools and resources to improve the capacities with regard to judicial cooperation in cybercrime cases. Furthermore, network structures can be activated more quickly.

When directing attention to the concrete tasks and structure of ECJN it becomes obvious that it primarily represents a Member State's initiative while being embedded within the wider agency framework. ECJN fosters "contacts between practitioners specialised in countering the challenges posed by cybercrime, cyber-enabled crime and investigations in cyberspace, and to increase the efficiency of investigations and prosecutions." (ECJN 2024). The network further "facilitates and enhances cooperation between competent judicial authorities by enabling the exchange of expertise, best practice and other relevant knowledge regarding the investigation and prosecution of cybercrime." (ECJN 2024). In this context the creation of a network alongside an existing agency namely Eurojust helps to enhance its competence with regard to cybercrime. Thereby ECJN also contributes to harmonizing the fragmented institutional landscape by complementing Europol's and EC3's work. The network contributes to enable a more comprehensive approach to tackle cybercrime across the EU.

The ECJN is composed of national representatives of the judicial authorities (Council 2016a). Eurojust supports the work of ECJN by hosting "regular meetings of the network, and supports the exchange of information between the EJCN's members and other stakeholders […]." (ECJN 2024). In addition to that, Eurojust participates in the ECJN Board (Eurojust 2024; see also Council 2016b). Therefore, the ECJN is embedded within the wider framework of Eurojust but functions as an intermediary between the Member State level including national authorities and the EU level to enhance judicial cooperation in cybercrime. Accordingly, the European Commission has no direct control over the network as the ECJN remains a Member State initiative. It can only be argued that the Commission at least has some indirect control over the network due to its embeddedness in Eurojust. This becomes obvious when consulting the reports of the network meetings (see for example Eurojust/ECJN 2023, 2024). The documents indicate that representatives from the Council *and* the European Commission attend the network meetings. Also, representatives from other agencies namely Europol and EC3 (and as already mentioned Eurojust) attend. However, there is no participation of Members from relevant European Parliament committees.

By referring back to the theoretical framework, the establishment of a network alongside an existing agency can be seen as an instance of informal governance. Though, ECJN is located at Eurojust, the network structure allows to act more autonomously for spontaneous coordination in cybercrime cases. This 'in-betweenness' of networks in official agency structures and semi-official arenas allows Member States to preserve their sovereignty while maintaining control in a policy area that concerns core state powers.

It further must be noted that it remains the decision of Member States to cooperate and coordinate at the EU level in cybercrime cases (see Busuioc & Groenleer 2013). Acknowledging that Member States primarily first investigate cybercrime cases on the national level, referring cases to Eurojust and cooperating through the ECJN may become an option when problems arise in solving the case or when multiple countries are involved in cybercrime cases (ibid.). Initiated by the EU Member States the ECJN helps to enhance the competence of Eurojust with regard to judicial cooperation in cybercrime on a more informal level. Coherent with the theoretical expectation that Member States avoid further delegation to the EU level in core state power policy areas, a network allows Member States to decide whether or not to cooperate in judicial matters on EU level.

8.2.4. Comparison of the capacity-building approaches

The creation of EU agencies is indicative of capacity-building. Agencies provide the necessary resources for core state power integration in the case of cybersecurity. As demonstrated there exists variation in which form demands for cybersecurity integration by capacity-building are addressed. The specific form of capacity-building approaches is influenced by the role EU actors assume in the cybersecurity dimensions. It is important to consider that the integration of cybersecurity is approached in a sectoral way. Sub-issue areas of cybersecurity such as network and information security and cybercrime fall under different EU mandates. Network and information security is approached by a market logic. The result was the creation of ENISA. However, the sub-area of cybercrime falls under JHA where Member States still play an important role. Here the EU addressed cybercrime by a task expansion of Europol and the creation of the ECJN at Eurojust. The variation within the EU's capacity-building efforts in cybersecurity can thus mainly be explained by the policy area cybersecurity issues are linked to and the extent to which different EU actors can play a role therein.

When comparing ENISA, Europol/EC3 and the ECJN it becomes clear that ENISA stems from a highly integrated policy area (single market) whereas Europol and Eurojust were initially founded on an intergovernmental basis. Though, cybersecurity generally concerns core state powers, sovereignty concerns can be assumed to be higher in cybercrime which falls under JHA than in the area of network and information security which is linked to the single market. ENISA as an implementation agency provides the Commission with relevant resources such as expertise for policy formulation but it "mainly regulates, coordinates, and certifies the build-up of national network and information security capabilities by the member states" (Genschel & Jachtenfuchs 2023). ENISA's mandate also demonstrates the prevalence of the 'regulatory state' (Kruck & Weiss 2023) and "the build-up and strengthening of national capacities" (Genschel & Jachtenfuchs 2023, 1455).

Both cases, the EC3 and the ECJN, illustrate the intergovernmental and voluntary nature of cooperation in cybercrime. Rather than performing operational tasks, EC3 supports the operational coordination in cybercrime between the Member States. Though, Eurojust as an agency can extend its reach with regard to judicial cooperation in cybercrime via a network, the network remains an intergovernmental and voluntary coordination platform. Even though the predominance of the intergovernmental cooperation level and the associated sovereignty costs in the area of cybercrime and JHA respectively drive the choice of more informal governance forms, the creation of a common point of reference in the case of the EC3 and a network alongside Eurojust do justice to the very nature cybercrime: Tackling cross-border cybercrime requires flexibility, speed and expertise. In addition to that, these rather informal modes reflect the bottom-approach to cybercrime: Member States primarily start operations and investigations on the national level before referring cases to the EU level.

When comparing the capacity-building approaches on a more general level, it can be observed that, irrespective of the actual form these approaches take, certain control mechanisms are established by EU actors in each case. The delegation of powers is therefore always accompanied by a re-balancing of EU principals' existing powers in form of control (Vos 2014) when grating independence to an agent. As illustrated most control mechanisms comprise the representation of (all) EU actors in the organizational structure of agencies or networks. The organizational structure very well reflects the connection between the EU level (i.e. European Commission and European Parliament representation) and the national level (i.e. Council representation).

By referring back to the theoretical framework, both supranationalism and intergovernmentalism are relevant in explaining the variation within the EU's capacity-building approaches. In the case of ENISA, EU actors have decided to delegate some tasks (mainly in the area of policy implementation) to a new agency whose mandate refers to the functioning of the single market, a policy area to which the Commission has been actively linking cyber-issues. In contrast, the cases of EC3 and ECJN illustrate that despite the supranationalization of JHA, intergovernmental arrangements between EU Member States are preferred with regard to cybercrime. Beside these new institutional structures in areas of cybersecurity, further capacity-building approaches are pursued. In the following, direct EU-level capacity-building approaches and indirect forms are explored.

8.3. Variation within the level of capacity-building approaches to cybersecurity

8.3.1. Securing ICT-infrastructure: Direct capacity-building by the creation of CERT-EU

Technological change and the interconnectedness of digital systems also bear cybersecurity risks for European Union institutions (European Parliament & Council 2023). Acknowledging that "the increased use of cloud services, the ubiquitous use of information and communication technology (ICT), the high level of digitalisation, remote work and evolving technology and connectivity are core features of all activities of Union entities" (European Parliament & Council 2023, 1) improving the cyber resilience of the EU institution's information and communication technologies is important. Especially under consideration that EU institutions, bodies and agencies increasingly become targets of cyber-attacks (CERT-EU 2023; ECA 2022; Odermatt 2018), building direct capacities should empower the EU to respond to cyber incidents on its own.

When further acknowledging that the cyber resilience of Union entities varies significantly (European Parliament & Council 2023), the creation of one provider for assistance in cases of cyber incidents for all Union entities can in addition to the implementation of cybersecurity measures contribute to attaining a high *common* level of cybersecurity. A combination of both external events such as the changing cyber threat landscape and endogenous interdependencies that arise due to the technological interconnectedness of Union entities as well as the need to install one cybersecurity provider for all Union entities made it possible to create EU-level capacities. CERT-EU provides the Union entities assistance to respond to cyber threats and can be regarded as an EU-level resource to contribute to a high common level of cybersecurity. The creation of CERT-EU was shaped by the supply side.

CERT-EU's legal basis is the regulation on measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (European Parliament & Council 2023) and its mandate is based upon Article 298 TFEU which concerns the support for the European Administration. CERT-EU is an inter-institutional provider for protecting the information and communication technology infrastructure of all EU institutions and bodies (CERT-EU 2024). It supports the EU to prevent, detect, mitigate and respond to cyberattacks and thereby contributes to Europe-wide incidence response coordination (ibid.). CERT-EU works in various teams which are dedicated to cyber threat intelligence, forensics and operational response, offensive security, cooperation, security development and operation, and security consultation (ibid.).

The initiative for CERT-EU goes back to the European Commission and its Secretariat General (see European Parliament & Council 2023, 4). It is administratively hosted by the Directorate-General for Digital Services of the European Commission and governed by the Inter-institutional Board that is chaired by the European Parliament (CERT-EU 2024). The Interinstitutional Board supervises the objectives by CERT-EU and provides strategic direction to CERT-EU as well as monitors and supports the implementation of the regulation (European Parliament & Council 2023). It is composed of representatives from all EU institutions including the EP, the Council, the Commission and cybersecurity-related agencies such as ENISA and the ECCC (ibid.). CERT-EU cooperates closely with national CSIRTs and is supported by ENISA (Kianpour & Frantz 2024).

Congruent with the expectation that the Commission supported the creation of direct capacities with its CERT-EU initiative, there is however no indication that Member States were not supportive of the initiative and resisted building EU-level capacities. This seems reasonable as the protection of EU entities from cyber incidents does not affect Member State's sovereignty and core state powers. Setting up CERT-EU reflects the general need to secure the EU administration from cyber-attacks. Direct capacity-building approaches as far as they concern the EU-level has overall support from all EU actors as in the case of CERT-EU since they can directly benefit from cybersecurity assistance. Still, CERT-EU is subject to oversight by all relevant EU actors such as the Commission, the Council and the EP through the Interinstitutional Board.

8.3.2. Financing EU cyber defence projects: Indirect capacity-building through the EDF

As already indicated with regard to the regulatory approach, cyber defence became integrated into the CSDP (Christou 2016; Ortiz Hernández 2024) as a reaction to external events such as the increase of cyber-attacks on military and civilian critical infrastructure, the emergence of hybrid warfare and Russia's war against Ukraine. These events have contributed to a heightened security awareness. As "cyber defence is a critical element in securing systems and infrastructures against cyber-attacks" (Christou 2016, 119) a comprehensive EU approach to cybersecurity also requires integration steps in cyber defence.

As Genschel and Jachtenfuchs (2014) argue the need to meet common defence challenges, also in cyberspace, creates demand for the consolidation of defense capacities at the EU level. The pooling of defence resources can lead to lower costs, better coordination and higher effectiveness (Genschel & Jachtenfuchs 2014). Even though there are indications that the EU moved towards defence integration in some respects (see Weiss 2014 for defence procurement and Mérand & Angers 2014 for military integration) and functional demands for capacity-building exist, directing attention to the supply side again may indicate why capacity-building in the (cyber) defence area is more limited and occurs in an indirect way.

Cyber defence falls under the CSDP and remains first and foremost a responsibility of the EU Member States (Shepherd 2022). Members States "can define the European level of governance" (Deschaux-Dutard 2020, 127). Decisions regarding a response to a cyberattack with serious consequences would be decided by the "intergovernmental principle of unanimity in the Council" (ibid., 122). The intergovernmental policy area is reflective of the Member State's reluctance to transfer much control to the EU in the defence sector due to sovereignty concerns and the political sensitivity of the policy area (Deschaux-Dutard 2020; Menon 2014; Odermatt 2018).

As already mentioned, divergent perceptions of the Member States regarding certain cyber defence issues due to the predominance of national strategic cultures regarding cyber defence (Deschaux-Dutard 2020; Ortiz Hernández 2024) also contribute to limiting defence integration. As a consequence, the "EU's cyberdefence capabilities remain rather limited, fragmented, and under-resourced." (Shepherd 2022, 167). In addition to the specific characteristics of the cyber defence policy area, it further must be noted that the EU has little capacity on its own in relation to defence because “it draws on national rather genuinely European power resources.” (Menon 2014, 73; see also Genschel & Jachtenfuchs 2014; 2023). The assets deployed in CSDP missions for example are Member State and not EU owned (Shepherd 2022). Therefore, “EU cyber defence is embedded in a global environment, which encompasses the member states cyber defence architectures […].” (Deschaux-Dutard 2020, 123).

Even though, cyber defence remains a sovereign competence of the Member States, the EU can act as a facilitator (Deschaux-Dutard 2020, 122) by pursuing indirect forms of capacity-building. Such form of capacity-building in (cyber) defence can be traced back to initiatives by the Commission which are based on a market logic. In particular, the Commission stresses the role of the EDF for investments in technologies for cyberdefence to increase technological sovereignty (European Commission 2022b). The European Defence Fund was established in 2021 by a regulation and relates to the competitiveness of the EU’s industry, technological research and development (European Parliament & Council 2021b). The proposal of the EDF goes back to the Juncker-Commission in 2017 (Commission 2017b; see also Hoeffler 2023). Its final adoption is assumed to reflect a compromise between the Commission and the Council over efficiency and sovereignty concerns (Hoeffler 2023). This policy instrument allows to finance projects of military research and development in e.g. cyber defence through the EU budget (Hoeffler 2023; see also Commission 2022).

A cyberdefence-related project financed by the EDF is the ‘EUCINF project’ that is developing a cyber and information warfare toolbox (EDF 2022; EUCINF 2024). The project addresses influence operations and coordinated disinformation campaigns in the realm of Cyber and Information Warfare (EUCINF 2024). It “will study, design, prototype, test and demonstrate cutting-edge capabilities in the domain of cyber information warfare” (Ortiz Hernández 2024, 60). The objective of the project is “to significantly enhance European capabilities in cognitive warfare […] through the development of a shared library […] of innovative configurable software products […].” (EUCINF 2024). For the project several private entities in the field of cybersecurity, defence, space, software development, technological research and threat intelligence were selected from 12 EU countries (EUCINF 2024). Even though the project is in its initial steps, the project aims to develop a “European coherent library of software configurable components” (Commission 2022c) which can be integrated in the Cyber and Information Warfare systems of Member States. Therefore, the project will contribute to improving the Member State’s capabilities with regard to their Cyber and Information Warfare systems. The EDF supports the project with a contribution of 33 million Euro (Ortiz Hernández 2024).

The EDF represents as case of security integration but also marks “a shift in EU policy instruments from market rules in the armament sector toward financing military capacity-building.“ (Hoeffler 2023, 1282). The EDF is also demonstrative of combining both regulation and capacity-building: “Regulation does not take the form of legal market rules but of tangible EU money.” (Hoeffler 2023, 1286). In the case of the EDF military-capacity building is limited to financing defence projects (Hoeffler 2023). The design of the EDF reflects the compromise between the Commission and Member States over the EU’s financing role and ownership of military assets (Hoeffler 2023). As a hybrid form of military capacity-building, the EDF “differs from existing national military capacity-building as the EU has a financing role but does not amount to supranational capacity-building because ownership is national and the centralisation of financial resources at EU level is limited.” (Hoeffler 2023, 1300).

The EU can, as exemplified by the EUCINF-project, indirectly contribute to capacity-building by financing projects in (cyber) defence. Whereas core state power integration does not take form of pooling national military and defence capabilities, the EU can play a financing role in cyber defence. Congruent with the expectation that regulation can indirectly contribute to capacity-building on Member State level, the EDF exemplifies a hybrid instrument for core state power integration.

8.3.3. Comparison of the direct and indirect capacity-building approaches

The EU uses regulation “to stimulate, steer and shape the creation and exercise of national capacities” (Genschel & Jachtenfuchs 2023, 1456). Capacity-building efforts on part of the EU can take indirect forms when the built-up of national capacities is supported by regulation as in the case of the EDF. Direct capacity-building efforts are confined to the EU-level exclusively and should empower the EU to react to cyber threats. CERT-EU represented an illustrative case of direct capacity-building. The difference between both approaches primarily lays in the policy area the cyber-issues fall under. Whereas CERT-EU directly supports the Union institutions, bodies, offices and agencies, the financing of cyber defence projects through the EDF indirectly contributes to enhancing Member States’s cyber and information warfare systems. Direct capacity-building approaches find support when e.g. the whole EU administration benefits from cybersecurity protection.

In contrast, in the area of cyber defence where the EU has a limited role, the EDF represents an option to enhance capacities by financing cyber defence projects. As Hoeffler (2023) stresses the EDF “does not amount to supranational capacity-building” (1300) but reflects a compromise between the Commission and the Member States over efficiency and sovereignty concerns. The EDF allows to finance research and development projects but excludes military acquisition (Hoeffler 2023). It can therefore be concluded that direct capacity-building is confined to cybersecurity areas that leaves core state powers and sovereignty concerns unaffected. This is the case when EU entities and personnel have resources at their disposal to respond to cyber-incidents. Indirect capacity-building (through regulation) is pursued in policy areas where the EU has a limited role and draws on national capacities such as in the case of cyber defence. By referring back to the theoretical framework, building direct capacities on the supranational level is confined to support the EU administration in responding against cyber incidents. Limits to supranationalism become visible in the case of the EDF where the EU fulfils a financing role but can thereby only indirectly enhance Member State's (cyber) defence capabilities.

9. Conclusion

9.1. Empirical findings and limits of the analysis

Starting point of the master thesis was the observation that the EU is active in security policymaking. Conventionally associated with core state powers, the EU even extended its activity in the digital security realm. Cybersecurity is now a central part of the EU's integration efforts. By acknowledging that cybersecurity integration as a case of core state power integration proceeds by regulation and capacity-building, the master thesis aimed to shed light on the question how variation within both integration approaches can be explained. Thereby the master thesis tried to provide a comprehensive account on the different integration instruments. The various EU cybersecurity landscape encompasses soft law, and hard law acts as well as capacity-building initiatives that are direct or indirect and take form of new agencies, agency task expansions or networks.

Building on the core state power literature an expanded theoretical framework was brought forward that takes into consideration the demand and supply side of core state power integration. It was argued that even though demand for cybersecurity integration exists, the actual supply of it depends on the extent to which EU actors control decision-making regarding the extension of regulation and capacity-building. It was assumed that supranational actors such as the Commission generally prefer cybersecurity integration by hard law acts and capacity-building initiatives that take form of new agencies and are built directly on EU-level. In contrast, Member States (acting through the Council) were considered to only selectively pursue cybersecurity integration depending for example on the sovereignty costs associated with such integration steps. Generally, EU Member States (acting through the Council) were assumed to respond to demands for cybersecurity integration by adopting soft law acts and by cooperating through more informal institutional structures such as networks to retain intergovernmental co-operation.

It was further argued that the way cyber-issues are linked to existing EU competencies as laid down by the treaties, determine the choice for core state power integration instruments. Cybersecurity dimensions such as network and information security and cyber defence are governed by different mandates and thus subject to different stages of development and dynamics (Christou 2016). Cyber-issues can be linked to EU areas of shared and intergovernmental competences. This has consequences on how far EU actors can partake in cybersecurity-integration decision-making. Differentiating between sub-areas of cybersecurity has proven to be crucial for understanding the variation in the EU's approach to cybersecurity as this has also consequences on how far sovereignty costs are affected from cybersecurity integration. Linking cybersecurity issues to the single market incurs less sovereignty costs and affects core state powers of the EU Member States less than cyber defence integration.

To assess the relevance of the different theoretical strands of the theoretical framework, a comparative case study of different core state power integration instruments was conducted. Variation within the EU's regulatory approach is expressed through the adoption of both hard law and soft law acts in the area of cybersecurity. By comparing the selected cases, variation in the EU's regulatory approach to cybersecurity can mainly be explained by the role of EU actors in decision-making processes and the area of EU competence to which the relevant cybersecurity dimensions are linked. The adoption of hard law acts (e.g. the Cyber Resilience Act) is made possible in areas of shared competences and in particular when cyber-issues are linked to the single market. Legal acts that require compliance of digital products with cybersecurity standards contribute to the harmonization of the single market and reduce transaction costs.

Congruent with supranationalism, the link between cybersecurity and the market allows the Commission to expand its power and push forward cybersecurity and market integration. Member States did not opt for a softer approach and supported the regulation as the cybersecurity of digital products placed in the single market does not raise any significant sovereignty concerns. In contrast, the CSDP under which cyber defence falls, incurs high sovereignty costs as the core state powers of EU Member States are directly affected. Soft law acts are adopted to set out common goals in cyber defence for example with regard to making defence systems more cyber secure. Falling under an intergovernmental area, the Council adopted a soft law act which emphasized voluntary and non-legally binding recommendations. Congruent with intergovernmentalism, cyber defence remains first and foremost a national responsibility.

When cybersecurity falls under the area of shared competence and relate to the functioning of the internal market, the adoption of hard law is likely. For example, the harmonization of the internal market in cybersecurity is attained by making cybersecurity standards legally binding. In contrast, when cybersecurity falls under the intergovernmental area of the CSDP, the adoption of soft law acts is likely. The Council for example adopts soft law acts in order to voice common goals and to adopt voluntary and non-legally binding standards and frameworks in the area of cyber defence. By referring back to the theoretical framework, it becomes clear that both supernationalism and intergovernmentalism are relevant in explaining variance in core state power integration. Depending to which EU competence area cybersecurity dimensions are linked, the role of supranational and intergovernmental actors is more or less prevalent.

Variation within the EU's capacity-building approach is expressed through the creation of new agencies, agency task expansions and the creation of networks as well as through direct and indirect initiatives. By comparing the selected cases, variation in the EU's capacity-building approach to cybersecurity can mainly be explained by the role of EU actors in decision-making processes and the area of EU competence to which the relevant cybersecurity dimensions are linked. The creation of a new agency (ENISA) was made possible by linking the cybersecurity dimension of network and information security to the functioning of the internal market. An agency provides the Commission with expertise and relevant resources to pursue cybersecurity integration. The case of ENISA showed that an implementation agency mainly regulates, coordinates and certifies the build-up of national network and information security capacities by Member States. The creation of an EU agency allows Member States to credibly commit to long-term policy objectives agreed on EU-level such as in the area of network and information security. The implementation of EU policies on national level is then supported by an agency. Therefore, integration by regulation is complemented by an agency in the case cybersecurity relates to the functioning of the internal market.

In contrast cyber-issues that are linked to JHA are mainly approached by expanding the tasks of existing agencies or by the creation of a network. The choice for these capacity-building approaches is reflective of the intergovernmental arrangements that have existed in JHA. Even though JHA now falls under shared competences, Member States pursue cybercrime mainly on intergovernmental level. Expanding the tasks of Europol by creating EC3 made it possible to pool information and expertise on EU level with regard to cybercrime as well as to enhance coordination and cooperation in cybercrime cases. The ECJN allows for enhancing judicial cooperation in cybercrime with the competent national authorities. Both structures allow to connect law enforcement with judicial cooperation in cybercrime. One the one hand it was argued that Member States retain intergovernmental arrangements within the area of cybercrime as sovereignty costs are higher and core state powers are more affected than in the case of network and information security. On the other hand, these rather informal arrangements in JHA reflect the very nature of cybercrime: Even though cybercrime is a cross-border phenomenon, most investigations start on the national level before EU Member States decide to cooperate on EU-level. Still, even these rather informal structures create basic European resources and capacities from which cooperation and coordination e.g. in the area of cybercrime can be enhanced.

More generally, the case studies have shown that irrespective of the specific form capacity-building approaches take and to which EU competences cyber-areas are linked, granting a certain degree of independence to these bodies is always accompanied by establishing and maintaining control mechanisms (e.g. through the representation of EU-actors in the organizational structure of agencies and bodies or by embedding sub-units or networks in the wider agency framework). The creation of capacities in these forms can therefore be seen as a compromise between supranational actors and EU Member States over responding to demands for core state power integration.

Capacity-building initiatives can either be direct on EU-level or indirect by supporting the built of national capacities through regulation for example. The comparative case study of direct and indirect capacity-building have shown that the EU can build direct capacities when these resources help the EU administration to e.g. react to cyber-incidents. However as far as the (cyber) defence capabilities are concerned, the EU is limited to indirect capacity-building approaches that aim at strengthening national (cyber) defence capabilities e.g. by financing research projects in these areas. The more cyber-dimensions affect core state powers and incur sovereignty costs, the more limited the role of the EU is and the more prevalent is the role of the Member States. Again, capacity-building approaches are reflective of the compromise between the EU and its Member States to address demands for (cyber)security integration.

What is more, the general limits of core state power integration as in the case of cybersecurity, become also visible when considering that the EU is mostly seen as a coordinator and facilitator through its capacity-building initiatives. Considering the cross-border nature of cybersecurity, the EU is well positioned to fulfil this role. The EU further avoids the duplication of national capacities by creating cooperation and coordination hubs as well as by coordinating and supporting existing capacities on national level. Whereas most initiatives do not amount to supranational capacity-building, especially in the area of (cyber) defence (see Hoeffler 2023), the EU continues to rely on national capacities for core state power integration.

In general, most cybersecurity dimensions fall within EU areas of competence where intergovernmentalism predominates. This is particular true for cybercrime and cyberdefence. Cybersecurity dimensions that are linked to the functioning of the internal market are more integrated. Whereas integration in cyberdefence is more limited, network and information security represents a highly integrated sub-area of cybersecurity. Cybercrime falls into the middle of both dimensions as exemplified by the new institutional structures; cooperation mostly remains intergovernmental with a supporting role of the EU.

EU cybersecurity represents a case of core state power integration. As has been shown throughout the analysis, cybersecurity encompasses different dimensions that influence the choice of core state power instruments. Generalizations to other security domains have to be carefully considered. However, the master thesis was first and foremost interested in exploring and explaining variation within the EU's regulatory and capacity-building approaches. Emphasis was put on the role of EU actors in decision-making concerning regulation and capacity-building and the EU's areas of competence to which cybersecurity-dimensions can be linked.

Alternative explanations that were not considered in the theoretical framework for example regard the question how far the demand side can influence the variation in the core state power instruments. It was basically assumed that there exists a general demand for cybersecurity integration. However, it should also be considered that the demand is not equal across cybersecurity dimensions. EU actors may regard some sub-areas of cybersecurity more important than others. The theoretical framework also presupposed that the position of the Council is equal to those of the Member States. Scholars point to certain limits to see both as distinct (see Roos 2017). It would therefore be interesting for future research to explore how national views and cybersecurity strategies are represented on EU level and what impact these positions have on concrete EU initiatives in cybersecurity. This should maybe also shed light on the limitations to (cyber)security integration when e.g. no common position on different cyber-issues can be found.

Further discussion is also required with regard to the very notion of cybersecurity. To draw a more comprehensive picture of the EU's cybersecurity landscape, cybersecurity is understood as encompassing different dimensions that even though they overlap are subject to very different EU competences. Therefore, seeing cybersecurity as a case of core state power has repercussions on how far one can assess the extent to which the integration of cybersecurity sub-areas actually affects core state powers. It was for example shown that network and information security affects core state powers less than cyber defence. Nevertheless, it remains important to have a differentiated view on cybersecurity to understand the EU's activity and limits in this field. Accounting for the very fact that the EU links cybersecurity sub-areas to different competences allows to gain a comprehensive understanding of the EU's cybersecurity landscape which should be maintained in future research.

9.2. Contribution to the core state power integration and EU cybersecurity literature

Though cybersecurity normally falls within the realm of EU Member States, cybersecurity also represents a policy field where the EU can fulfil a coordinating role due to the cross-border nature of cybersecurity. As the master thesis has shown, the EU is active in different cybersecurity dimensions to a varying degree and by various instruments. Considering the EU's activity as a case of core state power integration has allowed to shed light on the variation *within* its regulatory and capacity-building approaches. The master thesis sought to move beyond just differentiating between regulation and capacity-building. By taking account of the EU's cybersecurity landscape, it can be differentiated between soft law and hard law acts in the regulatory approach and between the creation of new agencies, agency task expansions and networks as well as direct and indirect initiatives in the capacity-building approach to cybersecurity.

The identified variation can mainly be attributed to the extent EU actors can partake in decision-making concerning cybersecurity integration and the way cybersecurity sub-areas are linked to areas of EU competence. It is crucial whether supranational actors can push forward cybersecurity integration by linking cybersecurity dimensions to already highly integrated policy areas or whether cybersecurity dimensions are addressed on intergovernmental level. Therefore, the master thesis put special emphasis on the different dimensions on cybersecurity .

The variation within the EU's regulatory approach points towards integration by hard law in case cybersecurity dimensions such as the area of network and information security are linked to the functioning of the internal market. Non-legally binding acts are adopted in cybersecurity sub-areas where decisions are made on intergovernmental level. Representing a less integrated policy area, the adoption of soft law acts in the area cyber defence allows for example to set out common EU goals.

The variation within the EU's capacity-building approach points towards the importance of new EU bodies such as agencies and networks that increasingly complement the EU's administration (Egeberg & Trondal 2011). The capacity-building approaches can be regarded as a compromise between relevant EU actors over responding to functional demands whilst carefully balancing competence and control. As has been shown agencies provide the Commission with relevant resources for policy formulation and help Member States with the implementation of Union policies e.g. in the area of network and information security. More informal modes of governance such as networks enhance operational cooperation and coordination in highly specialized cybersecurity areas such as cybercrime. Direct and indirect capacity-building initiatives have pointed towards the limits of core state power integration and the dependence of the EU on Member State capacities.

9.3. Implications of the findings and avenues for further research

On a more general level, the master thesis claims to adopt a more differentiated view on EU cybersecurity. The fact that cybersecurity sub-areas are linked to different EU competences which in turn influences the choice of core state power instruments, has implications for the EU's approach to cybersecurity. Cybersecurity as a multifaceted phenomenon finds expression in different policy fields as the result of an "increased spillover of EU cybersecurity policy from the Common Market and the Area of Freedom, Security and Justice […] to the Common Foreign and Security Policy […]" (Carrapico & Farrand 2024, 7). Despite falling under different EU policy areas, the dimensions of cybersecurity do converge and overlap (Porcedda 2023; Shepherd 2022). At the same time the variation within EU's capacity-building approaches indicates a certain institutional fragmentation and overlap with regard to the tasks of the agencies, sub-units and networks (Kipker 2023; Shepherd 2022).

This had led scholars to argue that the EU is not a coherent cybersecurity actor (Barrinha & Carrapico 2017). Some identified short-comings in the regulatory approaches and the lack of cooperation and harmonization (Bendiek et al. 2017) have been addressed in recent years e.g. by increased cooperation between relevant agencies and the adoption of laws. The institutional fragmentation and the overlap between task areas seems to be an unavoidable consequence when approaching cybersecurity through different policy areas. Evaluating the effectiveness and coherence of the sectoral approach to cybersecurity in the EU is beyond the scope of this master thesis but opens ways for future research.

Another point concerns the limits of the market-security nexus (Brandão & Camisão 2022; Liebetrau 2024) and the reliance on regulation (Kruck & Weiss 2023) instead of supranational capacity-building (Hoeffler 2023). The EU has pursued cybersecurity integration predominately by linking cyber-issues to the single market and relies mostly on regulation to e.g. incentivize or enhance the built up of national cyber defence capacities. Some cybersecurity dimensions are more integrated than other sub-areas of cybersecurity. The extent of cybersecurity integration and the differences in the EU's regulatory and capacity-building approaches point towards the question what role the EU *should* have in cybersecurity. Is more core state power integration by building supranational capacities demanded or feasible in the long-term or does the EU retain its well-suited coordinative role in cybersecurity?

It is therefore also of relevance to ask whether the EU's (mainly) soft approach to cyberdefence is sufficient considering the increasing geopolitical relevance of cyberspace. For future research it may be also fruitful to consider the impact of securitization (Backman 2022) on shifts in the EU's regulatory and capacity-building approaches in less integrated in cybersecurity sub-areas. Adopting a differentiated view on cybersecurity as illustrated in this master thesis is indispensable for understanding the EU's role in cybersecurity. Insights from the different dimensions of cybersecurity help to identify the potentials and limits of a European cybersecurity approach.

Bibliography

Abbott, K. W., & Snidal, D. (2000). Hard and soft law in international governance. *International Organization*, *54*(3), 421-456. https://doi.org/10.1162/002081800551280

Abbott, K. W., Genschel, P., Snidal, D., & Zangl, B. (2020). Competence-control theory: The challenge of governing through intermediaries. In K.W. Abbott, B. Zangl, D. Snidal, & P. Genschel (Eds.), *The Governor's Dilemma: Indirect Governance Beyond Principals and Agents* (pp. 3-36). Oxford University Press.

Backman, S. (2023). Risk vs. threat-based cybersecurity: The case of the EU. *European Security*, *32*(1), 85-103. https://doi.org/10.1080/09662839.2022.2069464

Balser, M., & Krüger, P.-A. (2024). 'Putins Hacker. Cyberattacken aus Moskau', *Süddeutsche Zeitung*, May 4/5.

Barrinha, A., & Carrapico, H. (2016). The EU's security actorness in cyber space: Quo vadis? In L. Chappell, J. Mawdsley, & P. Petrov (Eds.), *The EU, Strategy and Security Policy: Regional and Strategic Challenges -Routledge Studies in European Security and Strategy* (pp. 104-118). Routledge.

Bauer, J. M., & van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10), 706-719. https://doi.org/https://doi.org/10.1016/j.telpol.2009.09.001

Bendiek, A. (2012). European cyber security policy. *German institute for international and security affairs. Stiftung Wissenschaft und Politik.* https://www.swp-berlin.org/publications/products/research_papers/2012_RP13_bdk.pdf, accessed 08.01.2025.

Bendiek, A., Bossong, R., & Schulze, M. (2017). The EU's revised cybersecurity strategy: Half-hearted progress on far-reaching challenges. *German institute for international and security affairs. Stiftung Wissenschaft und Politik.* https://www.ssoar.info/ssoar/bitstream/handle/document/55103/ssoar-2017-bendiek_et_al-The_EUs_revised_cybersecurity_strategy.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2017-bendiek_et_al-The_EUs_revised_cybersecurity_strategy.pdf, accessed 11.01.2025.

Bendiek, A., & Maat, E. P. (2019). The EU's regulatory approach to cybersecurity. *German institute for international and security affairs, research division EU Working Paper. Stiftung Wissenschaft und Politik.* https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf, accessed 06.12.2024.

Bickerton, C. J., Hodson, D., & Puetter, U. (2015). The new intergovernmentalism: European Integration in the post-Maastricht era. *JCMS: Journal of Common Market Studies*, *53*(4), 703-722. https://doi.org/10.1111/jcms.12212

Biermann, F., & Rittberger, B. (2020). Balancing competence and control. In K.W. Abbott, B. Zangl, D- Snidal, & P. Genschel (Eds.), *The Governor's Dilemma: Indirect Governance Beyond Principals and Agents*, (pp. 180-202). Oxford University Press.

Blatter, J., & Blume, T. (2008). In search of co-variance, causal mechanisms or congruence? Towards a plural understanding of case studies. *Swiss Political Science Review*, *14*(2), 315-356. https://doi.org/10.1002/j.1662-6370.2008.tb00105.x

Blatter, J., & Haverland, M. (2012). *Designing case studies: Explanatory approaches in small-N research*. Palgrave Macmillan.

Blatter, J., Langer, P. C., & Wagemann, C. (2018). *Qualitative Methoden in der Politikwissenschaft*. Springer.

Blauberger, M., & Rittberger, B. (2015). Conceptualizing and theorizing EU regulatory networks. *Regulation & Governance*, *9*(4), 367-376. https://doi.org/10.1111/rego.12064

Börzel, T. A. (2021). *Why noncompliance. The politics of law in the European Union.* Cornell University Press. https://doi.org/doi:10.1515/9781501753411

Brandão, A. P., & Camisão, I. (2022). Playing the market card: The commission's strategy to shape EU cybersecurity policy. *JCMS: Journal of Common Market Studies*, *60*(5), 1335-1355. https://doi.org/10.1111/jcms.13158

Bundesamt für Sicherheit und Informationstechnik (BSI). (2024). Cyber Resilience Act. Cybersicherheit EU-weit gedacht. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html, accessed 17.12.2024.

Busuioc, M., & Groenleer, M. (2013). Beyond design: The evolution of Europol and Eurojust. *Perspectives on European Politics and Society*, *14*(3), 285-304. https://doi.org/10.1080/15705854.2013.817803

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor? *JCMS: Journal of Common Market Studies*, *55*(6), 1254-1272. https://doi.org/10.1111/jcms.12575

Carrapico, H., & Farrand, B. (2018). Cyber crime as a fragmented policy field in the context of the area of freedom, security and justice. In A. Ripoll Servent & F. Trauner (Eds.), *The Routledge Handbook of Justice and Home Affairs Research* (pp. 146-156). Routledge. https://doi.org/10.4324/9781315645629-12

Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of Covid-19: The case of EU cybersecurity policy. *Journal of European Integration*, *42*(8), 1111-1126. https://doi.org/10.1080/07036337.2020.1853122

Carrapico, H., & Farrand, B. (2024). Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. *JCMS: Journal of Common Market Studies*, *62*(1), 147-158. https://doi.org/https://doi.org/10.1111/jcms.13654

Cappellina, B., Ausfelder, A., Eick, A., Mespoulet, R., Hartlapp, M., Saurugger, S., & Terpan, F. (2022). Ever more soft law? A dataset to compare binding and non-binding EU law across policy areas and over time (2004–2019). *European Union Politics*, *23*(4), 741-757. https://doi.org/10.1177/14651165221111985

CEPOL. (2019). CEPOL Cybercrime Academy inaugurated. https://www.cepol.europa.eu/newsroom/news/cepol-cybercrime-academy-inaugurated, assessed 06.12.2024.

CEPOL. (2021). Cybercrime and Cyber-Related Crime. https://www.cepol.europa.eu/thematic-areas/cybercrime-and-cyber-related-crime, accessed 06.12.2024.

CERT-EU. (2023). Russia’s war on Ukraine: One year of cyber operations. https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf, accessed 06.12.2024.

CERT-EU. (2024). About us. https://cert.europa.eu/about-us, accessed 06.12.2024.

Chiara, P. G. (2022). The Cyber Resilience Act: The EU Commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements. *International Cybersecurity Law Review*, *3*(2), 255-272. https://doi.org/10.1365/s43439-022-00067-6

Christensen, J. G., & Nielsen, V. L. (2010). Administrative capacity, structural choice and the creation of EU agencies. *Journal of European Public Policy*, *17*(2), 176-204.

Christiansen, T., Follesdal, A., & Piattoni, S. (2003). *Informal Governance in the European Union: An Introduction.* In T. Christiansen & S. Piattoni (Eds.), *Informal governance in the European Union* (pp. 1-21). Edward Elgar Publishing.

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Springer.

Christou, G. (2018). The challenges of cybercrime governance in the European Union. *European Politics and Society,* 19 (3): 355-375. https://doi.org/10.1080/23745118.2018.1430722

Council of Europe. (2001). Budapest Convention on Cybercrime. https://rm.coe.int/1680081561.

Council of the European Union. (2001). *2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001F0413.

Council of the European Union. (2002). *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32005F0222.

Council of the European Union. (2004). *Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004F0068.

Council of the European. (2005). *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32005F0222.

Council of the European Union. (2008a). *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114.

Council of the European Union. (2008b). *Draft Council conclusions on setting up national alert platforms and a European alert platform for reporting offences noted on the Internet*. https://data.consilium.europa.eu/doc/document/ST-14667-2008-INIT/en/pdf.

Council of the European Union. (2008c). *Council conclusions of 27 November 2008 on a concerted work strategy and practical measures against cybercrime*. https://op.europa.eu/en/publication-detail/-/publication/7707eb72-fdb9-43f3-a4ff-6446403ff624/language-en.

Council of the European Union. (2009). *The Stockholm Programme -An open and secure Europe serving and protecting the citizens*. https://data.consilium.europa.eu/doc/document/ST-17024-2009-INIT/en/pdf.

Council of the European Union. (2010). *Draft Council conclusions on an Action Plan to implement the concerted strategy to combat cybercrime*. https://www.statewatch.org/media/documents/news/2010/mar/eu-council-revised-cyber-crime-conlcusions-5957-rev2-10.pdf.

Council of the European Union. (2013). *European Council 19/20 December 2013 Conclusions*. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/140245.pdf.

Council of the European Union. (2014). *EU Cyber Defence Policy Framework*. https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf.

Council of the European Union. (2015). *Council Conclusions on Cybediplomacy*. https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

Council of the European Union. (2016a). *Council conclusions on the European Judicial Cybercrime Network. Press release*. https://www.consilium.europa.eu/media/24301/network-en.pdf.

Council of the European Union. (2016b). *Draft Council Conclusions on enhancing the capacities of the European Judicial Cybercrime Network (EJCN)*. https://data.consilium.europa.eu/doc/document/ST-15003-2022-INIT/en/pdf.

Council of the European Union. (2017). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy*

Toolbox") -Adoption. https://ccdcoe.org/uploads/2018/11/EU-170607-CyberDiplomacyToolbox-1.pdf.

Council of the European Union. (2018a). *EU Cyber Defence Policy Framework (2018 update)*. https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf.

Council of the European Union. (2018b). *Council Conclusions on EU External Cyber Capacity Building Guidelines*. https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf.

Council of the European Union. (2019). *Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019D0797.

Council of the European Union. (2022). Council Conclusions on the development of the European Union's cyber posture. https://www.consilium.europa.eu/media/56358/st09364-en22.pdf.

Council of the European Union. (2023a). *Council Conclusions on the EU Policy on Cyber Defence*. https://www.consilium.europa.eu/media/64526/st09618-en23.pdf.

Council of the European Union. (2023b). *Revised Implementing Guidelines of the Cyber Diplomacy Toolbox*. https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf.

Council of the European Union. (2023c). Cyber defence: Council conclusions stress the importance of further strengthening the EU's resilience to cyber threats. Press release. https://www.consilium.europa.eu/en/press/press-releases/2023/05/23/cyber-defence-council-conclusions-stress-the-importance-of-further-strengthening-the-eu-s-resilience-to-cyber-threats/, accessed 19.12.2024.

Council of the European Union. (2024). Press Release. Cyber resilience act: Council adopts new law on security requirements for digital product. https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/

CSIRTs Network. (2024). About the CSIRTs Network. https://csirtsnetwork.eu/#about., accessed 06.12.2024.

Delinavelli, Giacomo. (2023). Cybersecurity for Europe without a legal basis? *European Law Blog*. https://doi.org/10.21428/9885764c.e3339223

Deschaux-Dutard, D. (2020). EU cyber defence governance: Facing the fragmentation challenge. In A. Calcara, R. Csernatoni & C. Lavallée (Eds.), *Emerging Security Technologies and EU Governance* (pp. 116-130). Routledge.

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and engineering ethics*, *20*, 701-715.

Dunn Cavelty, M., & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review*, *15*(1), 37-57.

Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy*, *30*(7), 1330-1352. https://doi.org/10.1007/s11948-014-9551-y

EDF. (2022). Selected Projects European Defence Fund (EDF) 2022. EUCINF. European Cyber and Information warfare toolbox. https://defence-industry-space.ec.europa.eu/document/download/abca2b84-bbba-409c-958d-a0767637b76a_en?filename=EUCINF%20-%20Factsheet_EDF22.pdf

Egeberg, M., & Trondal, J. (2011). EU-level agencies: New executive centre formation or vehicles for national control? *Journal of European Public Policy*, *18*(6), 868-887. https://doi.org/10.1080/13501763.2011.593314

Egeberg, M., & Trondal, J. (2017). Researching European Union agencies: What have we learnt (and where do we go from here)? *JCMS: Journal of Common Market Studies*, *55*(4), 675-690. https://doi.org/10.1111/jcms.12525

Egeberg, M., Trondal, J., & Vestlund, N. M. (2015). The quest for order: Unravelling the relationship between the European Commission and European Union agencies. *Journal of European Public Policy*, *22*(5), 609-629. https://doi.org/10.1080/13501763.2014.976587

ENISA. (2024a). Structure and Organisation. https://www.enisa.europa.eu//about-enisa/who-we-are, accessed 06.12.2024.

ENISA. (2024b). EU CyCLONe. European Cyber Crises Liasion Organisation Network. https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone, accessed 06.12.2024.

ENISA. (2024c). ENISA annual report on budgetary and financial management 2023. https://www.europarl.europa.eu/cmsdata/283436/ENISA%20RBFM%202023.pdf

Eurojust. (2021). Eurojust Annual Report 2021. https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-annual-report-2021.pdf

Eurojust. (2023). Eurojust budget 2023. https://www.eurojust.europa.eu/document/eurojust-budget-2023, accessed 31.12.2024.

Eurojust. (2024). European Judicial Cybercrime Network. https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network, accessed 06.12.2024.

Eurojust/ECJN. (2023). European Judicial Cybercrime Network 14th Plenary Meeting - Outcome Report. https://www.eurojust.europa.eu/sites/default/files/assets/european-judicial-cybercrime-network-14th-plenary.pdf

Eurojust/ECJN. (2024). 16th Plenary Meeting of the European Judicial Cybercrime Network - Outcome Report. https://www.eurojust.europa.eu/sites/default/files/assets/european-judicial-cybercrime-network-16th-plenary-outcome-report.pdf

European Commission. (1996). Commission on illegal and harmful content on the internet. http://aei.pitt.edu/5895/1/5895.pdf

European Commission. (2001a). *Communication from the Commission to the European Parliament, the European Economic and Social Committee and the Committee of the Regions -Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF*

European Commission. (2001b). *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions -Network and Information Security: Proposal for A European Policy Approach. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF*

European Commission. (2005). Green Paper on a European programme for critical infrastructure protection. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576

European Commission. (2006a). Communication. Strategy for a Secure Information Society. https://eur-lex.europa.eu/EN/legal-content/summary/strategy-for-a-secure-information-society-2006-communication.html

European Commission. (2006b). Communication from the Commission on a Programme for Critical Infrastructure Protection. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

European Commission. (2007). *Communication from the Commission: Towards a general policy on the fight against cyber crime*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52007DC0267

European Commission. (2009). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions -Critical Information Infrastructure Protection. Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52009DC0149

European Commission. (2010a). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions -A Digital Agenda for Europe.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

European Commission. (2010b). *Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF

European Commission. (2012). *Communication to the Council and the European Parliament Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre.* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2012:140:FIN

European Commission. (2013a). European Cybercrime Centre (EC3) opens on 11 January. Press release. https://ec.europa.eu/commission/presscorner/detail/en/ip_13_13, accessed 30.12.2024.

European Commission. (2013b). *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* -Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001

European Commission. (2016). *Joint Communication to the European Parliament and the Council - Joint Framework on countering hybrid threats a European Union response. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018*

European Commission. (2017a). *Joint Communication to the European Parliament and the Council -Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.* https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52017JC0450

European Commission. (2017b). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions -Launching the European Defence Fund. https://ec.europa.eu/docsroom/documents/23605

European Commission. (2020a). *Joint Communication to the European Parliament and the Council -The EU's Cybersecurity Strategy for the Digital Decade.* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018

European Commission. (2020b). *Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829

European Commission. (2020c). *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

European Commission. (2021a). *Commission Recommendation (EU) 2021/1086 of 23 June 2021 on building a Joint Cyber Unit.* http://data.europa.eu/eli/reco/2021/1086/oj

European Commission. (2021b). State of the Union Address by President von der Leyen. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701, accessed 17.12.2024.

European Commission. (2022a). Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454

European Commission. (2022b). *Joint Communication to the European Parliament and the Council -EU Policy on Cyber Defence. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022JC0049*

European Commission. (2022c). EU Funding and Tenders Portals. Cyber and information warfare toolbox. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2022-da-cyber-ciwt, accessed 05.01.2025.

European Commission. (2023a). *Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0209*

European Commission. (2023b). *Enhancing EU resilience: A step forward to identify critical entities for key sectors. Press release.* https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992, accessed 06.12.2024.

European Commission. (2023c). Commission welcomes political agreement on Cyber Resilience Act. Press release. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6168, accessed 16.12.2024.

European Commission. (2024a). NIS-Cooperation Group. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group, accessed 06.12.2024.

European Commission. (2024b). The EU Cyber Solidarity Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity, accessed 06.12.2024.

EU Cyber Direct 2024. (2024). Supporting the EU's cyber diplomacy. https://eucyberdirect.eu/about, accessed 12.12.2024.

European Court of Auditors. (2022). Special report. Cybersecurity of EU institutions, bodies and agencies – Level of preparedness overall not commensurate with the threats. https://op.europa.eu/webpub/eca/special-reports/hack-proofing-eu-institutions-05-2022/en/, accessed 02.01.2025.

European Union. (2022). Division of competences within the European Union. https://eur-lex.europa.eu/EN/legal-content/summary/division-of-competences-within-the-european-union.html, accessed 06.12.2024.

European Union. (2024). EU Interinstitutional Service. Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies (CERT-EU). https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/cybersecurity-service-union-institutions-bodies-offices-and-agencies-cert-eu_en, accessed 06.12.2024.

Europol. (2013). First year report. https://www.europol.europa.eu/sites/default/files/documents/ec3_first_year_report.pdf

Europol. (2023). Consolidated Annual Activity Report 2023. Europol Public Information. https://www.europarl.europa.eu/cmsdata/286518/Europol%20CAAR%202023.pdf.

Europol. (2024a). European Cybercrime Centre EC3. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, accessed 06.12.2024.

Europol. (2024b). Joint Cybercrime Action Taskforce (J-CAT). https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce, accessed 06.12.2024.

European Cybersecurity Competence Centre (ECCC). (2024a). About the European Cybersecurity Competence Centre. https://cybersecurity-centre.europa.eu/about-us_en, accessed 06.12.2024.

European Cybersecurity Competence Centre (ECCC). (2024b). National Coordination Centres. https://cybersecurity-centre.europa.eu/nccs-0_en, accessed 06.12.2024.

European Defence Agency. (2013). *Cyberdefence Factsheet.* https://eda.europa.eu/docs/default-source/eda-factsheets/2013-11-19-factsheet_cyber_defence, accessed 06.12.2024.

European Defence Agency. (2021). *Cyber defence built on European Cooperation.* https://eda.europa.eu/docs/default-source/brochures/2021-eda-cyber-defence.pdf, accessed 06.12.2024.

European Defence Agency. (2023). *EDA-led network of cyber defence teams starts with 18 EU countries*. https://eda.europa.eu/news-and-events/news/2023/02/10/eda-led-network-of-cyber-defence-teams-starts-with-18-eu-countries, accessed 06.12.2024.

European Parliament. (2017). *European Parliament resolution of 3 October 2017 on the fight against cybercrime.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0366.

European Parliament. (2021). *Recent Cyber-Attacks and the EU's Cybersecurity Strategy for the Digital Decade.* https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690639/EPRS_ATA(2021)690639_EN.pdf, accessed 06.12.2024.

European Parliament. (2023). Cyber Resilience Act: agreement with Council to boost digital products' security. Press release. https://www.europarl.europa.eu/news/en/press-room/20231106IPR09007/cyber-resilience-act-agreement-with-council-to-boost-digital-products-security, accessed 17.12.2024.

European Parliament. (2024). Cyber Resilience Act: MEPs adopt plans to boost security of digital products. Press release. https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products, accessed 16.12.2024.

European Parliament & the Council. (2001). *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32001L0029

European Parliament & the Council. (2004). *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

European Parliament & the Council. (2008). *Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:293:0001:0002:EN:PDF

European Parliament & the Council. (2009). *Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

European Parliament & the Council. (2011a). *Regulation (EU) No 580/2011 2008 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.* https://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1

European Parliament & the Council. (2011b). *Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32011L0093

European Parliament & the Council. (2013a). *Proposal for a Directive to the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union*. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52013PC0048

European Parliament & the Council. (2013b). *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN

European Parliament & the Council. (2016a). *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.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

European Parliament & the Council. (2016b). *Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol)*. http://data.europa.eu/eli/reg/2016/794/oj

European Parliament & the Council. (2019). *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 5.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

European Parliament & the Council. (2021a). *Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0887

European Parliament & Council. (2021b). *Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0697

European Parliament & the Council. (2022a). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).* https://eur-lex.europa.eu/eli/dir/2022/2555

European Parliament & the Council. (2022b). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. http://data.europa.eu/eli/dir/2022/2557/oj

European Parliament & the Council. (2023). Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. https://eur-lex.europa.eu/eli/reg/2023/2841/oj

European Parliament & the Council. (2024). *Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*. https://data.consilium.europa.eu/doc/document/PE-100-2023-REV-1/en/pdf

European Union. 2024. Legislative summary of the EU Cybersecurity Act. https://eur-lex.europa.eu/EN/legal-content/summary/the-eu-cybersecurity-act.html, accessed 06.12.2024.

Fahey, E. (2014). The EU's cybercrime and cyber-security rulemaking: Mapping the internal and external dimensions of EU security. *European journal of risk regulation*, *5*(1), 46-60. https://doi.org/10.1017/S1867299X00002944

Farrand, B., & Carrapico, H. (2021). The how and why of cybercrime: The EU as a case study of the role of ideas, interests, and institutions as drivers of a security-governance approach. In A. Lavorgna & T. J. Holt (Eds.), *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches* (pp. 23-41). Palgrave Macmillan Cham.

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435-453. https://doi.org/10.1080/09662839.2022.2102896

Font, N., & Pérez Durán, I. (2016). The European Parliament oversight of EU agencies through written questions. *Journal of European Public Policy*, *23*(9), 1349-1366. https://doi.org/10.1080/13501763.2015.1076875

Ganghof, S. (2019). Das y-zentrierte Forschungsdesign. In S. Ganghof (Ed.), *Forschungsdesign in der Politikwissenschaft: Eine theorieorientierte Perspektive mit Anwendungsbeispielen* (pp. 25-31). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-24260-2_5

Genschel, P., & Jachtenfuchs, M. (Eds.) (2014). *Beyond the regulatory polity? The European integration of core state powers*. Oxford University Press.

Genschel, P., & Jachtenfuchs, M. (2016). More integration, less federation: The European integration of core state powers. *Journal of European Public Policy*, *23*(1), 42-59. https://doi.org/10.1080/13501763.2015.1055782

Genschel, P., & Jachtenfuchs, M. (2018). From market integration to core state powers: The Eurozone crisis, the refugee crisis and integration theory. *JCMS: Journal of Common Market Studies*, *56*(1), 178-196. https://doi.org/10.1111/jcms.12654

Genschel, P., & Jachtenfuchs, M. (2023). The security state in Europe: Regulatory or positive? *Journal of European Public Policy*, *30*(7), 1447-1457. https://doi.org/10.1080/13501763.2023.2174580

Haas, E. B. (1961). International Integration: The European and the Universal Process. *International Organization*, *15*(3), 366-392. https://doi.org/10.1017/S0020818300002198

Hoeffler, C. (2023). Beyond the regulatory state? The European Defence Fund and national military capacities. *Journal of European Public Policy*, *30*(7), 1281-1304. https://doi.org/10.1080/13501763.2023.2174581

Hooghe, L., & Marks, G. (2019). Grand theories of European integration in the twenty-first century. *Journal of European Public Policy*, *26*(8), 1113-1133. https://doi.org/10.1080/13501763.2019.1569711

Jardine, E., Leverett, É., & Geer, D. (2022). Ransomware: Externalities, cost internalization, and security investment intentionality. https://ostromworkshop.indiana.edu/pdf/seriespapers/2022spr-colloq/jardine.pdf, accessed 16.12.2024.

Justaert, A., Keukeleire, S., Christiansen, T., & Neuhold, C. (2012). Informal governance and networks in EU foreign policy. In T. Christiansen & C. Neuhold (Eds.), *International Handbook on Informal Governance* (pp. 433-456). Edward Elgar Publishing.

Kaunert, C., Léonard, S., & Occhipinti, J. D. (2013). Agency governance in the European Union's Area of Freedom, Security and Justice. *Perspectives on European Politics and Society*, *14*(3), 273-284. https://doi.org/10.1080/15705854.2013.817806

Kelemen, D. (2005). The politics of Eurocracy: Building a new European state? In N. Jabko & C. Parsons (eds.) *The State of the European Union: With US Or Against US? European Trends in American Perspective Volume 7* (pp. 173-192). Oxford University Press.

Kelemen, D. (2012). EU agencies. In E. Jones, A. Menon, & S. Weatherill (Eds.), *The Oxford Handbook of the European Union* (pp. 392-403). Oxford University Press.

Kelemen, D., & McNamara, K. R. (2022). State-building and the European Union: Markets, War, and Europe's Uneven political development. *Comparative Political Studies*, *55*(6), 963-991. https://doi.org/10.1177/00104140211047393

Kelemen, D., & Majone, G. (2012). Managing europeanization: The European agencies. In J. Peterson, & M. Shackleton (Eds.), *The Institutions of the European Union third edition* (pp. 219-240). Oxford University Press.

Kelemen, R. D., & Tarrant, A. D. (2011). The political foundations of the Eurocracy. *West European Politics*, *34*(5), 922-947. https://doi.org/10.1080/01402382.2011.591076

Kianpour, M., & Frantz, C. (2024). Analysis of institutional design of European Union cyber incident and crisis management as a complex public good. *Regulation & Governance. Online first.* https://doi.org/https://doi.org/10.1111/rego.12640

Kipker, D.-K., Barudi, M., Beucher, K., & Bird, R. (2023). *Cybersecurity Rechtshandbuch*. (2nd ed.). C.H. Beck.

Krahmann, E. (2003). Conceptualizing security governance. *Cooperation and conflict*, *38*(1), 5-26. http://www.jstor.org/stable/45083967, accessed 06.12.2024.

Kruck, A., & Weiss, M. (2023). The regulatory security state in Europe. *Journal of European Public Policy*, *30*(7), 1205-1229. https://doi.org/10.1080/13501763.2023.2172061

Lavenex, S, & Wallace, W. (2005). Justice and Home Affairs. In H. Wallace, W. Wallace, & M. A. Pollack (Eds.), *Policy-making in the European Union* (5th ed.) (pp. 457-479). Oxford University Press.

Lavenex, S. (2020). Justice and Home Affairs: Exposing the limits of political integration. In H. Wallace, M. A. Pollack, C. Roederer-Rynning, & A. R. Young, A. (Eds.) *Policy-making in the European Union* (8th ed.). Oxford University Press.

Leuffen, D. (2007). Fallauswahl in der qualitativen Sozialforschung. In T. Gschwend, & F. Schimmelfennig (Eds.), *Forschungsdesign in der Politikwissenschaft* (pp. 201-222). Campus Verlag.

Levi-Faur, D. (2011). Regulatory networks and regulatory agencification: Towards a Single European Regulatory Space. *Journal of European Public Policy*, *18*(6), 810-829. https://doi.org/10.1080/13501763.2011.593309

Liebetrau, T. (2024). Problematising EU Cybersecurity: Exploring how the Single Market functions as a security practice. *JCMS: Journal of Common Market Studies, 62*(3), 705-724. https://doi.org/https://doi.org/10.1111/jcms.13523

Mahoney, J., & Thelen, K. (2010). A theory of gradual institutional change. In J. Mahoney, & K. Thelen (Eds.), *Explaining institutional change: Ambiguity, agency, and power* (pp. 1-37). Cambridge University Press.

Majone, G. (1997). From the positive to the regulatory state: Causes and consequences of changes in the mode of governance. *Journal of public policy*, *17*(2), 139-167. https://doi.org/10.1017/S0143814X00003524

Maricut, A. (2016). With and without supranationalisation: The post-Lisbon roles of the European Council and the Council in justice and home affairs governance. *Journal of European Integration*, 38(5), 541-555. https://doi.org/10.1080/07036337.2016.1178253

Menon, A. (2014). Defence policy and the logic of 'high politics'. In P. Genschel & M. Jachtenfuchs (Eds.), *Beyond the regulatory polity? The European integration of core state powers* (pp. 66-86). Oxford University Press.

Mérand, F., & Angers, K. (2014). Military integration in Europe. In P. Genschel & M. Jachtenfuchs (Eds.), *Beyond the regulatory polity? The European integration of core state powers* (pp. 46-65). Oxford University Press.

Migliorati, M. (2020). The post-agencification stage between reforms and crises. A Comparative assessment of EU agencies' budgetary development. *JCMS: Journal of Common Market Studies*, *58*(6), 1393-1412. https://doi.org/https://doi.org/10.1111/jcms.13044

Moravcsik, A. (1998). *The choice for Europe. Social purpose and state power from Messina to Maastricht*. Cornell University Press, Ithaca.

Moravcsik, A., & Schimmelfennig, F. (2019). Liberal Intergovernmentalism. In A. Wiener, T.A. Börzel, & T. Risse (Eds.), *European Integration Theory*. 3rd edition. (pp. 64-84). Oxford University Press.

Moret, E. & Pawlak, P. (2017). *The EU Cyber Diplomacy Toolbox – Towards a cyber sanctions regime?* European Union Institute for Security Studies. https://data.europa.eu/doi/10.2815/399444

Niemann, A., Lefkofridi, Z., & Schmitter, P. C. (2019). Neofunctionalism. In A. Wiener, T.A. Börzel, & T. Risse (Eds.), *European Integration Theory*. 3rd edition (pp. 43-63). Oxford University Press.

Öberg, J. (2021). Guest editorial: EU agencies in transnational criminal enforcement: From a coordinated approach to an integrated EU criminal justice. *Maastricht Journal of European and Comparative Law*, *28*(2), 155-163. https://doi.org/10.1177/1023263x211005977

Odermatt, J. (2018). The European Union as a cybersecurity actor. *iCourts Working Paper Series*, 128: 1-20. https://dx.doi.org/10.2139/ssrn.3144257

Ortiz Hernández, E. (2024) Towards the autonomous defence capabilities of the European Union: Upgrading cyber defence policy. *Global Policy*, *15*(S8), 57–62. Available from: https://doi.org/10.1111/1758-5899.13412

PESCO. (2024a). PESCO Projects. https://www.pesco.europa.eu, accessed 06.12.2024.

Porcedda, M. G. (2023). *Cybersecurity, privacy and data protection in EU Law: A law, policy and technology analysis. Hart Studies in Information Law and Regulation*. Bloomsbury Publishing.

Puetter, U. (2012). Europe's deliberative intergovernmentalism: The role of the Council and European Council in EU economic governance. *Journal of European Public Policy*, *19*(2), 161-178. https://doi.org/10.1080/13501763.2011.609743

Reitano, T., Oerting, T., & Hunter, M. (2015). Innovations in international cooperation to counter cybercrime: The joint cybercrime action taskforce. *The European Review of Organised Crime*, *2*(2), 142-154. https://standinggroups.ecpr.eu/sgoc/wp-content/uploads/sites/51/2020/01/reitanoetal.pdf

Rittberger, B., Ruffing, E., Weinrich, M., & Wonka, A. (2024). The competence-control dilemma and the institutional design of European Union agencies. *Governance, 37*(4), 1413–1431. https://doi.org/10.1111/gove.12858

Roos, C. (2017). The Council and European Council in EU Justice and Home Affairs Politics. In A. Ripoll Servent & F. Trauner (Eds.), *The Routledge Handbook of Justice and Home Affairs Research* (1st ed.) (pp. 421-433). Routledge. https://doi.org/10.4324/9781315645629

Ruffing, E. (2022). European (networked) agencies between independence and influence. *Journal of European Public Policy*, *29*(10), 1546-1567. https://doi.org/10.1080/13501763.2022.2069844

Ruffing, E., Weinrich, M., Rittberger, B., & Wonka, A. (2023). The European administrative space over time: Mapping the formal independence of EU agencies. *Regulation & Governance*, 18: 740-760. https://doi.org/10.1111/rego.12556

Sandholtz, W., & Sweet, A. S. (2012). Neo-Functionalism and supranational governance. In In J. Erik, M. Menon, & S. Weatherill (Eds.), *The Oxford Handbook of the European Union* (pp.18-33). Oxford University Press.

Schmittner, C., Veledar, O., Faschang, T., Macher, G., Brenner, E. (2024). Fostering cyber resilience in Europe: An in-depth exploration of the Cyber Resilience Act. In M. Yilmaz, P. Clarke, A. Riel, R. Messnarz, C. Greiner, & T. Peisl (Eds.), *Systems, Software and Services Process Improvement.* Springer, Cham. https://doi.org/10.1007/978-3-031-71139-8_26

Schimmelfennig, F. (2018). European integration (theory) in times of crisis. A comparison of the euro and Schengen crises. *Journal of European Public Policy*, *25*(7), 969-989. https://doi.org/10.1080/13501763.2017.1421252

Schimmelfennig, F., Leuffen, D., & Rittberger, B. (2015). The European Union as a system of differentiated integration: Interdependence, politicization and differentiation. *Journal of European Public Policy*, *22*(6), 764-782. https://doi.org/10.1080/13501763.2015.1020835

Seawright, J., & Gerring, J. (2008). Case Selection Techniques in Case Study Research: A menu of qualitative and quantitative options. *Political Research Quarterly*, *61*(2), 294-308. https://doi.org/10.1177/1065912907313077

Shepherd, A. J. (2022). *The EU security continuum: Blurring internal and external security*. Routledge.

Sivan-Sevilla, I. (2021). Europeanisation on demand: The EU cybersecurity certification regime between market integration and core state powers (1997–2019). *Journal of public policy*, *41*(3), 600-631. https://doi.org/10.1017/S0143814X20000173

Streeck, W., & Thelen, K. (2005). Introduction: Institutional change in advanced political economies. In W. Streeck, & K. Thelen (Eds.), *Beyond continuity: institutional change in advanced political economies* (pp. 1-39). Oxford University Press.

Sweet, A. S., & Sandholtz, W. (1997). European integration and supranational governance. *Journal of European Public Policy*, *4*(3), 297-317. https://doi.org/10.1080/135017697800000011

Sytas, A., Erling, B., & Ahlander, J. (2024). 'European nations denounce Russian hybrid attacks, cable cut probes launched', Reuters, November 19. https://www.reuters.com/business/media-telecom/lithuania-steps-up-surveillance-sea-following-damage-undersea-cable-2024-11-19/, accessed 08.01.2025.

Tagesspiegel. 12.12.2024. EU-Rat lobt Enisa und fordert mehr Ressourcen. https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/eu-rat-lobt-enisa-und-fordert-mehr-ressourcen, last accessed 29.12.2024.

Terpan, F. (2015). Soft law in the European Union—The changing nature of EU law. *European Law Journal*, *21*(1), 68-96. https://doi.org/10.1111/eulj.12090

Terpan, F., & Saurugger, S. (2021). Soft and hard law in times of crisis: Budget monitoring, migration and cybersecurity. *West European Politics*, *44*(1), 21-48. https://doi.org/10.1080/01402382.2020.1738096

Thatcher, M. (2011). The creation of European regulatory agencies and its limits: A comparative analysis of European delegation. *Journal of European Public Policy*, *18*(6), 790-809. https://doi.org/10.1080/13501763.2011.593308

Treaty on European Union. (2012). OJ 326, 26.10.2012, p. 18. *Article 4*. http://data.europa.eu/eli/treaty/teu_2012/art_4/oj

Treaty on European Union. (2012). OJ 326, 26.10.2012, pp. 30–31. *Article 24*. http://data.europa.eu/eli/treaty/teu_2012/art_24/oj

Treaty on European Union. (2012). OJ 326, 26.10.2012, pp. 38-41. *Articles 42-46*. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF

Treaty on the Functioning of the European Union. (2016) *OJ C 202, 7.6.2016, p. 50. Article 2.* http://data.europa.eu/eli/treaty/tfeu_2016/art_2/oj

Treaty on the Functioning of the European Union. (2016) *OJ C 202, 7.6.2016, p. 51. Article 3.* http://data.europa.eu/eli/treaty/tfeu_2016/art_3/oj

Treaty on the Functioning of the European Union. (2016). *OJ 202, 7.6.2016, p. 59. Article 26.* http://data.europa.eu/eli/treaty/tfeu_2016/art_26/oj

Treaty on the Functioning of the European Union. (2016).*OJ 202, 7.6.2016, p. 38–39. Article 42.* http://data.europa.eu/eli/treaty/teu_2016/art_42/oj

Treaty on the Functioning of the European Union. (2008). *OJ 115, 9.5.2008, p. 79–80. Article 82.* http://data.europa.eu/eli/treaty/tfeu_2008/art_82/oj

Treaty on the Functioning of the European Union. (2008). *OJ 115, 9.5.2008, p. 80–81. Article 83.* http://data.europa.eu/eli/treaty/tfeu_2008/art_83/oj

Treaty on the Functioning of the European Union. (2016). *OJ C 202, 7.6.2016, p. 81–82. Article 85.* http://data.europa.eu/eli/treaty/tfeu_2016/art_85/oj

Treaty on the Functioning of the European Union. (2016). *OJ 202, 7.6.2016, p. 84. Article 88.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12016E088

Treaty on the Functioning of the European Union. (2008). *OJ 115 , 9.5.2008 p. 94–95. Article 114.* http://data.europa.eu/eli/treaty/tfeu_2008/art_114/oj

Treaty on the Functioning of the European Union. (2016). *OJ 202, 7.6.2016, p. 126. Article 173.* http://data.europa.eu/eli/treaty/tfeu_2016/art_173/oj

Treaty on the Functioning of the European Union. (2016). *OJ 202, 7.6.2016, p. 131. Article 188.* http://data.europa.eu/eli/treaty/tfeu_2016/art_188/oj

Treaty on the Functioning of the European Union. (2016). *OJ 202, 7.6.2016, p. 144. Article 215.* http://data.europa.eu/eli/treaty/tfeu_2016/art_215/oj

Treaty on the Functioning of the European Union. (2012). *OJ C 326, 26.10.2012, p. 173–175. Article 294.* http://data.europa.eu/eli/treaty/tfeu_2012/art_294/oj

Treaty on the Functioning of the European Union. (2016). *OJ C 202, 7.6.2016, p. 176. Article 298 TFEU.* http://data.europa.eu/eli/treaty/tfeu_2016/art_298/oj

Trondal, J. (2014). The rise of a European public administration: European capacity building by stealth. In P. Genschel & M. Jachtenfuchs (Eds.), *Beyond the regulatory polity? The European integration of core state powers* (pp. 166-186). Oxford University Press.

Trubek, D. M., & Trubek, L. G. (2007). New governance & legal regulation: Complementarity, rivalry, and transformation*.* *Columbia Journal of European Law*, *1047*(13), 1-26. https://ssrn.com/abstract=988065

Vos, E. (2014). European agencies and the composite EU executive. In C. Monda, E. Vos, & M. Everson (Eds.), *European agencies in between institutions and member states* (pp. 11-47). Wolters Kluwer Law International.

Vos, E. (2018). *EU agencies on the move: Challenges ahead* (1 ed.) SIEPS. SIEPS No. 2018:1. https://www.sieps.se/globalassets/publikationer/2018/sieps-2018_1-web.pdf, accessed 06.12.2024.

Weiss, M. (2014). Integrating the acquisition of Leviathan's swords? The emerging regulation of defence procurement within the EU. In P. Genschel & M. Jachtenfuchs (Eds.), *Beyond the regulatory polity? The European integration of core state powers* (pp. 27-45). Oxford University Press.

Wonka, A., & Rittberger, B. (2010). Credibility, complexity and uncertainty: Explaining the institutional independence of 29 EU agencies. *West European Politics*, *33*(4), 730-752. https://doi.org/10.1080/01402381003794597

Appendix

Expanded summary of the EU's regulatory approach to cybersecurity

Integration instrument: Regulation	Hard/soft law?	Content summary
Communication from the Commission: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (2001a).	Soft law	Policy initiatives in the context of the broader Information Society and Freedom, Security and Justice objectives: Network and information security and cybercrime. - Legislative proposals for criminal law harmonization. - Indirect capacity-building proposals such as setting-up specialised units at national level, training and cooperation.
Communication from the Commission: Network and Information Security -Proposal for A European Policy Approach (2001b).	Soft law	Proposal of a European policy approach on Member State and EU level: - Awareness raising - European warning and information system - Technology support - Support for market orientated standardization and certification - Legal framework - International co-operation.
Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.	Hard law	Member States shall take the necessary measures to secure network and information security. Illegal access to information systems shall be punishable under criminal law. Member States shall establish a point of contact for the exchange of information on offences related to attacks against information systems.
Communication from the Commission on a Programme for Critical Infrastructure Protection (2006).	Soft law	The communication lays out a plan to identify and reduce vulnerabilities of Member States' critical infrastructure.
Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.	Hard law	The directive establishes a procedure for the identification and designation of European critical infrastructures and a common approach to the assessment of the need to improve the protection of such infrastructures. Member States shall take

		the necessary measures to comply with the directive.
Communication from the Commission: Critical Information Infrastructure Protection. Protecting Europe from Large Scale Cyber-Attacks and Disruptions-Enhancing Preparedness, Security and Resilience (2009).	Soft law	The communication calls for better cooperation and coordination across Europe and sets out an action plan on how to tackle challenges posed by large scale cyber-attacks (including preparedness, prevention, detection, response, mitigation, recovery, international cooperation and implementing criteria for the ICT sector).
Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009.	Hard law	The directive made it mandatory for telecommunications operators to report cyber-incidents to the national regulatory authority.
Joint Communication from the Commission -Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013).	Soft law	Network and information Security: - Achieving cyber resilience by identification of NIS vulnerabilities - Raising awareness on EU and Member State level Cybercrime: - Reducing cybercrime - Commission helps to enhance operational capability to combat cybercrime through funding programs - EU helps Member States to coordinate and collaborate in cybercrime and law enforcement by the help of agencies such as Europol/EC3, CEPOL and Eurojust Cyber defence: - Develop cyber defence capabilities under CSDP Single Market: - The strategy sets out different objectives on how to develop industrial and technological resources for cybersecurity and on how to foster research and development investments and innovation External relations: - The strategy sets out different objectives to “mainstream cyberspace issues into EU external relations and the Common Foreign and Security Policy”

		Coordination between national and EU level: - Strategy calls for optimizing coordination between the national and EU level across the different sub-areas of cybersecurity and the related agencies (on national and EU level). Case of major cyber incident or attack: - EU provides support mechanisms to Member States in case of a major cyber incident or attack “depending on the nature, magnitude and cross-border implications of the incident.”
Directive (EU) 2016/1148 of concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).	Hard law	The Directive lays down measures to achieve a high common level of security of network and information systems within to Union to improve the functioning of the internal market. - Obligation for Member States to adopt a national strategy on NIS. - Creation of a computer security response teams’ network (CSIRTs network), see capacity-building. - Establishment of a security and notification requirements for operators of essential services and for digital service providers. - Obligation for Member States to designate national competent authorities, single point of contacts and CSIRTs with tasks reacted to NIS. - Member States are obliged to identify operators of essential services. - Member States shall adopt a national strategy on the security of network and information systems defining the strategic objectives and policy and regulatory measures to achieve and maintain a high level of NIS. - Member States shall designate a component national authority that shall monitor the application of the Directive. - Member States shall establish a single point of contact with a liaison function for cross-border cooperation and the CSIRT-network.

		- Member States shall designate one or more CSIRTs. - Establishment of a Cooperation Groups (Member State representatives, Commission and ENISA) and the CSIRTs-network. - Member States shall ensure that operators of essential services and digital service providers notify cyber-incidents to the component authorities. - Standardization and voluntary notification are encouraged. - Member States shall lay down rules on penalties applicable to infringements of national provisions based on the Directive.
Joint Communication from the Commission-Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (2017).	Soft law	Strengthening cyber resilience: - Strengthening ENISA. - Proposal of an EU cybersecurity certification framework. - Implementation of the NIS-Directive (2016). - Increase rapid emergency response. - Proposal of a cybersecurity competence network and centre. - Enhancing cyber skills. Creating effective EU Cyber Deterrence: - Identify malicious actors. - Enhance public-private partnerships against cybercrime. - Improve Member States cybercrime investigative capabilities. - Stepping up political response as under the EU diplomatic toolbox. - Building cybersecurity deterrence through Member States' defence capability Strengthening international cooperation on Cybersecurity: - Maintain bilaterial cyber dialogues. - Cybersecurity capacity building in third countries. - Foster EU-NATO cooperation.

Joint Communication to the European Parliament and the Council -The EU's Cybersecurity Strategy for the Digital Decade (2020).	Soft law	The Communication stresses the geopolitical dimension of cybersecurity. The strategy set outs different objectives: - Increase resilient infrastructure and critical services. - Proposal to build a network of Security Operations Centres across the EU. - Explore ways to provide an ultra-secure communication infrastructure. - Making full use of the 5G-Toolbox. - Commission will consider new rules to improve cybersecurity of products and services in the Internal Market. - Contribute to secure Internet connectivity. - Enhance cyber skills and training possibilities. - Proposal of a Joint Cyber Unit. - Tackling cybercrime. - Using the Cyber diplomacy toolbox and exploring options for further restrictive measures (such as sanctions) in cases of cyber-attacks. - Boosting cyber defence capabilities by increasing EU and Member States cooperation under the CSDP and by building on EDA, PESCO and the EDF. - Promotion of EU values in cyberspace on UN-level. - External capacity-building and EU-NATO cooperation. - Proposal for common binding rules on cybersecurity for all EU institutions, bodies and agencies.
Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).	Hard law	The Directive lays down: - obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity and computer security incident response teams.

		- Cybersecurity risk-management measures and reporting obligation for entities identified as critical. - Rules and obligations on cybersecurity information sharing. - Supervisory and enforcement obligations on Member States.
Regulation 2024/2847 of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements - Cyber Resilience Act (2024).	Hard law	The Regulation sets out requirements for products with digital elements with a view to ensure that products are safe before placed on the market. The law introduces EU-wide cybersecurity requirements for the design, development, production and making available on the market.
Commission communication on illegal and harmful content on the internet (1996).	Soft law	The communication presents certain policy options to reduce illegal and harmful content on the Internet: - Cooperation between Member States. - Need for a common European Framework for liability of access providers and host service providers. - Helping the process of self-regulation. - Community action to support the use of filtering systems and rating systems.
Council of Europe Convention on Cybercrime -Budapest Convention (2001).	Hard law	The Budapest Convention is the only binding international agreement on cybercrime. It contains sections on: - Measures to be taken at the national level (regarding criminal law, computer and content related offences and procedural law). - International cooperation (extradition, mutual assistance, transborder access to computer data).
Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.	Hard law	The Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children, child pornography and solicitation of children for sexual purposes. Further, it introduces provisions to strengthen the

		provision of those crimes and the protection of the victims thereof. Member States shall take the necessary measures to implement the directive.
Communication from the Commission: Towards a general policy on the fight against cybercrime (2007).	Soft law	The Communication sets out certain objectives: - Improve and facilitate coordination and cooperation between cybercrime units, other authorities and experts in the EU. - Develop an EU Policy Framework on the fight against cybercrime with Member States and relevant stakeholders. - Awareness raising. - Strengthening operational law enforcement cooperation and EU-level training. - Strengthening dialogue with industry. - Harmonisation of national legislation.
Draft Council conclusions on setting up national alert platforms and a European alert platform for reporting offences noted on the Internet (2008).	Soft law	The Draft Council conclusions invites Member States to set up a national alert platform for the purpose of centralising alerts on offences notes on the internet and invites Europol to establish a European platform which should function as a point of convergence of national platforms.
EU Cyber Defence Policy Framework (2014/2018).	Soft law	The Cyber Defence Policy Framework support the development of cyber defence capabilities of EU Member States. Priorities of the EU Cyber Defence Policy Framework are: - Supporting the development of Member States cyber defence capabilities related to CSDP by the help of the Capability Development Plan. - Enhancing the protection of CSDP communication networks used by EU entities. - Promotion of civil-military cooperation and synergies with wider EU cyber policies, relevant EU

		institutions and agencies as well as with the private sector. - Improve training, education and exercises opportunities.
Joint Communication to the European Parliament and the Council -EU Policy on Cyber Defence (2022).	Soft law	Departing point of the Communication is Russia’s war against Ukraine. It “has been a wake-up call for all questioning the EU’s approach to security and defence, […] including in cyberspace.” The communication proposes a strategy containing: - Strengthening common situational awareness and coordination within defence community. - Enhancing coordination with civilian communities. - Enhancing the cyber resilience of the defence ecosystem. - Ensuring EU cyber defence interoperability and coherence of standards. - Develop cyber defence capabilities (EU supporting the further development of military capabilities e.g. through the EDF). - Enhancing research efforts in key technologies for cyber defence. - Increasing the number of EU cyber defence workforce by the help of new initiatives such as the proposed Cyber Skills Academy. - Strengthening EU-NATO cooperation and cyber-dialogues such as with Ukraine.
Council Conclusions on Cyberdiplomacy (2015).	Soft law	The Council Conclusions on Cyberdiplomacy stress the importance to promote and protect human rights and fundamental freedoms in cyberspace. The Council Conclusions upholds the position that international law is applicable in cyberspace.
Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (2017).	Soft law	The “Cyberdiplomacy Toolbox” contains restrictive measures for a joint EU diplomatic response to malicious cyber activities.

Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.	Hard law	The Council Decision includes economic sanctions as a response to cyber-attacks with a significant effect which constitutes an external threat to the Union or its Member States.
Council Conclusions on the EU Policy on Cyber Defence (2023).	Soft law	The Council Conclusions stresses *inter alia* the role of the EU in cyber defence and sets out different objectives regarding securing the EU defence ecosystem, investing in cyber defence capabilities and cooperation with international partners.

Expanded summary of the EU's capacity-building approach to cybersecurity

Integration instrument: Capacity-building	**Type of capacity-building**	**Aim/target**
European Cybersecurity Competence Centre (ECCC)	Agency	The agency makes strategic investment decisions and pools resources from the EU and its Member States, and indirectly the industry to improve and strengthen technology and industrial cybersecurity capacities. The agency coordinates funding.
National Coordination Centres related to ECCC	Network (coordination with national centers)	The National Coordination Centres function as points of contact at national level to support the Competence Centre in fulfilling its mission and objectives.
Computer-Emergency-Response Team (CERT-EU)	Direct EU capacity-building	An inter-institutional provider that contributes to the security of the ICT infrastructure of EU institutions, bodies and agencies. The team helps to prevent, detect, mitigate and respond to cyberattacks, and by acting as the cybersecurity information exchange and incident response coordination hub.
ENISA -The European Union Agency for Cybersecurity	New agency	The agency primarily supports the built-up of national capacities in cybersecurity. But also engages in direct capacity-building through training, exercises and awareness-raising.
National Liaison Officers Network (ENISA)	Network	The National Liaison Offices Network facilitates the exchange of information between ENISA and the Member States and supports ENISA in disseminating its activities.
NIS-Cooperation group	Network (for Member State coordination)	The group was established for the NIS implementation. It should contribute to achieve a high common level of security for network and information systems in the EU. It facilitates the cooperation and exchange of information among EU Member States.
CSIRT-network	Network	The network is composed of national CSIRTs and CERT-EU. It should contribute the exchange of information, to

	(operational cooperation between Member States)	implement a coordinated response to an incident and to provide assistance to the coordinated disclosure of vulnerabilities.
European Cybersecurity Certification Framework (see Cybersecurity Act)	Indirect EU capacity-building	A European Cybersecurity Certification Framework aims at harmonizing the digital single market for ICT products, services and processes. ENISA is involved in developing cybersecurity certification schemes.
European Cyber Crises Liaison Organization Network (EU-CyCLONe)	Network (cooperation with Member States national authorities)	A cooperation network for Member States national authorities that is in charge of cyber crisis management. ENISA supports the network operationally. It was established under the NIS-Directive.
Europol	Agency	At first the agency was assigned a coordinating role in cybercrime.
European Cybercrime Centre at Europol (EC3)	Agency -task expansion	Europol's tasks in relation to cybercrime were extended by establishment of the European Cybercrime Centre. EC3 provides operational, strategic, analytical and forensic support to Member States' investigations. EC3 supports training and capacity-building for relevant Member State authorities.
Cybercrime Action Taskforce (J-CAT)	Network organization	The taskforce is a permanent operational team (located at Europol/EC3) that works on high-profile cases for cybercrime investigations.
European Judicial Cybercrime Network (Eurojust)	Network (cooperation between judicial authorities)	The network facilitates and enhances cooperation between competent judicial authorities.
Cybercrime Academy (CEPOL)	Direct EU capacity-building	CEPOL hosts a specialized training center for law enforcement officials.
European Defence Agency	Agency -task expansion	The EDA supports the EU Member States in improving their defence capabilities and facilitates collaboration for Ministries of Defence.
Military CERT-Network	Network	The network was established to enhance the level of cooperation in the

		cyber domain at EU level. The military CERTs also participate in Cyber Defence exercises with the EDA.
PESCO projects related to cyberdefence	Direct EU capacity-building	Several Member States participate in different PESCO projects that are related to cyberdefence.
European Defence Fund	Indirect capacity-building	The EDF incentives and supports defence research projects and development such as in the area of cyberdefence (see for example the EUCINF project[7]).

[7] See for details on the project https://defence-industry-space.ec.europa.eu/document/download/abca2b84-bbba-409c-958d-a0767637b76a_en?filename=EUCINF - Factsheet_EDF22.pdf, accessed 06.12.2024, and https://eucinf.eu/, accessed 06.12.2024 and for the funding details https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2022-da-cyber-ciwt, accessed 05.01.2025.

Summary of the theoretical framework and expectations for the analysis

Variation in the EU's regulatory approach	**Hard law & soft law.**
Demand for regulation in cybersecurity	- *Negative policy externalities* (inadequate security standards, incoherent national legal frameworks, a lack of coordination interconnectedness of cyberspace). - Reduction of negative externalities by creating a common European regulatory framework. - EU as a policy coordinator, transfer of competence to the supranational level. - *Exogenous interdependence*: Demand for integration as a reaction to external shocks/events (changes in technology, the increase of cyber-attack and geopolitical tensions). - A response to exogenous interdependence could reflect the EU's digital independence and sovereignty discourse. - *Endogenous interdependence*: Integration within one policy area may lead to the integration of functionally related policy areas (functional spill-over and path dependencies).
Hard law & soft law	- *Hard law* = legally binding acts such as regulations or directives. - *Soft law* = non-binding acts such as communications, recommendations, guidelines, and strategies.
The **supply** conditions for the choice between hard and soft law in cybersecurity. *Actors who "control decisions concerning EU regulation [...] and have an interest in using this control for extending EU regulation."* ⇨ Supranational actors prefer hard law acts while Member States through the Council rather resort to soft law acts.	**Supranational actors [European Commission, the European Court of Justice (ECJ) and the European Parliament (EP)]:** - *Theory: Supranationalism* - These actors favor more integration as it "tends to increase their authority, resources and prestige, and thus serves their institutional self-interest. - These actors always prefer hard law acts over soft law acts as a way to extend EU integration (propose legislation, EU law enforcement, co-legislation). **Intergovernmental level / EU Member States (through the Council):** - *Theory: Liberal Intergovernmentalism* ⇨ States as the critical actors in EU integration that "seek to achieve goals primarily through intergovernmental negotiation and bargaining". - Adoption of hard law acts can reduce transaction costs and strengthen the credibility of commitments and facilitate cooperation within a legal framework. - Legally binding acts assure compliance with rules among actors. - However, legally binding acts incur sovereignty (especially high in areas to national security: Concerns for national security can "act as brake on European integration") and legal costs. - Adoption of soft law instruments as an alternative. - Avoids sovereignty costs, allows Member States to deal with uncertainties in complex issue areas, can facilitate compromise and cooperation, focus on a particular situation instead of accommodating divergent national circumstances and preferences (that arise due to asymmetries of interdependence). - Soft law as a steppingstone towards hard law.

Areas of EU competence as scope conditions for the EU's regulatory approach to cybersecurity *As the EU treaties "do not provide the EU with an explicit cybersecurity competence" cybersecurity sub-issues are linked to existing EU competences.*	The area of EU competence is considered to influence the extent to which actors can control decisions concerning EU regulation and use this control for extending EU regulation: - The EU has for example *exclusive competences* in specific aspects of the internal market and in monetary policies (Article 3 TFEU). - The EU and its Member States can adopt legally binding acts in areas of *shared competences* such as the internal market, energy, freedom, security and justice and research, technological development and space (Article 4 TFEU). - The EU has only *supporting competences* (Article 6 TFEU) for example in the area of industry. - Most decisions in the EU's areas of competences fall under the *ordinary legislative procedure* and legal acts are adopted under qualified majority voting (Article 294 TFEU). - CFSP = *intergovernmental policy area* (defined and implemented by the European Council and by the Council of the European Union). - Most decisions are taken by unanimity (also: CSDP).
Theoretical expectations: **Hard law & soft law** ⇨ *Supranational actors prefer hard law acts* ⇨ *Member States either opt for hard or soft law*	- Commission proposes hard law acts in areas of the Single Market. ⇨ Commission primarily seeks cybersecurity integration by linking cyber-issues to the area of the Single Market. - In areas of shared and supporting competences both hard and soft law can become viable options depending on the Member States' assessment of the costs of hard law and consideration of soft law as an alternative. - Cybersecurity issues can be linked to areas of shared competences such as freedom, security and justice, research or technological development or as well to areas of supporting competences such as industry. - Due to functional demand conditions EU Member States can be willing to agree to hard law acts in these policy areas. - In areas of shared competences, the Member States (through the Council) and the European Parliament can control decisions concerning the extension of EU regulation through the ordinary legislative procedure. - even in certain areas of shared competence (e.g. JHA) intergovernmental cooperation still persists and soft law acts are preferred over hard legal acts. - In intergovernmental policy areas such as the CFSP and CSDP, the adoption of soft law acts is expected due to the Member State's role in these domains and the predominance of sovereignty concerns. - Member States influence and retain control on intergovernmental level. - Member States retain control over decisions concerning the extension or regulation. - In the area of CFSP and CSDP, Member States are assumed to use their control by limiting cooperation to the intergovernmental level and by only adopting non-legally binding decisions. - In the case of cybersecurity, the extent to which cyber-issues can be linked to shared competences can determine the legal choice. - In these areas hard law can become a viable option as sovereignty costs are less pertinent and EU actors control decisions for extending EU regulation. - In intergovernmental areas where sovereignty costs are high, the adoption of soft law is expected.

	- Sovereignty costs are expected to vary across cybersecurity dimensions: • Member States should be less willing to give up sovereignty in areas of cyberdefence as this area immediately affects the core state powers of national Member States. • The functional demand for cooperation in cyberdefence might however induce Member States to adopt soft law acts such as frameworks or strategies. • Member States should be less concerned with integrating network and information security or critical infrastructure protection as the functional demand conditions (for example when considering the cross-border nature of cybersecurity) should outweigh the sovereignty costs. • An agreement to hard law acts can be expected here.

Variation in the EU's capacity-building approach	**Agencies & networks.**
Demand for capacity-building in cybersecurity	- Economies of scale ("when it is cheaper in terms of economic, administrative or political unit costs to consolidate core state powers at the European level rather than exercise them disjointedly at the national level"). - Allows for better coordination and efficiency. - Capacities on EU-level in the case of cybersecurity is reasonable due to its cross-border nature: The consolidation of European capacities to strengthen cyber resilience to react to cyber threats in a coordinative way can be more efficient. - Exogenous interdependence: Exogenous shocks/events such as cyber-attacks shifts in geopolitics make salient vulnerabilities and dependencies of the EU. - A response to such circumstances can be reflective of the EU's digital independence and sovereignty discourse (regain digital autonomy through developing own capacities). - Endogenous interdependencies: The creation of capacities in one policy area may give rise to create further capacities in functionally related policy areas due to interconnectedness of cyberspace. - Demand for capacity-building may also depend on pre-existing capacities on Member State level (duplication is less efficient). - Past decisions to create capacities on the national level can condition capacity-building on EU level.
Supply conditions for capacity-building in the form of agencies and networks in cybersecurity	- Capacity-building relates to the creation of EU resources for exercising core state powers. - These resources are primarily found in agencies. - For supranational actors, namely the Commission and the EP, "the idea of establishing autonomous European agencies was an attractive second-best means through which to expand the EU's regulatory capacity". - EU agencies supply the Commission with relevant organizational capacities. - EU agencies contribute to the centralization of regulatory functions on EU level. - The creation of agencies allows Member States to pursue integration without further supranationalism and a way for Member States to resist any significant expansion of the Commission's power. - For Member States the creation of agencies can also be seen as an attempt to credibly commit to long-term policy objectives and to deal with uncertainties. - Creation of agencies remains a decision of national governments and head of states and therefore the role and tasks of agencies are considered to be more limited -especially in areas related to security. - Member States are expected to only delegate authority to administrative bodies that are subject to direct and indirect control. - Member States limit agencies' autonomy.

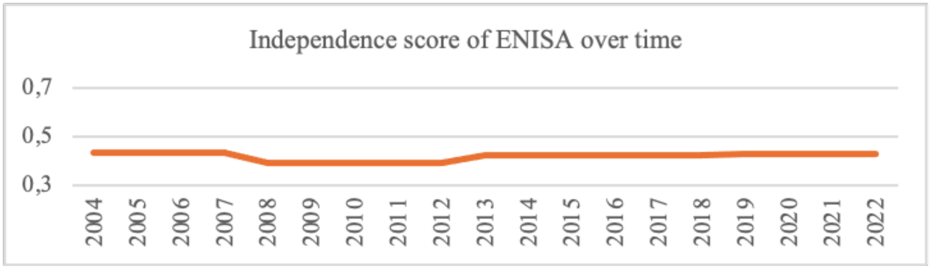
Theorizing agencies and networks.	- Delegation to agencies = principal-agent and competence-control theory. - Granting of authority to the supranational level by indirect governance and delegation. - Principals (European Commission, Council and European Parliament) grant authority to an agent (EU agencies) to fulfil certain tasks (functional motivation). - Principals limit the independence of the agent by installing control mechanisms. - The Commission and the EP favor more independent agencies - Member States want to keep agencies under (intergovernmental) control e.g. through representation of appointees of Member State governments in agencies' management boards. - Capacity-building in form of agencies depends on the actor's willingness to grant competences and independence to them. - EU actors have to balance competence and control. - The actual design of agencies is politically motivated and "the result of political compromise involving EU law-makers in the Council of Ministers, the European Parliament, and the European Commission." - Further decision: Create a new agency or expand the tasks of (existing) agencies. - Layering as gradual institutional change through amendments, additions, or revisions to an existing set of institutions. - EU actors can decide whether to work within existing institutions and to gradually change these or to create new ones. - Creation of networks (alongside agencies) = as a form of informal governance. - Networks as an intermediary between domestic agencies, national actors, EU agencies and the EU-level. - Networks as a form of orchestration: (Re)establish control or enhance competence. - Indication towards the combination of delegation and orchestration. - Networks can enhance operational capacities (experts and equipment for preventing, discouraging, deterring and responding to malicious cyber activities). - Networks can enhance implementing capacities on the national level in order to assure the application of EU regulation. - Networks can also be considered an effort to harmonize the fragmented institutional landscape through agencies. - Networks can also be seen an alternative choice to the delegation to agencies when political commitment is weak, and resources are limited. - Control can be enhanced by adding an agency to an established network.

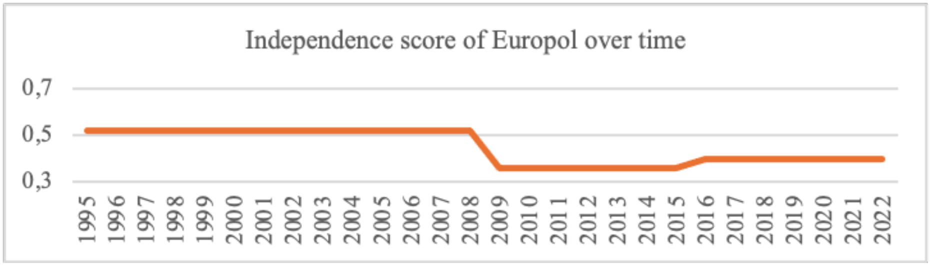
Areas of EU competence as scope conditions for the EU's capacity-building approach to cybersecurity	- New agencies are created in areas where the Commission enjoys considerable competences such as related to the Single Market (hereby the Commission will link cyber-issues to the Single Market). - In this area, Member States through the Council can agree to establish an agency but they make sure to keep control over such bodies through e.g. Member State representation in the agencies' board. - It must be noted that in certain areas of shared competence, despite the communitarization of certain policy areas (such as JHA), intergovernmental decision-making arrangements and cooperation still persist.
Theoretical expectations: Agencies & networks	- In intergovernmental areas that directly affect core state powers and incur sovereignty costs, it can be expected that Member States rather agree on expanding the tasks of an existing agency to deal with certain cyber-issues given functional demands for capacity building. - In intergovernmental areas (defence or diplomacy): Here Member States retain control over capacity-building decisions in these policy domains, extensive delegation to agencies is unlikely as Member States are reluctant to give up sovereignty. - Networks as a more informal mode of governance, can help to enhance operational and implementation capacities and coherence between policy fields. - In areas where cyber-issues are linked to shared competences networks can be expected to be added along existing agencies to enhance operational and implementation capacities. - For Member States looser network structures can function as an alternative to (further) delegation in intergovernmental policy areas to facilitate operational cooperation in cyber specific domains.

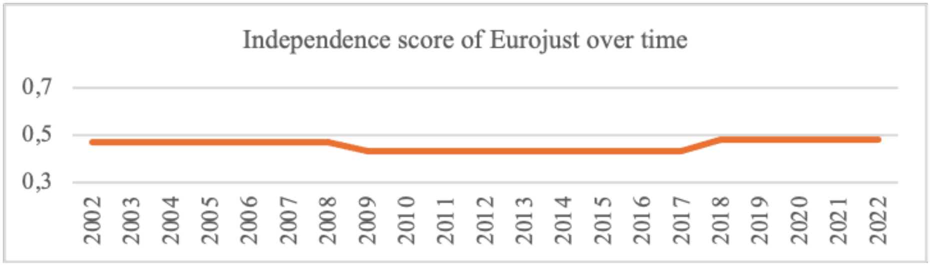
Variation in capacity-building	**Direct and indirect forms of capacity-building**
Theoretical expectations: **Direct & indirect forms of capacity-building**	- *Direct capacity-building* = at EU-level when the building of capacities empowers the EU to either directly respond to cyber-issues or by creating resources on EU-level in the long-term (direct capacity-building approaches can contribute to improving operational activities to prevent or deter cyberattacks, by providing training and skills to EU officials in cyber-related fields or by funding EU-level projects on cybersecurity). - *Indirect capacity-building* = supporting the built-up of national capacities. - Regulation thus often aims at building capacities on national level that indirectly contribute to the overall capacities of the EU. - Indirect capacity-building approaches (through regulation, i.e. hard or soft rules) can include the setting-up of information points and liaison offices on national-level or incentives for investment in cyber technologies. - Supranational actors: prefer direct capacity-building over indirect capacity-building as it extends EU-level resources. - Commission will resort to indirect capacity-building proposals by incentivizing the built-up of capacities for "the exercise of national core state powers" (especially in areas of intergovernmental competence). - Member States are expected to be more willing to support initiatives aiming at enhancing national capacities –rather than pooling resources on EU-level. - Indirect capacity-building approaches are also expected in cases where cyber issues are linked to shared competences as the EU has to rely on the capacities of Member States in security matters.

Data on the level of independence of selected of EU agencies

Independence score[8] of selected EU agencies that deal with (sub-areas of) cybersecurity over time.

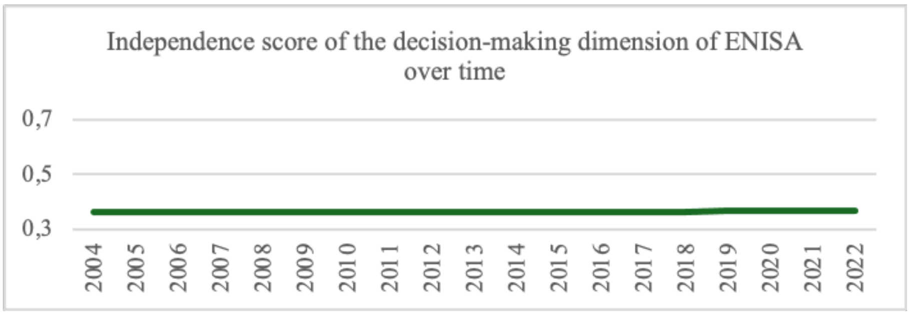


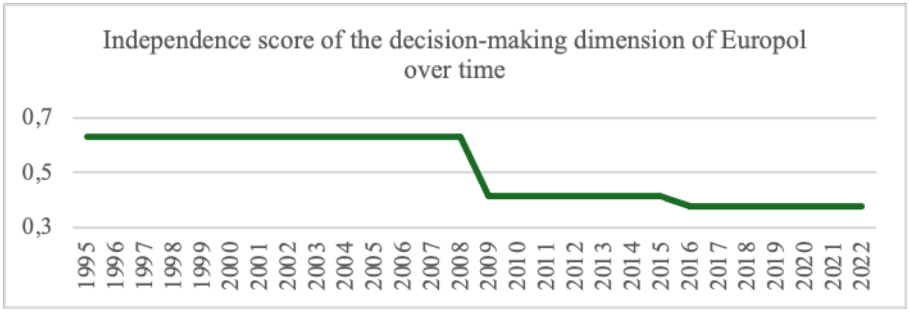


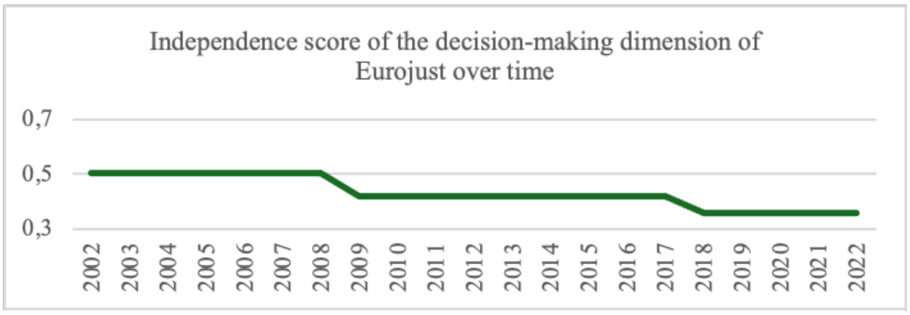


[8] Independence score of the agency (mean of c1-c5). For further information on the different scores please consult Ruffing et al. (2023) and the appendix of the study. The data were provided by Martin Weinrich. Based on the data, I assembled the different graphs for the selected agencies (ENISA, Europol, and Eurojust). The data of the study are available from the authors on request (contact: martin.weinrich@uni-osnabrueck.de).

Independence score of the decision-making[9] dimension of selected EU agencies that deal with (sub-areas of) cybersecurity over time.

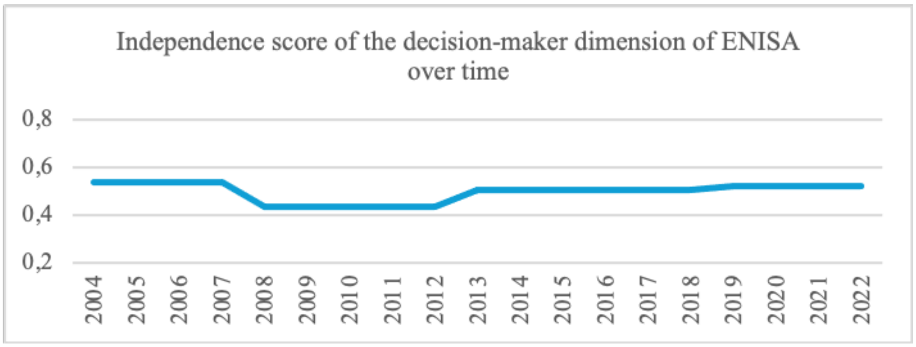


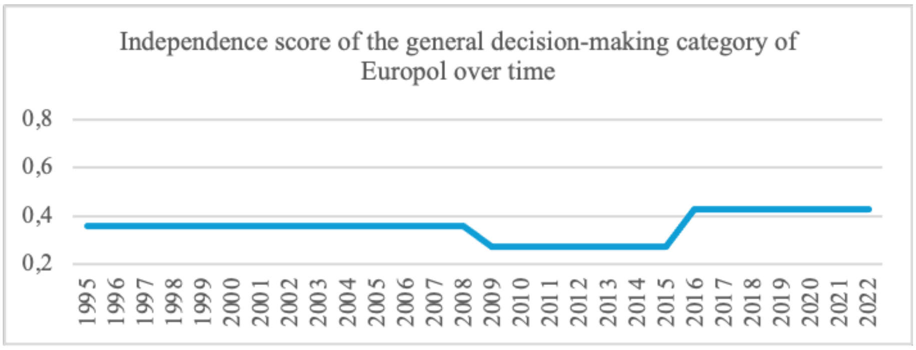


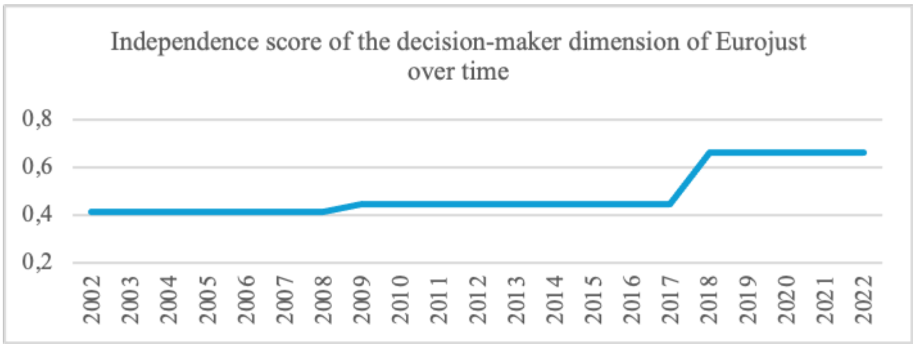


[9] Independence score of the decision-making dimension (mean of c1, c2 and c3).

Independence score of the decision-maker[10] dimension of selected EU agencies that deal with (sub-areas of) cybersecurity over time.

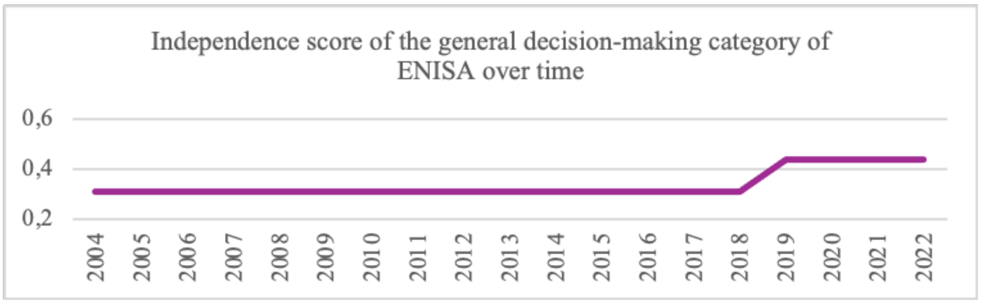


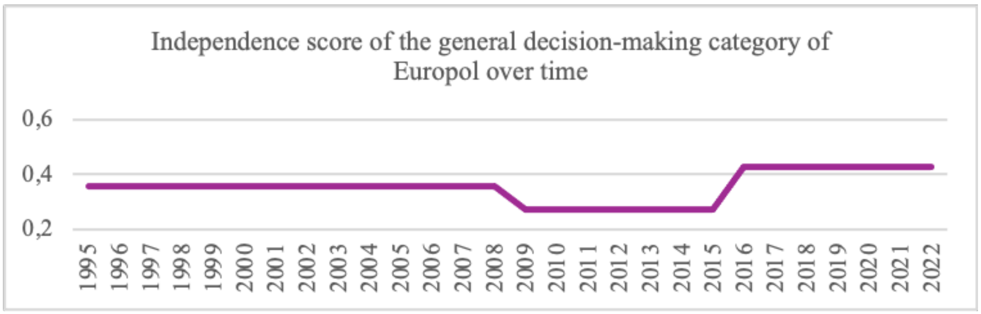


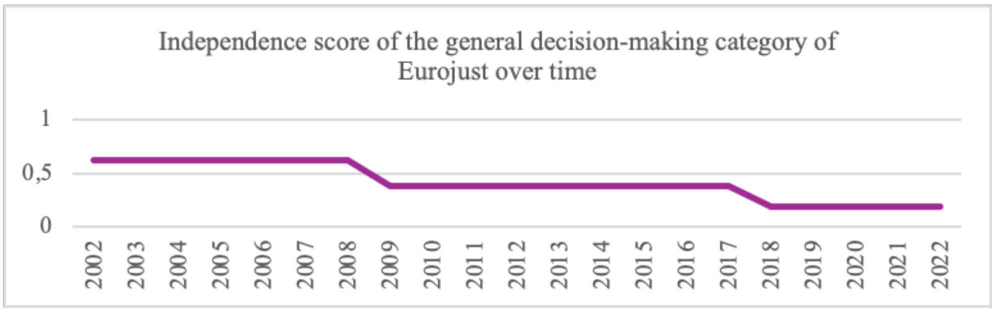


[10] Independence score of the decision-maker dimension (mean of c4 and c5).

Independence score of the general decision-making[11] category of selected EU agencies that deal with (sub-areas of) cybersecurity over time.

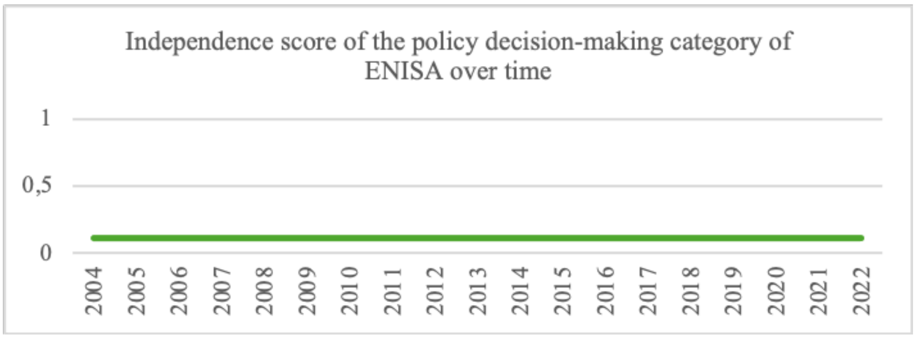


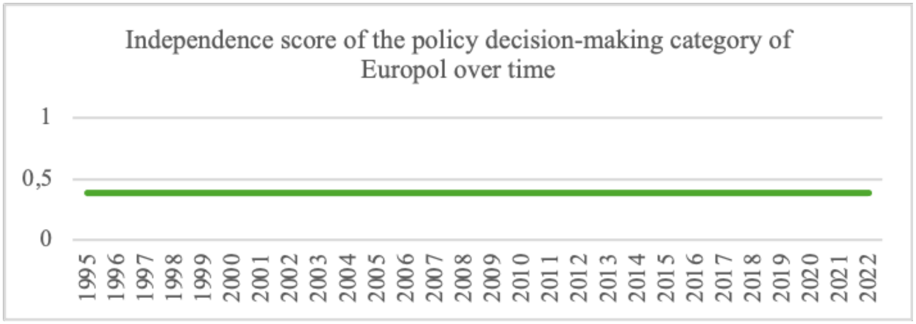


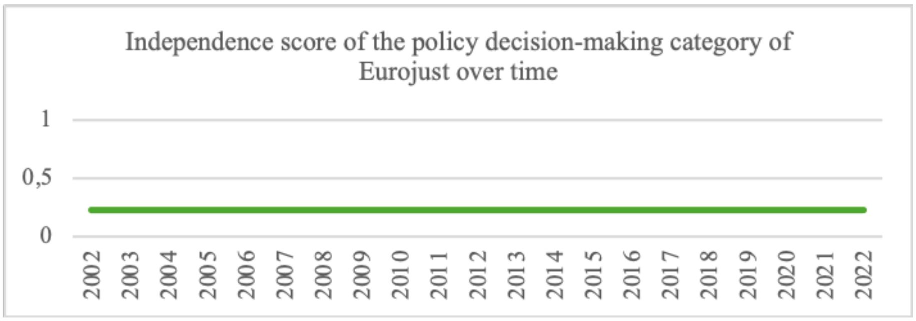


[11] Independence score of the general decision-making category (mean of V1-V4).

Independence score of the policy decision-making[12] category of selected EU agencies that deal with (sub-areas of) cybersecurity over time.

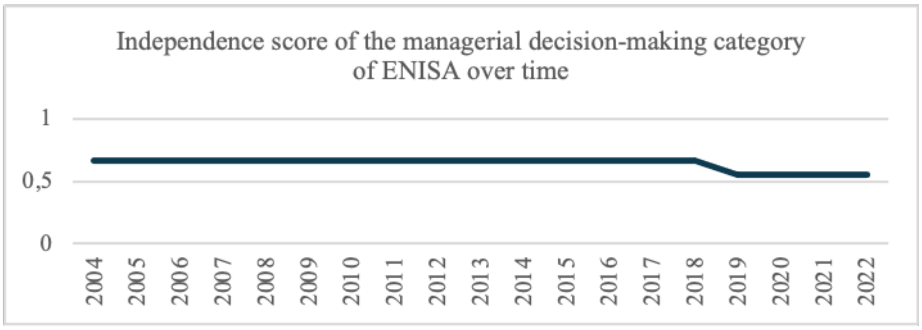


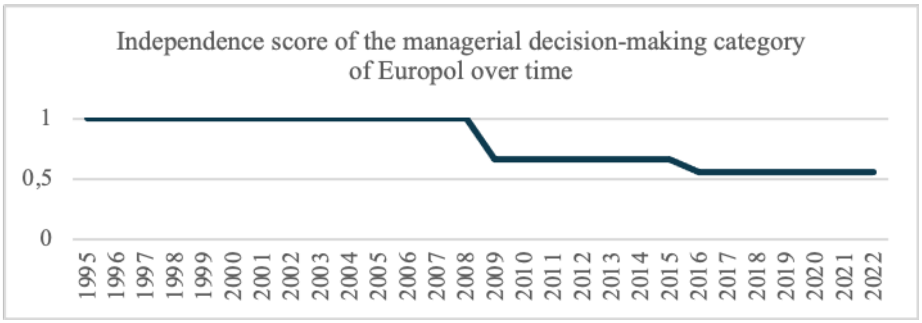


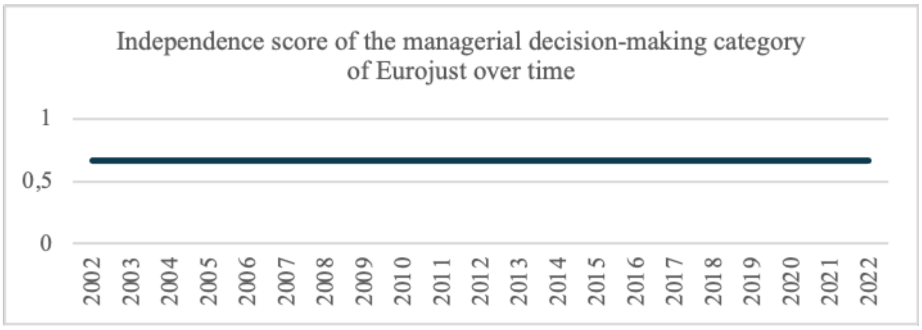


[12] Independence score of the policy decision-making category (mean of V5-V7).

Independence score of the managerial decision-making[13] category of selected EU agencies that deal with (sub-areas of) cybersecurity over time.

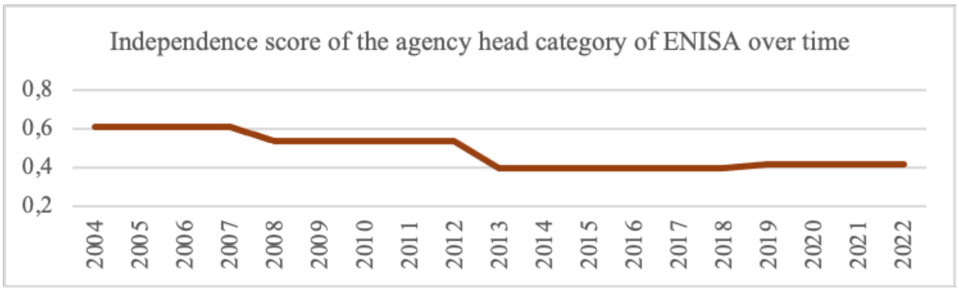


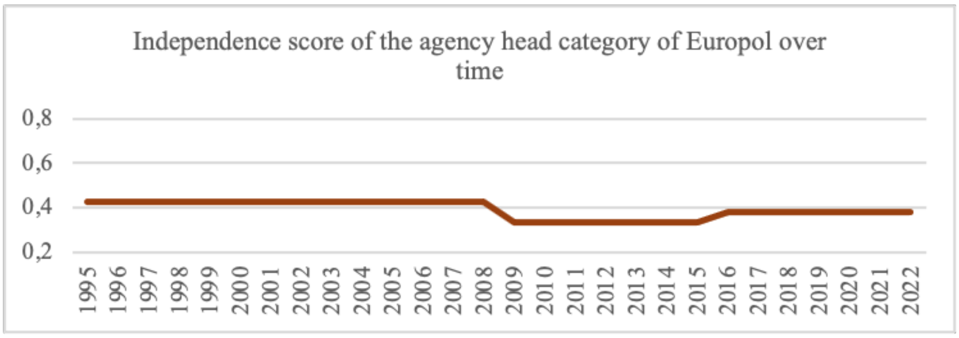


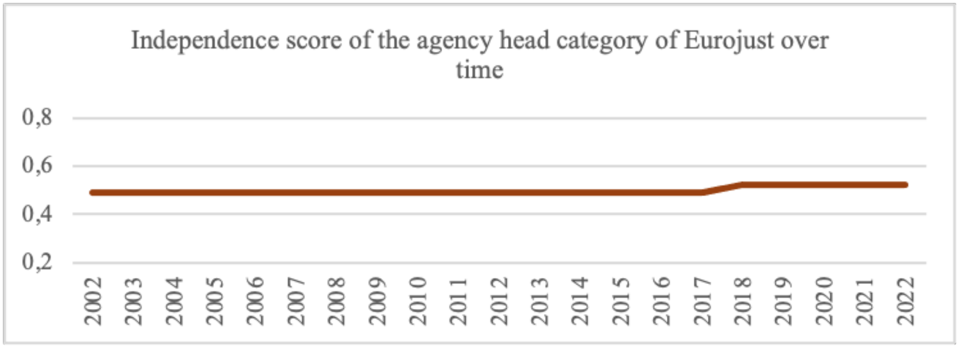


[13] Independence score of the managerial decision-making category (mean of V8-V10).

Independence score of the agency head[14] category of selected EU agencies that deal with (sub-areas of) cybersecurity over time.

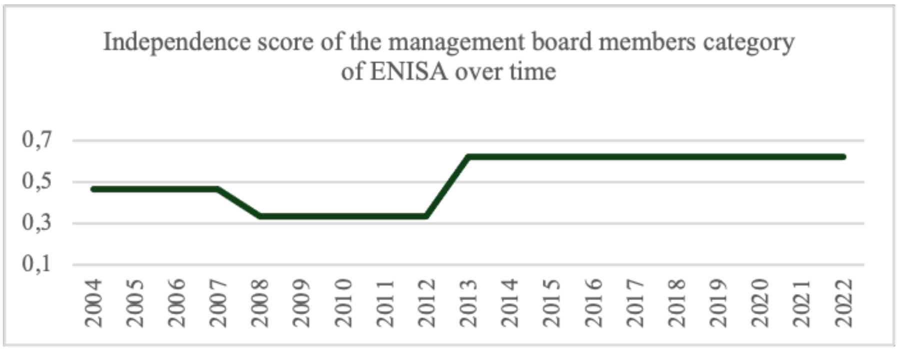


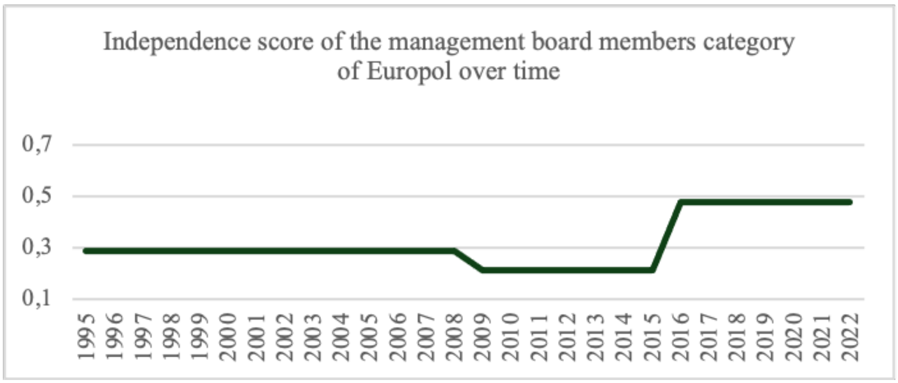


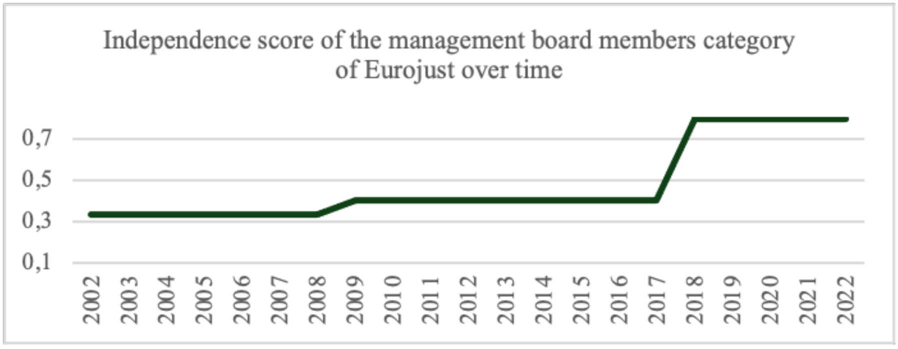


[14] Independence score of the agency head category (mean of V11-V17).

Independence score of the management board members[15] category of selected EU agencies that deal with (sub-areas of) cybersecurity over time.







[15] Independence score of the management board members category (mean of V18-V24).