Ivanova, Maria:

Explaining European Integration in Cybersecurity. The Multidimensional Influences on European Integration in the Field of Cybersecurity.

Bachelorarbeit, Sommersemester 2021

Sozialwissenschaftliche Fakultät

Ludwig-Maximilians-Universität München

https://doi.org/10.5282/ubm/epub.77240

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

GESCHWISTER-SCHOLL-INSTITUT
FÜR POLITIKWISSENSCHAFT

Münchener Beiträge
zur Politikwissenschaft

herausgegeben vom
Geschwister-Scholl-Institut
für Politikwissenschaft

2021

Maria Ivanova

Explaining European Integration in Cybersecurity. – The Multidimensional Influences on European Integration in the Field of Cybersecurity.

Bachelorarbeit bei
Prof. Dr. Berthold Rittberger
2021

Table of Contents

Abbreviations

DdoS attacks	distributed denial-of-service attacks
EC	European Commission
ENISA	European Network and Information Security Agency
EU	European Union
GDPR	General Data Protection Regulation
LI	Liberal Intergovernmentalism
NIS	Network and Information Security
TEU	Treaty on the European Union

Explaining European Integration in Cybersecurity. The Multidimensional Influences on European Integration in the Field of Cybersecurity.

1 Introduction

Over the last decades, the European Union (EU) has significantly expanded functionally, geographically and institutionally. One of the newest fields of functional expansion is cybersecurity whereby significant progress has been achieved in a short period of time. Cybersecurity is nowadays part of the efforts pursued within the scope of the Digital Single Market Strategy of the EU and as a part of the Single Market, Innovation and Digital expenditure area of the EU budget is allocated the third-largest budget share after agriculture and cohesion (European Commission n.d.). The importance of the digital transformation in the EU is furthermore, reflected in the 2019-2024 Commission priority "A Europe fit for the digital age" (European Union 2021). This prioritization of cybersecurity at Union level is not surprising if the connectedness on the Internet within the EU is considered. The latest data shows that 89 % of European citizens use the Internet, which puts the EU second after North America (InternetWorldStats 2021). Taking into account the connectedness to the Internet of enterprises the numbers are just as high. According to Eurostat data, 90 % of enterprises rely on Internet access for their work and 77 % of all enterprises have websites, while 50 % use social media according to 2019 Eurostat data (Eurostat 2019a). Even though private users in the EU are careful with the data they are providing online (Eurostat 2019b) and 99 % of the enterprises have existing cybersecurity measures in place (Eurostat 2019a), the number of cyberattacks is constantly growing, as well as the costs of cybercrime, which are expected to reach 6 trillion worldwide by the end of 2021 (Morgan 2020).

The presented data shows that efforts from the European Union in the field of cybersecurity are necessary if the European Union wants to establish itself as a leader in this field, as outlined in the Commission priorities for 2019-2024 (European Commission 2019). However, a lot of states only began developing their cybersecurity policies at national level after the initiatives at European Union level. Therefore, this paper raises the question of why did the European Union pursue integration in the field of cybersecurity before the existence of such policies at national level.

As cybersecurity was emerging as a new policy field subject to European regulation, one of the main challenges for the European Commission (EC) was the definition of this new area of

European policymaking and its scope. Given that national cybersecurity strategies and the definitions used in them are very different, the decision on an EU-wide definition made the Commission's endeavor more challenging (Brandão and Camisão 2021). Up to the present day, there is not an established EU-wide definition of cybersecurity, whereby different definitions are used depending on the context of different initiatives at EU level (Fuster and Jasmontaite 2020). For the purposes of this paper cybersecurity in the EU will be understood as defined in the Cybersecurity Strategy of 2013. "Cyber-security 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. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein" (European Commission 2013a). This definition implies a wide scope of the policy area of cybersecurity which in turn enables EU initiatives in a variety of fields.

The field of cybersecurity has been a subject of International Relations scholars for the last decades and has been explored through the lenses of classical International Relations theories like liberalism and realism. Some scholars see cyberspace as a borderless space that relies on international cooperation for its preservation, whereas the more realist theorists argue that it is dominated by the same power structures as the real world (see Manjikan 2010). While there are differing views on how cyberspace can be perceived in the context of international relations, there is a broad agreement that cyberspace enables access to online territory to a variety of actors such as states, companies, individuals and others (see Lambach 2016; Kasper 2020). Cyberattacks have consequences for all of these actors – from individual freedom and privacy abuses to implications for political power and financial stability. When it comes to governance of cyberspace it stands out that states lack the expertise, capacities and resources to govern this new domain (Farrand and Carrapico 2018), which on the other hand is closely related to their economies. Moreover, private companies make up a large part of territory owners in the online domain and their involvement ranges from providing Internet and online access (Farrand and Carrapico 2018) to securing cyberspace through their services. This imbalance of states´ capacities compared to the capabilities of the private sector leads to the creation of public-private partnerships for the shared governance of the field in a lot of countries, which is also the case for the European Union (Farrand and Carrapico 2018; Carr 2016).

As previously outlined cybersecurity incidents can have enormous costs for economies and the interdependence of countries due to the economic integration within the European Union makes cybersecurity in the scope of the Union an economical issue, which is also the preferred framing chosen by the European Commission in the presentation of a variety of its initiatives (Brandão and Camisão 2021; Wessel 2015). The abolition of the pillar system in the EU, introduced with the Lisbon Treaty gave EU institutions more flexibility when it comes to legal bases of legislation, whereby network and information security (NIS) Directive is considered a matter related to the Internal Market and the General Data Protection Regulation (GDPR) is based on the protection of individuals and their rights (Wessel 2015). The economic framing as a way for the European Commission and transnational private actors to shape this new policy field gives reasons to believe that supranationalism would be a suitable explanatory theory of the developments in cybersecurity. This framing of cybersecurity matters on European level challenges the understanding of cybersecurity as a simply security-related area, although some scholars see the field of cybersecurity as a field dominated by states within the context of the European Union (see Kasper and Vernygora 2020; Christou 2019; Sliwinski 2014) and argue that the intergovernmental character of the field is the biggest hindrance in the way of more European integration in the field of cybersecurity (Sliwinski 2014). Article 4 of the Treaty on European Union (TEU) explicitly establishes that national security is a competence of the member states (TEU 2012). As it is related to national sovereignty it can, according to realist intergovernmentalism, be considered a field of high politics, which means that the states are unlikely to delegate authority to the European level in this field (Hoffmann 1982; Leuffen et al. 2022). Furthermore, states have made use of this fact and continue to have very different national approaches to cybersecurity (Štitilis et al.). Yet, over the last decades cybersecurity is a policy area that has increasingly become the focus of European level regulation with legislative Acts like the Network and Information Security Directive (NIS Directive) and its dedicated agency – the European Network and Information Security Agency (ENISA), which challenges intergovermentalist assumptions.

Supranationalist and intergovernmental approaches to European integration have long been the two major and competing schools of European integration. From the founding of the EU and the initial expansion of the functional and geographical scope of the Union through the major changes brought by the Maastricht Treaty and the diverging outcomes of the crises in the last two decades, the two theories have sought to provide the more convincing arguments than the other (Leuffen et al. 2022). In the meantime, the EU has become a lot more complex and significantly expanded its competencies, whereby there are barely any fields that are not governed in some capacity at European level as well (Bickerton et al. 2015; Schimmelfennig and Rittberger 2015).

When observing developments in the EU, questions related to the applicability of traditional European integration theories to the policy area of cybersecurity arise, as the interdependence, the role of transnational actors and sovereignty sentiments make the processes since the 1990s hard to explain with just one European integration theory. Therefore, this paper aims to tackle the relevance of explanations often seen as contradictory and through outcome explaining process tracing and a chronological analysis of the processes in cybersecurity at Union level delivers a comprehensive explanation of European integration in the field. By using the theories of supranationalism and intergovernmentalism the biggest milestones in EU cybersecurity are analyzed in order to see what are the driving forces of integration in this field.

First, the key theoretical assumptions of supranationalism and intergovernmentalism are outlined and presented as part of the theoretical framework applied to explain integration in the field of cybersecurity. The next section outlines the research design, method and data used for the paper, which is followed by the application of the framework on the case of cybersecurity in the European Union. The results show the involvement of a variety of actors shaping integration processes in cybersecurity at EU level. Moreover, EU cybersecurity is marked by the initiatives of supranational actors and path dependence, while in regard to big milestones with an impact on national policies the states exercise a restrictive role to supranational ambitions. In the final part of this text, the limitations of this paper and the potential for future research in the field are discussed.

2 Theory

2.1 Supranationalism

Supranationalism emerged as a theory with the rise of the European Union in the 1950s and was largely formed by the neofunctionalist work of Ernst Haas, especially through his book “The Uniting of Europe” (1958). The theory has its roots in International Relations and is developed from the opposition against the dominating realist beliefs in the anarchical structure of the international system shaped by distrust and power struggles. Neofunctionalists instead argued that institutionalization has the potential to establish a system based on rules (Leuffen et al. 2022).

In his book, Haas (1958) introduces a new understanding of international relations and cooperation, as well as the central to neofunctionalism concept of spillover. The "The Uniting of Europe" emphasizes this new to International Relations theories integration, whereby states voluntarily agree to delegate power to a centralized authority, and provides an analysis on the reasons for this integration. Pluralism and interdependence are described as favorable conditions for the formation of the European Coal and Steel Community (ECSC). Haas highlights that an entity of international cooperation will only make changes in its level of integration if the said entity through its actions provides strong incentives for more or less centralized action. Different actors involved in policymaking such as parties, transnational groups and governments are presented as rational in the sense that they follow their self-interest and pursue personal gains within the system of integration by turning to the federal authority in case of potential benefit. Stakeholders that see self-interest in working with the centralized authority, in turn, contribute to the need for more centralized action and through this contribute to deeper integration. Because of the centralized authority, domestic stakeholders have incentives to communicate across nations, cooperate and directly communicate to supranational authorities. These processes are not driven by the European citizens but by small elite groups that pursue their goals by using supranational means (Haas 1958).

Another central finding from the analysis of Ernst Haas is the spillover effect which brought economic integration in the 1950s for the ECSC. The argument is that by delegating authority to a supranational entity in a specific field it becomes necessary to pursue further integration in other policy areas to avoid unwanted costs and instead maximize the gains for different stakeholders involved. Even more skeptical actors would make adjustments which in turn supports the integrative processes. The fast progress in integration from ECSC to pursuing more economical integration through the removal of tariffs, barriers to free movement, currency restriction, etc., and the establishment of the European Economic Community confirm the role of the spillover effects in the process (Haas 1958, 283-317).

Even though "The Uniting of Europe" was released in times when cooperation in Europe was solely economic and within the scope of just 6 member states of the European Coal and Steel Community, it demonstrates arguments on European integration, which transcended the ECSC and are still relevant for European integration research in the present day of a much more integrated European cooperation. Building upon the work of Haas (1958) Pierson (1996), Stone Sweet and

Sandholz (1997) develop further assumptions shaping supranationalist train of thought, most of which Haas approves of in his 2004 introduction to “The Uniting of Europe”.

Pierson (1996) introduces the concept of path dependence in European integration and claims that even though member states do have a big role in shaping integration they often find themselves in a constrained position, whereby the reasons for this are institutional. On the one hand, member states make the conscious choice for the establishment of European institutions. However, because these institutions take on a variety of tasks like coordination, mediation and monitoring, which gives them access to resources, the institutions tend to develop their interests and pursue them, while also aiming to increase their autonomy. Another reason for the gaps occurring in state control is the limited time scope of the mandates of politicians and the implications of their decisions, as politicians tend to focus on short-term effects of their decisions which matter more for their electoral success. This makes long-term effects less important to be considered by politicians in the context of electoral democracies. Furthermore, the wide functional scope and intensity of European decision-making give an advantage to supranational actors which possess expertise and resources and as already mentioned follow their own agenda. The change in governments and their preferences is one more reason for institutional outcomes that diverge from the initial intentions. The burdens of reversing or significantly changing existing European policies and institutions are big, while the reversal of policies or exit from arrangements are unattractive because of the already achieved adaptation to them across the system (Pierson 1996).

A further prominent contribution to supranationalism has been made by Stone Sweet and Sandholtz (1997), who place the emphasis on supranational institutions. One of the major points raised in their revision of Haas’ neofunctionalism is that European integration should not be explored as a process that inevitably leads to the formation of a federal state. The two supranationalist scholars base their theory on the causal relationship between three factors – transnational exchange, supranational organization and rule-making. The first stage which gives rise to integration is intensified transnational interactions which based on the rational self-interest of these actors produce demands for supranational governance. In response to these demands, supranational organizations react, while also using these interests to secure more autonomy and power for themselves. As a result of the response of supranational organizations, they produce rules, which as the last component of the causal mechanism of the theory shape and restrict the behavior of actors involved in European policy-making. In this process transnational groups emerge and grow, having new demands for supranational regulation, which ties in with the concept of functional spillover proposed by Haas (Stone Sweet and Sandholtz 1997). In a further study of gender equality and free movement of goods policies, Stone Sweet and Brunell (1998) show evidence for the proposed causal mechanism and specifically for the increase of responsiveness of the European Community to demands from transnational actors, as the legal structures of the Community enabled direct contact of transnational actors with supranational authorities.

2.2 Intergovernmentalism

This section of the paper presents the key assumptions of the second major school of thought in the field of European integration selected for the purposes of this paper. Intergovernmentalist theorists, who see states as the driving forces of European integration, claim that their theory dismantles the assumptions of supranationalism, whereby Stanley Hoffman and Andrew Moravcsik are some of the most prominent scholars who shaped intergovernmentalism.

Stanley Hoffman (1966) argues that member states have not lost their control over international integration and are the main actors that decide the appropriate level of international cooperation. Furthermore, the author points out that national member state differences become apparent as soon as integration is more than just economic and matters of "high politics" are at stake. The creation of the European Community followed the Second World War and the cooperation through this supranational institution strengthens the nation-state and is used by the states to achieve their goals (Hoffmann 1966). Areas of high politics are the ones that have a direct relation to national sovereignty and autonomy and can be considered areas that are more likely to be politicized. This sovereignty-focused theory of intergovernmentalism can also be referred to as realist intergovernmentalism (Schimmelfennig and Rittberger 2015).

Building upon the core assumption of the early works on intergovernmentalism – member states are in control of integratory processes in the European Union, Andrew Moravcsik (1998) developed his theoretical framework with a more liberal take on integration by taking into account processes of preference formation on the national level, which are then represented by state officials at the international level in the EU. He further clarified the main assumptions about politics that liberal intergovernmentalism (LI) is based on. First of all, LI sees states as the main actors in international relations under the conditions of anarchy, whereby they pursue their goals through international negotiations. Secondly, the theory is based on the idea that states are rational actors and base their decisions on calculations of potential utility. These two assumptions are the basis for the three-stage framework proposed by Andrew Moravcsik (Moravcsik and Schimmelfennig 2009).

The theory acknowledges the condition of interdependence as central for European integration. Moravcsik presents a three-stage framework consisting of preference formation, international bargaining and institutionalization of the international agreements. Firstly, preferences in liberal intergovernmentalism are considered exogenous to intergovernmental bargaining and as a product of domestic competition between groups, whereby the dominating groups are represented by governments in intergovernmental bargaining (Moravcsik and Schimmelfennig 2009; Moravcsik 1998). The preferences that drive integration in the European Union are predominantly economic interests and they are seen as evolving in response to developments in the global economy over time (Moravcsik 1998, 3), which explains the differences in preferences constellations at different points in history. The other type of national preferences outlined in the "The Choice for Europe" (1998) are geopolitical, which are also seen as related to economic preferences, as the common threats can have economic implications for multiple states and in turn shared action against such threats will strengthen the national state and bring economic benefits. The definition of these two types of preferences that shape European integration complements the understanding of LI that state preferences can vary across states and issues (Moravcsik 1998).

Intergovernmental bargaining is the second stage of integration processes and focuses on interdependence and the distribution of benefits. In terms of information asymmetries, LI assumes that state representatives act under complete information, as all necessary information is exchanged between officials in negotiations. Furthermore, governments are considered to be efficient policy entrepreneurs and do not have to rely on supranational organizations to secure outcomes (Moravcsik 1998, 66). The course of intergovernmental bargaining reflects differences in preference constellations, information and asymmetries in interdependence, which form the bargaining power of states. The states closest to the status quo possess the highest bargaining power (Moravcsik and Schimmelfennig 2009).

The final stage of the process of integration as shaped by states according to Andrew Moravcsik is the choice of institutions. The assumption is that based on the outcomes of negotiations member states choose the appropriate institution to secure the results, which is seen as an informed choice by the member states and as a way to ensure cooperation and prevent cooperation problems through control and reduction of transaction costs. Institutions are seen as tools that states use to their advantage in order to achieve their goals (Moravcsik and Schimmelfennig 2009; Moravcsik 1998, 9).

2.3 Choice of Theories

In the field of European integration scholarship, three theories are the main shapers of the scientific discourse – supranationalism, intergovernmentalism and the more recently prominence gaining postfunctionalism. For the purposes of this paper supranationalism mostly based on the groundwork of Ernst Haas (1958) and liberal intergovernmentalism of Andrew Moravcsik are chosen as the basis for the theoretical framework explaining European integration in the field of cybersecurity. This section provides an explanation for the choice of these theories over the postfunctionalist explanations in the context of cybersecurity in the European Union.

Despite all the major differences in the core assumptions of intergovernmentalists and supranationalist, there are some similarities which create the basis for the application of the theories on the same case. Both supranationalism and intergovernmentalism stem from International Relations theories, whereby supranationalism is mostly inspired by historical institutionalism and intergovernmentalism by rational institutionalism (Schimmelfennig et al. 2015). Furthermore, both theories are based on the assumption that actors which are involved with European integration are rational in their actions. In the context of both theories, interdependence is an important factor for the development of international cooperation (Schimmelfennig et al. 2015). Both theoretical approaches recognize the importance of the same core actors in the process of integration: states, transnational actors and supranational institutions. However, they have differing opinions on which of these stakeholders are dominating the processes of European integration (Hooghe and Marks 2009). Moreover, both schools of European integration theories see European integration as elite-driven and not subjected to the opinion of the masses (Peterson 2001).

Tsebelis and Garett (2001) connect assumptions of the two approaches by putting institutions in the focus of their analysis and argue that states make decisions in their choice of institutions, taking into account the potential consequences of the institutional choice. Therefore, it is reasonable look at institutions both as dependent and independent variable, which will be the approach taken in this paper. Even though the two theories can be considered competing, some scholars argue that they do not necessarily aim to explain the same types of phenomena in European integration, whereby intergovernmentalism focuses on major political changes like the Treaties and supranationalists shed a light on daily political decisions (Peterson 2001, Stone Sweet and Sandholz 1997). However, the crises of the last decades have pushed European integration theorists and many representatives of the two theory families have skillfully applied the old theories to the newest developments in European integration (see Schimmelfennig 2018, Biermann et al. 2019). Furthermore, Peterson (2001) argues that supranationalist theorists and intergovernmentalists have complementary and not opposing claims. Stone Sweet and Sandholz (1997) for example see intergovernmental bargaining as part of the integrative processes driven by increased transnational interactions, Moravcsik (1998) acknowledges the role of supranational organizations, which in some cases have proposed initiatives accepted by governments as the Single European Act.

In the case of postfunctionalism, the gaps between ontological assumptions are wider which makes the theory irrelevant for this research paper on cybersecurity. Firstly, the theory is derived from sociology and more specifically constructivism, whereby constructivism as a theory implies a different understanding of structures such as institutions which are seen as a reflection of norms, identities and values. This is in contrast to the view of institutions as tools in the integration processes, which supranationalists and intergovernmentalists base their assumptions on. Secondly, because of the emphasis on social interactions and structures in the formation of preferences, constructivism sees preferences as endogenous and subject to adaptation and change during negotiations. Lastly, constructivist theories explore actors outside the elite and take into account individuals in the sense of public officials and citizens as potential drivers of integration through their identities (Schimmelfennig and Rittberger 2015). Postfunctionalism claims to reflect the new developments in European integration as European Union politics increasingly have implications for citizens as well, unlike the early years of solely economic integration (Hooghe and Marks 2009). Hooghe and Marks (2009) argue that politicization of European integration among the mass population has changed European politics and given rise to identity politics, whereby public opinion is increasingly influencing the course of integration. This happens through the structures of party competition and the decision of parties on how to frame specific issues based on the potential gains and costs for them.

In the context of cybersecurity in the European Union, however, the theory of Hooghe and Marks (2009) is harder to apply. Kasper and Vernygora (2020, 199) claim that the field of cybersecurity is too broad and related to a variety of policy fields to be politicized by parties, which also traditionally do not have a stance on European cybersecurity on their party programs yet. Furthermore, the authors reveal that cybersecurity is less present in citizens' lives, which in turn makes mobilization on this issue less likely. This claim is supported by Eurobarometer data on cybersecurity and GDPR, both revealing a relatively low level of informedness of citizens when it comes to their rights online (see Special Eurobarometer 2019; Special Eurobarometer 2020). The issue is mostly shaped at European level by the elites, whereby for a long period of time a big part of the European Union member states did not even have a national cybersecurity strategy (see European Parliament 2013; Brandão and Camisão 2021), which shows that the policy field of cybersecurity is not very present in Europeans' lives.

Based on the presented arguments above, supranationalism and intergovernmentalism will be used as a basis for the explanation of cybersecurity integration and postfunctionalism is ruled out as a theory, which can appropriately explain the course of European integration in the field of cybersecurity.

3 Research Design, Method and Data

This paper can be defined as a y-centric theory-based explanation, whereby theories of European integration are applied to the case of cybersecurity. Scholars working with European integration theories often adopt process tracing as a method for their research as it enables an in-depth analysis of phenomenons (see Stone Sweet and Sandholtz 1997, 313; Schimmelfennig 2001). In order to answer the question of why did the European Union pursue integration in the field of cybersecurity, in this paper y-centric explaining outcome process tracing is selected as a method. Explaining outcome process tracing is considered most adequate for this paper because of the specificity of the field of cybersecurity, more precisely because of the multistakeholder involvement in cybersecurity governance. The method enables application of multiple theories in order to best explain the developments in cybersecurity, a field in which a lot of member states did not have any strategies and legislation before the push for harmonization at European level. This type of process tracing is traditionally adopted for the exploration of puzzling cases, which differ from the norm (Beach and Pedersen 2013). As an example guiding the work with this method the work of Schimmelfennig (2001) on the Eastern enlargement and state's positions is taken into account.

The core assumptions of supranationalism and intergovernmentalism have been presented and will be used for the analysis of integration steps in the field of cybersecurity. The way the method will be applied is through a chronological analysis of the biggest milestones, which shaped cybersecurity as a policy field in the European Union. The next paragraph presents the key steps in cybersecurity integration and categorizes them into three separate stages. Based on the evidence presented it will be decided whether supranationalism or intergovernmentalism offer a better explanation of the different milestones in cybersecurity integration so far. This approach enables a comprehensive explanation, which fits the specifics of the case presented (Beach and Pedersen 2013).

The scope of this paper is the period between the first mentions of cybersecurity at supranational level in the EU in the 1990s until 2019 when the European Cybersecurity Agency ENISA was last regulated and granted a permanent mandate. This time period is selected although new initiatives in the field of cybersecurity are ongoing and emerging, because by that time the first cybersecurity Directive (NIS) was passed and the Cybersecurity Agency of the Union was established, which marks the completion of the first steps as part of the established policy field of cybersecurity. The goal is to trace back processes from the start and explore the role of different actors, especially with a focus on supranational actors and members states, as they are the dominating drivers of integration according to the two major schools of European integration. Therefore, a period of time, in which the influence of all the relevant actors mentioned should be selected. While the Commission had a leading role from the beginning of the integration processes in cybersecurity, states mobilized at a later point, more specifically after the release of the Cybersecurity Strategy and around the work of the adoption of the following pieces of legislation: NIS Directive and the Regulation on ENISA, which both mark the first effort for harmonization of member state law on cybersecurity (see Christou 2019).

Based on literature on cybersecurity in the EU (see Christou 2019; Kasper and Vernygora 2020; Brandão and Camisão 2021) 3 time periods which will be analyzed separately in this paper are determined. The first one is in the early years of European integration, which is marked by the first Commission initiatives and ends with the eEurope initiative introduced by the Prodi Commission in 1999. The next time period is the rise of security threats in the European Union, which starts in 2001 with 9/11 and is followed by the cyberattacks on Estonia and ends with the comprehensive approach to cybersecurity at European level through the Cybersecurity Strategy published in 2013. This period is mostly shaped by reactive initiatives at EU level, whereas the last period analyzed is related to the long process of the negotiations on the NIS Directive and the expansion of the scope of ENISA until 2019, whereby the member states had a major role when shaping the legal acts.

These periods are chosen by taking into account the different historical developments, rhetoric and evolution of cybersecurity initiatives at EU level. The first stage stands out with a strong economic rhetoric and a number of non-binding initiatives, whereas the rhetoric during the second stage shifts more towards a combination of security and economics. The last stage in the 2010 is the period of time with the most EU legislative acts related to cybersecurity, amongst which are the NIS Directive, GDPR, the Regulations on ENISA etc.

For the analysis in this paper data and official documentation from European Commission, Council of the EU and other EU institutions' official websites are used. The processes of the ordinary legislative procedure related to ENISA and the NIS Directive are analyzed using the European Parliament Legislative Observatory, while the rest of the data is primarily based on existing literature. Using data from these sources enables a first-hand objective analysis of the positions of these institutions, whereby the Commission is seen as a supranational actor and a policy entrepreneur, the activity of which is considered to be reflected in Communications and legislative proposals. Respectively the Council of the EU and the European Council are considered as intergovernmental institutiona which represent the interests of the member states and their dominant societal interest groups. The data used for the understanding of the position of the Council is derived from Resolutions and official positions regarding legislative proposals. The influence of transnational groups is explored through scholarly contributions and the existence of international forums enabling the formation of transnational demands. Through this analysis of the processes, the main drivers of European integration in this field should be revealed.

4 First steps towards cybersecurity in the European Union

In 1990 the Commission released a Communication which highlighted the importance of data protection and information security calling on for more EU regulation in these fields (Commission of the European Communities 1990; Brandão and Camisão 2021, 6). With it, the EC launched a proposal for a Directive concerning the protection of individuals in relation to the processing of personal data, which is a major step towards integration in the field of information. The Directive 95/46/EC (1995) highlights privacy as an individual right of European citizens and the importance of regulating personal data at EU level as a vital step towards enabling the functioning of the

Internal Market. As in the next initiatives presented in this paper the reasoning behind the first Commission initiatives is economic. However, in 1992 a Council Decision 92/242/EEC (1992) was passed, in which states encouraged only limited supranational efforts in the area of information security, while explicitly stating that the member states preserve their control over information systems security at the national level (Brandão and Camisão 2021, 6). This points to the constraining influence of member states on EU supranational institutions as proposed by intergovernmentalists, who argue that supranational organizations cannot pursue their own agenda because member states are in control of them and use them as tools to pursue their goals (Moravcsik 1998). However, the next integration steps accelerated by the Treaty of Maastricht show different developments.

4.1 The first initiatives of the EU and functional spillover

The Maastricht Treaty is seen as a major step in European integration whereby it laid the foundations for the common currency and deeper economic integration and established a legal framework for common foreign and security policy. The expansion of EU competences led to the chances of deeper integration, which respectively spilled over into the field of network and information security as presented in the following paragraphs.

The first mention of network and information security at EU level happened in the Bangemann report in 1994 (Christou 2019, 7), which comes after the adoption of the Maastricht Treaty in 1993 that significantly expanded the competencies of the EU. The report was prepared at the request of the European Council, which wanted to get recommendations on measures that could be taken to improve Union action in the field of information (Cordis 1994). The report outlined recommendations that strongly focus on the potential benefits for the Internal Market while also acknowledging the challenges faced in this field (Bangemann Report 1994; Berleur and Galand 2005). Berleur and Galand (2005, 39-40) find through their analysis of the Report that economic values is the most prevalent indicator in the report.

Even though at first it seems like the Council had a decisive role in the Report, it is of high importance to look closer at the authors of the Bangemann Report, which was mainly prepared by representatives of the private sector from transnational firms such as Volvo, IBM, Telefonica and others (Bangemann Report 1994, 2; Berleur and Galand 2005, 38). The benefits presented in the report are mainly of economic nature and the potential challenges to the future information revolution in Europe require regulation of privacy and information security to ensure maximum benefits for the members of the Single Market (Bangemann Report 1994, 21). The report was adopted by the Council and marked the beginning of the economic framing of the importance of the information sector, which was later taken over by the European Commission (Brandão and Camisão 2021).

The background of the members of the group behind the report and the strong economic focus show that transnational interest came into play when it came to a demand for shaping information regulation in the EU. These findings confirm the supranationalist expectation that integration develops when there is demand from transnational groups, which turn to supranational institutions in this case the European Council. Furthermore, the emphasis in the report on the importance of introducing EU measures ensuring privacy and information security points to the functional spillover related to previous integration steps in the framework of the Internal Market, which apart from the pressure from transnational actors is driven by the rational interest to avoid potential costs due to the lack of privacy and information security measures. Some examples of the rational thought are the facts presented in the Bangemann Report such as the potential reduction of costs through the implementation of electronic communication like emails, teleworking and distance learning (Bangemann Report 1994).

4.2 The Commission as a supranational policy entrepreneur

Over the years after the adoption of the Bangemann Report, the European Commission took noticeable action in response to the transnational demand for integration in the field of information. Under the leadership of Romano Prodi during his 1999-2004 mandate as President of the European Commission, a variety of communications were released, the eEurope initiative started and the European Union agency for information and network security was established in 2004. The initiatives will be analyzed in the current section, however, it first needs to be pointed out that Prodi was part of the Bangemann group (Bangemann Report 1994; Berleur and Galand 2005) and had close ties to European industrial power through his previous work as a President of the IRI – the Institute for Industrial Reconstruction, which by 1993 was the seventh biggest company in the world (Reference for Business 2021). This once again shows the influence of transnational economic interest on European policies.

In response to the adoption of the Bangemann report in the Council Conclusions of the Summit in Corfu (European Council 1994), the Commission went on to release an Action Plan through a Communication to the Parliament and Council in July 1994, in which emphasis was placed on 4 key areas also stressed in the Bangemann report - legal and regulatory framework, societal and cultural aspects, promotion and networks and basic services (Commission of the European Communities 1994). In light of the Bangemann recommendations, the latter Communication marks the first mention of the ambition to establish a supranational authority in the field of information from the side of the EU (Commission of the European Communities 1994, 3). This Action Plan was followed by a Rolling Action Plan in 1996, proposed by the EC, establishing even more goals in the field of information. Among the accomplishments of the first Plan are the liberalization of the telecommunications sector, the support of regional initiatives and the support given out to the multimedia content industry in Europe (European Commission 1996). The revised plan aims at improvement of the business environment, ensuring better education on information, tackling challenges of information society for citizens and investing in international cooperation (European Commission 1996).

In 1995 the European Commission started a new initiative called the Information Society Forum, which aimed to bring together its 128 members from businesses, industries, trade unions, youth organizations, etc. The Forum's goal is to provide European institutions with advice and incentivize reflection related to the rise of new technologies in Europe (Cordis 1996). This Commission initiative promotes the socialization and exchange of transnational groups and with this the development of European integration in the field of information. Furthermore, through forums like this the Commission establishes the important connection between these actors and supranational institutions and through this platform makes the voices of transnational groups heard and taken into consideration in the formation of future proposals.

The Commission continued pursuing the expansion of its competencies by tasking the University of Würzburg to provide an informative report about the legal issues of computer-related law, whereby the findings of the study encourage more centralized action in the European Union regarding cybercrime, whereby the study includes specific recommendations for the establishment of EU level law in the field of information security (Sieber 1998). This specific study can be seen as an effort of the EC to follow its own agenda and gain more authority through expertise and capacities. This action is then followed by the eEurope initiative of the European Commission, which marked the start of the mandate of the Prodi Commission, whereby the initiative was introduced by the newly established Directorate General dedicated to Information Society (Berleur and Galand 2005, 44). The eEurope initiative outlined 10 ambitious priorities and set deadlines for their implementation in the years shortly after the publication of the Communication on the initiative (European Commission 1999), which were not binding due to the non-binding nature of Communications. Among the priorities were online healthcare, online government, intelligent transport and electronic participation for disabled persons (European Commission 1999), all of which show the high ambitions of the Prodi Commission.

The described developments in this section show the driving role of the European Commission for the progress in the area of information and the relative lack of state involvement. By highlighting the relation to the Internal Market and the potential benefits and costs, the Commission managed to illustrate the urgency of policy in the area of information. Furthermore, it has to be taken into consideration that the above-mentioned initiatives were all decisively shaped by the recommendations of the Bangemann report in 1993, which can be concluded based on their texts that either refer to the report or reflect the Report's priorities. This observation illustrates the path dependence over the years. Therefore, it can be concluded that at this stage supranationalism provides the best explanation of the developments. Supranational institutions and transnational actors led the way, while states tended to accept and support the proposed initiatives, which, however, had no binding impact on states. While these initiatives laid the groundwork for the future development of cybersecurity in the EU, goals remained rather vague and harmonization of national law was pursued only through the Directive concerning the protection of individuals in relation to the processing of personal data.

5 Threats – an intensifier of European cybersecurity integration

5.1 Conventional terrorism and the establishment of ENISA

Some scholars present the EU as reactive in the realm of cybersecurity. In September 2001 the world experienced the deadliest terrorist attack in history when 4 commercial US planes were hijacked and crashed into different buildings in the US. The incident had a worldwide impact and shaped the perception of terrorism and security worldwide. The attacks had a severe economic impact on the global economy and the US and showed that information and communication networks infrastructure can be threatened by attacks (Christou 2019, 11), which made action against terrorist threats in the European Union urgent.

Along with a variety of measures to combat terrorism, the Commission continued its ambitions from the 1990s to create an European authority responsible for coordination and harmonization in the context of information policies and proposed a Regulation establishing the European Network and Information Security Agency, which was rapidly adopted in a year and was completely functional by 2005. What is interesting to observe, is the change in the framing of the issue, which had previously predominantly been shaped by economic rhetoric as shown in the previous section. Instead, “the language of risk” (Christou 2019, 11) is adopted by the European Commission in its proposal. Although the explanatory memorandum of the proposal begins by presenting the connectedness of Europeans and European business as reasons for more international cooperation in cybersecurity, it does not go on to outline economic costs and benefits, which is a different approach compared to the early communications of the Commission. The emphasis is clearly on security, critical infrastructure, the new emerging threats to the Union and the need for a centralized approach despite concerns and lack of trust coming from member states. The impact of the 9/11 attacks is not just assumed by this paper but is explicitly mentioned in the explanatory memorandum of the Commission proposal in 2001, stressing that computer and communication systems are increasingly in charge of public infrastructure such as public transportation infrastructure, which is a matter of national security as the incidents of 2001 have shown (European Commission 2003, 2).

What stands out is the Commission’s initiative to establish the Agency, which can be seen as a natural continuation of the earlier action taken by the Commission in the field of information. The ambitious eEurope initiative and the rise of new threats to national security give incentive to aim for even more integration in the policy area of information. It is notable to mention that the EC, taking into account the recommendations of the Bangemann Report, included the creation of a centralized authority in the field of information in its 1994 Action Plan (Commission of the European Communities1994). The Council did not explicitly state a position on the establishment of an authority in the field of information even during the extraordinary summit after the attacks (European Council 2001). The 9/11 attack seems to have been the perfect time for the Commission to react and use the opportunity to pursue its agenda. The ambition of the Commission is also reflected in the initial proposal, in which the Commission wants to be the sole stakeholder responsible for the decision on the potential extension of the mandate of ENISA and wants to be represented by the same amount of members in the Management Board of the Agency as the Council (see European Commission 2003).

While the initiative to establish the Agency comes as a big attempt to deepen integration and expand the competencies of supranational institutions such as the Commission, the framing of the issue can be seen as what Moravcsik describes as geopolitical with the goal of achieving economic benefits and preventing costs (Moravcsik 1998). In terms of preferences, the member states are facing a clear threat to all of them due to the interconnectedness of their economies which makes international cooperation desired. Examples of this are the mentions of the importance of improved security for businesses (European Commission 2003). ENISA can also be seen as an entity empowering the states, especially due to the fact that cyber threats are of cross-border nature and a lot of states had a low level of preparedness for attacks. Furthermore, the competencies of ENISA do not interfere with the sovereignty of states, as ENISA in its first mandate was mainly responsible for assistance to the Commission and the member states. What stands out is the amendment of the original proposal, brought up by the member states regarding the role of the Agency. The Council proposes that the role of the Agency is only restricted to an advisory role (Council of the European Union 2003) and with this stopping the Commission’s ambition to provide the Agency with power to coordinate national cybersecurity measures and facilitate the implementation of Community measures (European Commission 2003). Moreover, the member states amended the parts of the proposal related to the Management Board of the Agency, whereby the Council changes the number of six Council representatives in the Management Board to one representative from each member state, while also reducing the number of representatives selected by the Commission (see European Commission 2003, Council of the European Union 2003). These changes can be seen as quite fundamental for the established Agency, whereby the course of integration through the careful choice of an institution seems to be under the control of the nation-states, which strategically changed the original proposal to preserve their national sovereignty, whole also ensuring vital benefits of cooperation.

To sum this section up, the path dependence and supranational entrepreneurship of the Commission have to be acknowledged as important for the establishment of the Agency. However, the member states made significant changes to the core of the proposed Regulation on ENISA through which they shaped the functions of the Agency. In this context, the theory of Andrew Moravcsik seems to better explain the outcome of this step of integration in the field of information and network security.

5.2 Cyberattacks and EU Cybersecurity Strategy

A day after the signing of the Final Act on ENISA, Europe experienced what is often referred to as the European 9/11, a deadly terrorist attack at the Atocha train station in Madrid (European Commission 2021). A year later a massive attack of suicide bombers in London shook Europe again. While the threats were increasing in the realm of terrorism, the threat in cyberspace soon became apparent with the consecutive attacks on Estonia and Lithuania in 2007, followed by the spread of the computer worm Conficker (see Christou 2019; Brandão and Camisão 2021).

In 2007 Estonian authorities decided to move a memorial commemorating Soviet Liberation from Nazism from the city center of Tallinn, which led to civil unrest among Estonian ethnic Russians. This event was followed by a massive series of distributed denial-of-service (DDoS) attacks on Estonian public and private infrastructure. The websites of all ministries were attacked, as well as the online infrastructure of two banks and some political parties. Given the dependence of Estonia on digital infrastructure these attacks had a major impact and made the state incapable to react to the attack. The costs estimated by one of the attacked Banks were around 1 million (Herzog 2011, 50-52). The cyberattacks on Estonia were a sign to the international community what detrimental effect on the functioning of states cyberattacks can have and how even individuals can be behind such attacks (Herzog 2011, 52). Multiple European countries, as well as international organizations such as NATO and the EU with ENISA, helped the recovery of the Estonian systems and helped to assess the situation (Herzog 2011, 54).

Just one year later Lithuania faced a similar situation, whereby the state triggered numerous attacks after passing a law, which bans communist symbols across the country. Over 300 public and private websites were damaged by the attacks that made communist symbols appear on the attacked sites (Danchev 2008). Later attacks that year targeted the tax office website of the country (The Baltic Times 2008), aiming to destabilize the country. Over the next years after these two major attacks, significant cyberattacks on public infrastructure have been experienced by Germany, Belgium, France, the European Commission and Latvia, whereby some attacks were on private actors like in Germany, whereas others targeted governments (Belgium) and in the case of the Commission and France aimed to get access to confidential information ahead of the major political meeting of G20 in 2011 (Center for Strategic & International Studies n.d.). Additionally, EU member states were the main victim of the worm Conficker. Several incidents targeting public security infrastructure in the UK occurred, while the German Armed Forces and the French Navy dealt with the mass spread of the virus in their systems in early 2009 (Spiegel 2009). The attack on the Manchester City Council cost 1.5 million pounds including direct service-related costs and cleanup costs (Manchester City Council 2009, 8), whereas the costs that the worm has had worldwide have been estimated to amount to more than 9 billion (Danchev 2009).

All these incidents showed countries the destabilizing effect (Kello 2017, 213) of cyberattacks and the costs they can have. The large increase in the number of cyberattacks presented the European Union with a challenge that it had to react to but did not yet possess the capacities to do so. The lack of capacities to provide assistance to the attack on EU member states experiencing cyberattacks became especially apparent in comparison to NATO, which as an international organization solely responsible for defense provided Estonia with assistance to tackle the attacks (Herzog 2011), while ENISA could only provide assessment of the situation due its limited scope. Based on studies of the European Commission, in 2007 the Commission released a Communication, which highlights the cross-border impacts of cybercrime and therefore the need for international cooperation at EU level, whereby the concerns of the Commission got confirmed by the following events in Estonia (see European Commission 2007; Brandão and Camisão 2021). The approach to cybersecurity until the Treaty of Lisbon had been considered fragmented (see Brandão and Camisão 2021, 1; Kasper 2020) due to the existing legal framework of the Union. The Lisbon Treaty enabled a more comprehensive approach to cybersecurity in the European Union which is reflected in the next initiatives of the Union (Dewar 2015), although cybersecurity is not explicitly mentioned as a competence established by the Treaty. In response to the variety of cyber threats and with the newly gained flexibility when it comes to the legal aspect of Commission initiatives, the Commission proceeded to release a variety of initiatives in the realm of cybersecurity – the Internal Security Strategy, the Digital Agenda for Europe and the Cybersecurity Strategy of the EU. A noticeable change is to be observed in the names of these initiatives that refer to the cyberspace and the threats coming from it as a separate domain that needs specific measures and cooperation.

The other clear change observed is the recognition of the problem by member states. Before 2013 only 13 member states had dedicated cybersecurity strategies on the national level (European Parliament 2013) and only 16 had ratified the Council of Europe Convention on Cybercrime before 2010 (Council of Europe, n.d.), whereby a clear increase follows with the rise of the salience of cybersecurity in the EU (König and Wenzelburger 2018). The role of the European Commission can be seen as vital, as the Commission was the actor pushing for more integration in cybersecurity once again utilizing the economic rhetoric (Brandão and Camisão 2021) which became of great importance in the context of the Global Recession.

The establishment of the Digital Agenda for Europe was majorly influenced by the Commission's economic rhetoric and was the first step towards recognizing the importance of cybersecurity as a distinct policy field in the EU. Security and economic benefits are presented as interconnected and of high importance for the Single Market and the recovery from the Global Recession, taking into account that the ICT sector made up 5% of EU's GDP. The Agenda sets the goal to pursue a variety of legislative initiatives in the field of information security, including the expansion of the competencies of ENISA (Commission 2010a). The security aspects of the Digital Agenda were later outlined in the Internal Security Strategy of the Commission, where five strategic objectives were presented, among which raising levels of security for businesses and individuals in the cyber domain, whereby the increased number of attacks is stressed in the Commission Communication. The proposed steps to tackle cybersecurity are expressed in building up law enforcement and judiciary capacities, improving the response to cyberattacks and cooperation with industries. Furthermore, each country had to establish a national Computer Emergency Response Teams (CERT), whereby the EU institutions also create such teams (European Commission 2010b).

These two Commission initiatives laid the groundwork for the first international cybersecurity strategy, the first EU document explicitly putting forward a framework for the field of cybersecurity. The Strategy adopts a comprehensive approach and uses a pillar structure similar to the structure established by the Treaty of Maastricht for the EU focusing on resilience, cyber defense and combating cybercrime (Carrapico and Farrand 2020; European Commission 2013a). The Strategy is also released together with the NIS Directive, as part of the efforts to ensure network and information security across the Union by establishing minimum standards for the national level of network and information security including the requirement for the development of national strategies, obligatory reporting of significant incidents by providers of services related to critical infrastructure and the creation of CERTs and national authorities responsible for NIS (Commission 2013b).

In the case of the variety of initiatives following the turbulent rise of cyber threats, the European Commission stood out with its leading role emphasizing the importance of a more unified approach to the cyber domain and its benefits and costs. All of the above initiatives stress the value of international cooperation and the expertise of the already established supranational institutions such as ENISA, CEPOL and EUROPOL, whereby the aim in 2010 was the establishment of an European Cybercrime Center to further help member states build up their capacities. The expertise of supranational authorities is vital to the member states especially given that a lot of the countries did not have a cybersecurity strategy at national level.

After the EU liberalized the telecommunications sector as part of its first initiatives in the 90s, the private sector was seen as the main target of cybercrime, which changed after the establishment of ENISA. In 2009 the Council released a Resolution, which highlighted how a multi-stakeholder approach to cybersecurity should be at the core of EU network and information security regulation. This shows the readiness of member states to work with the private sector to achieve common goals and can be seen as a sign of acknowledgment of the expertise at supranational level. This argument is complemented by the proposal for extension of the mandate of ENISA (Carrapico and Farrand 2020, Council of the European Union 2009). Given that a majority of countries did not even include the private sector in their cybersecurity strategies before 2016, this Resolution seems to represent an unexpected position of the Council. These demands of the member states are also reflected in all the Commission initiatives presented above.

What can be observed in the Cybersecurity Strategy and the initiatives developed after the adoption of the Lisbon Treaty is a spillover into the field of security, although it is closely related to the preservation of the Internal Market. The Lisbon Treaty which enabled the more comprehensive approach to different aspects of cybersecurity (Carrapico and Farrand 2020) can also be seen as a result of spillover processes when it comes to the big changes in the functioning of the Union. While the Lisbon Treaty can be regarded as an endogenous factor for integration, the terrorist and cyberattacks are exogenous (Carrapico and Farrand 2020) and shaped the rhetoric and sped up the reaction of the EU after 2009. This is reflected additionally in the number of legislative proposals released after the first attack in 2001 – the Regulation establishing ENISA, the GDPR, NIS Directive, Directive on attacks on information systems, Data Retention Directive, etc. This is a big difference compared to the period before 2001 when the only adopted legislative act related to cybersecurity was the Directive on data protection.

Apart from supranational stakeholders having an important role in these integration processes mainly through the provision of expertise, which the member states do not possess to govern cybersecurity successfully on their own, Pierson’s concept of path dependence is to be observed too. The 2001 NIS Communication is the first EC Communication predominantly focused on security and lays out priorities such as the creation of CERTs as a measure to counter attacks, awareness-raising, international cooperation (European Commission 2001). Other EU initiatives focused on resilience, the coordinating role of the EU and coherence in policies and tools (Carrapico and Farrand 2020, 1115). These priorities continued being pursued and became key priorities in the Cybersecurity Strategy of the EU. What also shows the path dependence is the expanded mandate and role of ENISA, which was an Agency largely shaped by the member states in 2003. However, the initially laid down tasks of ENISA by the Commission in 2003 like the task to assist member states in the implementation of Union-wide cybersecurity measures was then pursued with the next Regulation on ENISA, whereby the Council had a critical role to push for the extension of the mandate of ENISA in its Resolution (Council of the European Union 2009).

Adaptation to the supranational regulation in the field of cybersecurity has occurred and the threats only emphasized the importance of international cooperation and the potential costs of an exit. Therefore, I conclude that the stage influenced by the rise of attacks was largely shaped by endogenous and exogenous factors, whereby the response was mainly handled by supranational institutions like the Commission, while the new initiatives and pieces of legislation build upon the content of existing initiatives. The economic logic was interconnected with the security rhetoric and due to the lack of expertise and capacities member states supported this big jump into integration and regulation of the new policy field of cybersecurity.

6 The institutionalization of cybersecurity as a policy field in the EU

6.1 The revised role of ENISA

In the years between 2010 and 2019, ENISA was subject to Regulation two times, whereby the expansion of competencies and mandate of ENISA can be seen as significant steps in the integration process in cybersecurity.

In 2009 the Council of the EU proposed an extension of the mandate of ENISA (Council of the European Union 2009) for the second time after 2008 (ENISA n.d.), whereby given the increased salience of the issue at European level and the rise of cyberattacks the European Commission went on to propose an ambitious Regulation expanding the objectives and tasks of ENISA in 2010. The new Regulation 526/2013 highlighted the role of ENISA as a coordinator between states, supranational institutions and private actors in the multistakeholder approach of the EU to cybersecurity. Furthermore, it is important to note that the initially proposed task of ENISA (European Commission 2003) as an advisor to member states when it comes to the implementation of EU measures in the realm of cybersecurity became a part of the Regulation 526/2013 adopted in 2013. Not only is the role of the private sector central to the expanded role of the Agency, but the Agency gained a role to support the development of EU policies, capacity building and standardization, while it also is expected to closely work with other EU relevant bodies to establish synergies especially in the field of cybercrime and privacy (Regulation 526/2013). The adoption of the NIS Directive 2016/1148 made the role of ENISA more central and important and given the positive evaluation of the Agency's work the Commission proposed a permanent mandate of ENISA and establishing it as the cybersecurity Agency of the EU and as a vital contact point for stakeholders in the domain of cybersecurity in the EU.

Compared to the role of ENISA as only an analytical and advisory actor with a very limited scope during its first mandate, the current role of ENISA is significantly bigger in the field of cybersecurity. I argue that some of the major factors that shaped the role of ENISA as an integration milestone were path dependence and the role of transnational private actors. In terms of path dependence, ENISA was established as an authority to be responsible for network and information security. As the policies evolved the role of ENISA had to be adapted accordingly. Moreover, the willingness of member states to extend the mandate of the Agency show that they have overtime not just benefited from it, but also adapted to the existence of ENISA, which supports the arguments of Pierson (1996). Not only did the Agency get changed because of the adoption of the NIS Directive, but also because of the Telecoms Package which emphasized the role of private actors, therefore creating a need for more centrality of the private sector in the tasks of the Agency (Farrand and Carrapico 2018). In regard to the private actors, Farrand and Carrapico (2018) argue that their role as regulators of policies at EU level increased whereby the European Commission had an active role in facilitating this multistakeholder approach reflected in the Regulations on ENISA as well. Intergovernmentalists might argue that the interests of national private actors are represented by states on the EU level, however, it has to be acknowledged that many EU initiatives starting from the Information Society Forum have enabled the exchange between private actors, whereby these exchanges lead to transnational interests and interdependence directly communicated to the supranational authorities such as ENISA and the

Commission. This process of the rising importance of the private sector can be seen as an outcome of the variety of international forums like Forum of Incident Response and Security Teams and the Internet Engineering Task Force, whereby different lobby groups further highlight the influence of transnational interests and their role in the field (Kasper 2020, 178).The establishment of ENISA as a contact point for multistakeholder communication about cybersecurity can be seen as another step encouraging this type of supranational communication, which would lead to more integration in the cybersecurity domain in the future.

6.2 The NIS Directive

The NIS Directive is a focal point for the development of cybersecurity policy in the EU. It took the Council and the Parliament 41 months to adopt the NIS Directive. With 89 % of European legislative Acts being passed during the first reading in the mandate of the 2014-2019 Commission and with the average time for acts to be passed at second reading taking around 40 months (European Parliament n.d.), the NIS Directive can be seen as a more contentious topic for the institutions and therefore also as an important step for all stakeholders involved.

The adopted NIS Directive is aiming to 1) increase the levels of cybersecurity across the Union by improving national cybersecurity capabilities through the establishment of competent national authorities, 2) establish minimum requirements for security and notification particularly in regard to digital service and essential service providers, 3) create grounds for better international cooperation within the Union through a network of CSIRTs and the establishment of a supranational cooperation group and 4) introducing appropriate penalties at national level that help ensure the achievement of the outlined goals in the Directive 2016/1148.

After the Directive was proposed the European Social and Economic Committee, which is comprised of representatives of employers, workers and other interest groups, released an opinion on the Directive stating that it gives too much flexibility to member states, most of which are still lacking in their cybersecurity commitments at national level which creates big differences across the Union. Therefore, the Committee expressed the need for stricter binding measures through a Regulation instead of a Directive, which only enables too much freedom in the interpretation and implementation of the legislative act (European Economic and Social Committee 2013). The amendments later passed by the European Parliament reflect the concerns of the European Data Protection Supervisor that the proposed Directive by the Commission is not offering a holistic approach to cybersecurity and fails to include provisions about data protection (European Data Protection Supervisor 2013; European Parliament 2014).

Based on the amendments of the Parliament and after further interinstitutional negotiations the Council then adopted its position before the Second Reading, whereby a few changes to the original proposal stand out as a reflection of the position of the Council. Firstly, the Council adopted the establishment of a network of national CSIRTs instead of the originally proposed Union NIS cooperation plan proposed by the Commission. The network indirectly includes the Commission as an observer and ENISA as an advisor, which is vastly different compared to the initial proposal which foresaw a central role of ENISA and the Commission to shape a common EU NIS approach to cooperation (see European Commission 2013b; European Commission 2016, 52016PC0363, Directive 2016/1148). Instead, an intergovernmental network was established. Secondly, the Council excluded public administration as an operator of essential services, although during a public consultation related to the Directive more than 90 % of the respondents indicated that public administration should report security breaches to the national competent authority (European Commission 2013b).

The above-presented developments show the clear involvement of the member states, which keep the Commission's ambitions within limits through their positions. Parallel to these negotiations the increasing interest of the member states was also demonstrated in the rhetoric and priorities of the Council Presidency Trios since 2011 and the establishment of intergovernmental advisory platforms such as the Friends of the Presidency Group on Cyber Issues and later the Horizontal Working Group on Cyber Issues (Kasper and Vernygora 2020, 194-198). The problems when it comes to trust and information sharing from the side of member states have been highlighted by the Commission in 2001 already (European Commission 2003, 2) and continued to shape the decisions of the Council (Kasper and Vernygora 2020). The preservation of the national sovereignty and the control of states over international institutions is evident in the adopted NIS Directive. When it comes to the exclusion of public administration from the NIS Directive, Kasper and Vernygora (2020) interpret this as a sign that member states see this as a big infringement on their national sovereignty. Moreover, the establishment of the CSIRTs network instead of a supranational EU NIS cooperation plan shows the willingness of the states to keep cybersecurity intergovernmental and not allow unintended consequences to emerge due to supranational involvement. Based on the states preferences the institution, in this case, the NIS Directive was shaped by the dominating role of the member states, which makes Andrew Moravcsik's intergovernmentalism an appropriate explanatory theory for this milestone.

7 Conclusion

The goal of this paper was to answer the question of why did the European Union pursue cybersecurity integration by using the theories of liberal intergovernmentalism and supranationalism. The analysis of the processes that led to the establishment of the policy field of cybersecurity at Union level shows that due to the involvement of a variety of stakeholders in cybersecurity management different both theoretical approaches can be applied. The paper explored 3 periods of time, starting with the earliest steps towards integration in cybersecurity in the 1990s, which was predominantly shaped by the strong role of the European Commission as a supranational institution and a strong economic logic related to the spillover effect of the Internal market. Furthermore, this stage is marked by a strong influence of transnational groups. The next stage is shaped by the increasing threats in the realm of terrorism and cyber threats, therefore the economic rhetoric can be seen as intertwined with the security rhetoric. After both 9/11 and the cyberattacks in the late 2000s, a mobilization of supranational authority at Union level is to be observed, especially related to the establishment and expansion of ENISA. Apart from the exogenous shocks, the Lisbon Treaty as an endogenous driver of integration enabled a more comprehensive approach to cybersecurity in the EU. The Commission initiatives which followed the attacks and the Treaty of Lisbon stand out with their roots in older initiatives which shows the path dependence of the integration process. However, an exception in this process is the first Regulation on ENISA, which was largely shaped by the preferences of the member states and was reflected in their institutional choice for the Agency through the Regulation. This member state involvement is however less pronounced in the revisions of the Regulations on ENISA in the 2010s when the member states agreed on and were a part of the initiation of a significant expansion of the Agency's scope. Together with the last extensions of ENISA, this paper explores the NIS Directive as the final identified time period. The process of the negotiations on the NIS Directive slightly resembles the situation with the first ENISA Regulation, whereby significant changes were made to the originally proposed Regulation by the Commission. The long negotiations revealed the dominant role of states, which introduced changes to the proposal that showcase sovereignty concerns and willingness to restrict supranational authority in the field of cybersecurity.

As shown above both supranationalism and intergovernmentalism deliver explanations for different milestones in the process of cybersecurity integration. A few conclusions can be made based on the results. First, the Commission, its economic logic and its communication with transnational groups were the reasons for the emergence, development and expansion of cybersecurity regulation at Union level. Second, the role of supranational and transnational actors reaches its limits when new legislative acts are introduced, whereby states significantly shape the final acts in line with their interests and sovereignty concerns. Third, path dependence is prevalent in the initiatives in the field of cybersecurity, while stakeholders including member states adapt to the existing EU level policies and act within the established framework of existing rules, which continues the pursuit of integration. Therefore, the long NIS Directive process of negotiations can be seen as the first step towards adaptation of the member states, which would likely delegate more authority to the supranational actors in the future as was the case with ENISA. Based on these conclusions it can be said that supranational theory explanations can best be applied for the beginnings of integrational processes, as well as for the exploration of long term integration in the field of cybersecurity through the concept of path dependence, while liberal intergovernmentalism can mainly be applied to the legal acts following the ordinary legislative procedure, especially when these acts pose a new ambitious and innovative proposal of the Commission. For this reason and due to the adaptation as a consequence of the first NIS Directive, it could be expected that the current proposal for NIS 2 Directive would be less contentious for the member states.

The present paper analyzed some of the biggest milestones in the history of cybersecurity at EU level by using European integration theories. However, due to its limited scope, the paper does not include an in-depth analysis of legislative acts from the fields of security (Directive on attacks on information systems) and fundamental rights (GDPR), although they are closely related to the field of cybersecurity. Similarly, the only supranational institutions, subject of this analysis, are the Commission and ENISA, although many other bodies such as Europol's EC3, the European Defense Agency and CERT-EU (Kasper 2020) are involved with EU cybersecurity policy. Moreover, the role of NATO in cybersecurity is not taken into consideration in this paper, whereby the specialization of NATO in the field of security and its higher expertise and capacities compared to the EU might have an influence on cybersecurity integration in the EU, as states might consider the cooperation with NATO sufficient for their national level of cybersecurity. However, NATO is more focused on securing its structures and means required for main tasks, so the activity of

NATO in cybersecurity can be seen as mostly related to the purpose of the organization (Štitilis et al. 2017), whereas in the EU the implications for states and their cybersecurity policies are bigger and more far-reaching.

In terms of the application of European integration theories, a more detailed approach can be taken and it would be interesting to observe the differences among member states' preferences, which would also enable a better analysis using the framework of Moravcsik. Moreover, it has to be acknowledged that postfunctionalism might become more relevant in the future of cybersecurity policymaking when the issue is more present in the lives of the mass public in the EU and therefore, is more likely to be politicized. However, based on the current state of cybersecurity, which is primarily elite-driven in the EU, this is unlikely to happen in the short term.

To conclude, the field of cybersecurity in the EU is still new and in a lot of countries only emerging after the initiatives at EU level. The amount of legislative acts created is low, while the connectedness of businesses and individuals is rising and so are the number and variety of cyber threats. The future will show how far EU integration will go in the policy area of cybersecurity and what theories explain integration patterns best might change. But as of the current state of cybersecurity, it is shaped by a variety of factors and even though slower than other policy fields, it is moving towards more centralized action.

References:

Bangemann Report. 1994. Europe and the Global Information Society: Recommendations to

the European Council, High Level Group on Information Society.

Beach, D., Pedersen, 2013. Process-Tracing Methods: Foundations and Guidelines. University of Michigan Press.

Berleur, J. and Galand, J.-M., n.d. ICT Policies of the European Union: From an Information Society to eEurope. Trends and visions. pp.37–66.

Biermann, F., Guérin, N., Jagdhuber, S., Rittberger, B. and Weiss, M. 2019. Political (non-)reform in the euro crisis and the refugee crisis: a liberal intergovernmentalist explanation, *Journal of European Public Policy*, 26(2), pp. 246-266.

Brandão, A.P. and Camisão, I., 2021. Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy. *JCMS: Journal of Common Market Studies*.

Bickerton, C.J. and Hodson, Dermot and Puetter, U. 2015. The new intergovernmentalism: European integration in the post-Maastricht era. *Journal of Common Market Studies*, 53 (4), pp. 703-722. ISSN 0021-9886.

Carr, M., 2016. Public-private partnerships in national cyber-security strategies. *International Affairs*, 92(1), pp.43–62.

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), pp. 1111-1126.

Center for Strategic & International Studies. n.d. Significant Cyber Incidents Since 2006. [Online]. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/210604_Significant_Cyber_Events.pdf?Ig0rKRzJ9Bc2WS95MJVt1pkZll5eJLE7, [Accessed 06.2021.].

Christou, G., 2019. The collective securitisation of cyberspace in the European Union. *West European Politics*, 42(2), pp. 278-301.

Commission of the European Communities. 1990. Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990DC0314&from=EN, [Accessed 06.2021.].

Commission of the European Communities. 1994. Europe's Way to the Information Society. An Action Plan. [Online]. Available at: https://op.europa.eu/en/publication-detail/-/publication/deed9eb9-0b6e-11e4-a7d0-01aa75ed71a1/, [Accessed 06.2021.].

Cordis. 1994. Bangemann report: Europe and the global information society. [Online]. Available at: https://cordis.europa.eu/article/id/2730-bangemann-report-europe-and-the-global-information-society, [Accessed 06.2021.].

Cordis. 1996. Information Society Forum's first annual report puts people first[Online]. Available at: https://cordis.europa.eu/article/id/6511-information-society-forums-first-annual-report-puts-people-first, [Accessed 06.2021.].

Council of Europe. n.d. [Online] Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures, [Accessed 06.2021.].

Council of the European Communitites. 1992. Council Decision of 31 March 1992 in the field of security of information systems (92/242/EEC). [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31992D0242, [Accessed 06.2021.].

Council of the European Union. 2003. Information society, eEurope 2005: European network and information security Agency. [Online]. Available at: https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=265333&t=e&l=en, [Accessed 06.2021.].

Council of the European Union. 2009. Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security. [Online]. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:en:PDF, [Accessed 06.2021.].

Danchev, D. 2008. 300 Lithuanian sites hacked by Russian hackers. *ZDNet.* [Online]. Available at: https://www.zdnet.com/article/300-lithuanian-sites-hacked-by-russian-hackers/, [Accessed 06.2021.].

Danchev, D. 2009. Conficker's estimated economic cost? $9.1 billion. *ZDNet.* [Online]. Available at: https://www.zdnet.com/article/confickers-estimated-economic-cost-9-1-billion/, [Accessed 06.2021.].

Dewar, R. 2015. Cyber-Lisbon? The Impact of the Treaty of Lisbon on European Union Cybersecurity Policy. [Conference Proceedings] (Submitted).

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. *Official Journal of the European Union.* [Online]. Available at: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32016L1148, [Accessed 06.2021.].

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union.* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046, [Accessed 06.2021.].

European Economic and Social Committee. 2013. Opinion of the European Economic and Social Committee on the ‘Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union’. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013AE1414, [Accessed 06.2021.].

European Commission. 1996. Europe at the Forefront of the Global Information Society: Rolling Action Plan. [Online]. Available at: http://aei.pitt.edu/5660/1/5660.pdf, [Accessed 06.2021.].

European Commission. 1999. eEurope - An information society for all.[Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l24221, [Accessed 06.2021.].

European Commission. 2001. 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. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298, [Accessed 06.2021.].

European Commission. 2003. Proposal for a Regulation of the European Parliament and the Council Establishing the European Network and Information Security Agency.[Online]. Available at: https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2003/0063/COM_COM(2003)0063_EN.pdf, [Accessed 06.2021.].

European Commission. 2007. Towards a general policy on the fight against cybercrime. [Online] Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF. [Accessed 06.2021.].

European Commission. 2010a. A Digital Agenda for Europe. [Online]. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF, [Accessed 06.2012.].

European Commission. 2010b. The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. [Online]. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF, [Accessed 06.2012.].

European Commission. 2013a. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. [Online]. Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, [Accessed 06.2021.].

European Commission. 2013b. Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. [Online]. Available at: https://ec.europa.eu/digital-single-market/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and, [Accessed 06.2021.].

European Commission. n.d. Headings: spending categories. [Online]. Available at: https://ec.europa.eu/info/strategy/eu-budget/long-term-eu-budget/2021-2027/spending/headings_en, [Accessed 06.2021.].

European Commission. 2016. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT pursuant to Article 294(6) of the Treaty on the Functioning of the European Union concerning the position of the Council on the adoption of a Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52016PC0363, [Accessed 06.2021.].

European Commission. 2021. Commissioner Johansson's speech at the 17th European Day of Remembrance of Victims of Terrorism. [Online]. Available at: https://ec.europa.eu/commission/commissioners/2019-2024/johansson/announcements/commissioner-johanssons-speech-17th-european-day-remembrance-victims-terrorism_en, [Accessed 06.2021.].

European Council. 1994. European Council at Corfu 24-25 June 1994 Presidency Conclusions. [Online]. Available at: https://www.europarl.europa.eu/summits/cor1_en.htm, [Accessed 06.2021.].

European Council. 2001. Conclusions and plan of Action of the extraordinary European Council meeting on 21 September 2001. [Online]. Available at: https://www.consilium.europa.eu/media/20972/140en.pdf, [Accessed 06.2021.].

European Data Protection Supervisor. 2013. Executive summary of the Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: An open, safe and secure cyberspace' , and on the Commission proposal for a directive concerning measures to ensure a high common level of network and information security across the Union. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014XX0204%2805%29, [Accessed 06.2021.].

European Parliament. n.d. Activity Report. Developments and Trens of the Ordinary Legislative Procedure. [Online]. Available at: https://www.europarl.europa.eu/cmsdata/198032/activity-report-2014-2019_en.pdf, [Accessed 06.2021.].

European Parliament. 2013. EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace. European Parliament Resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP)). [Online]. Available at: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0376+0+DOC+PDF+V0//EN. [Accessed 06.2021.].

European Parliament. 2014. Position of the European Parliament adopted at first reading on 13 March 2014 with a view to the adoption of Directive 2014/…/EU of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014AP0244, [Accessed 06.2021.].

European Union. 2021. European Union priorities for 2019-2024. [Online]. Available at: https://europa.eu/european-union/about-eu/priorities_en, [Accessed 06.2021.].

European Union Agency for Cybersecurity. n.d. ENISA Mandate and Regulatory Framework. [Online]. Available at: https://www.enisa.europa.eu/about-enisa/regulatory-framework, [Accessed 06.2021.].

Eurostat. 2019a. Digital economy and society statistics - enterprises. [Online]. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_enterprises#Access_and_use_of_the_internet, [Accessed 06.2021.].

Eurostat. 2019b. Digital economy and society statistics - households and individuals. [Online]. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Privacy_and_protection_of_personal_identity_.282016_survey.29 , [Accessed 06.2021.].

Farrand, B. Carrapico, H. 2018. Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism. Bures O., Carrapico H. (eds) Security Privatization. Springer, Cham., pp. 197-217 https://doi.org/10.1007/978-3-319-63010-6_9.

Fuster, G.G. and Jasmontaite, L. 2020. Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In: *The International Library of Ethics, Law and Technology*. The International Library of Ethics, Law and Technology, pp.97–115.

Haas, E. B. 1958. The Uniting of Europe. Political, social, and economic forces, 1950-1957. Stanford, CA: Stanford University Press.

Herzog, S. 2011. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, 4(2), pp. 49–60. *JSTOR*, www.jstor.org/stable/26463926 [Accessed 06.2021.].

Hoffmann, S. 1966. Obstinate or Obsolete? The Fate of the Nation-State and the Case of Western Europe. *Daedalus*, 95(3), pp. 862-915.

Hooghe, L., Marks, G., 2009. A Postfunctionalist Theory of European Integration: From Permissive Consensus to Constraining Dissensus. *British Journal of Political Science,* 39, pp. 1–23. doi:10.1017/s0007123408000409.

Internet World Stats. 2021. Internet Usage in the European Union. [Online]. Available at: https://www.internetworldstats.com/stats9.htm, [Accessed 06.2021.].

Kasper, A., Vernygora, V. 2020. Towards a 'Cyber Maastricht': Two Steps Forward, One Step Back. M. Harwood, S. Moncada, R. Pace, (Eds.). *The future of the European Union : Demisting the Debate*, pp. 186-210.

Kasper, A. 2020. EU cybersecurity governance – stakeholders and normative intentions towards integration. In M. Harwood, S. Moncada, R. Pace, (Eds.), *The future of the European Union: Demisting the Debate.* Msida: Institute for European Studies, pp. 166-185.

Kello, L. 2017. The Virtual Weapon and International Order. Yale University Press. *JSTOR*, www.jstor.org/stable/j.ctt1trkjd1. [Accessed 06.2021.].

König, P.D., Wenzelburger, G. 2019. Why parties take up digitization in their manifestos. *Journal of European Public Policy*, 26(11), pp. 1678-1695, DOI: 10.1080/13501763.2018.1544268.

Lambach, D. 2020. The Territorialization of Cyberspace. *International Studies Review*, 22(3), pp. 482–506.

Leuffen, D., Rittberger, B., Schimmelfennig, F. 2022. Integration and Differentiation in the European Union. Palgrave Macmillan.

Manchester City Council. 2009. Report for resolution. [Online]. Available at: https://www.manchester.gov.uk/egov_downloads/Item_11.pdf, [Accessed 06.2021.].

Manjikian, M. 2010. From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly* 54(2), pp. 381–401.

Moravcsik, A. 1998. The choice for Europe: social purpose and state power from Messina to Maastricht. Ithaca, N.Y., Cornell University Press.

Moravcsik, A., Schimmelfennig F. 2009. Liberal Intergovernmentalism. *Theories of European Integration.* Oxford Oxford University Press, pp. 67-87.

Morgan, S. 2020. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. [Online]. Available at: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, [Accessed 06.2021.].

Peterson, J., 2001. The choice for EU theorists: Establishing a common framework for analysis. *European Journal of Political Research*, 39, pp. 289–318. doi:10.1111/1475-6765.00578.

Pierson, P., 1996. The Path to European Integration. *Comparative Political Studies*, 29, pp. 123–163. doi:10.1177/0010414096029002001.

Reference for Business. 2021. History of Instituto per la Ricostruzione Industriale S.p.A. [Online]. Available at: https://www.referenceforbusiness.com/history2/98/Istituto-per-la-Ricostruzione-Industriale-S-p-A.html, [Accessed 06.2021.].

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 Text with EEA relevance. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0526. [Accessed 06.2021.].

Schimmelfennig, F., 2001. The Community Trap: Liberal Norms, Rhetorical Action, and the Eastern Enlargement of the European Union. *International Organization*, 55(1), pp.47–80.

Schimmelfennig, F. Rittberger B. 2015. The EU as a system of differentiated integration : a challenge for theories of European integration?. *European Union : power and policy-making*, Fourth edition, Milton Park, Abingdon, New York : Routledge, pp. 33-62.

Schimmelfenning, F. 2018. European integration (theory) in times of crisis. A comparison of the Euro and Schengen crises. *Journal of European Public Policy* 25(7): pp. 969-989.

Sieber, U. 1998. Legal Aspects of Computer-Related Crime in the Information Society. [Online]. Available at: https://www.law.tuwien.ac.at/sieber.pdf, [Accessed 06.2021.].

Sliwinski, K. F. 2014. Moving beyond the European Union's Weakness as a Cyber-Security Agent. *Contemporary Security Policy*, 35(3), pp. 468-486.

Special Eurobarometer. 2019a. The General Data Protection Regulation. [Online]. Available at: https://europa.eu/eurobarometer/surveys/detail/2222, [Accessed 06.2021.].

Special Eurobarometer. 2020. Europeans' attitudes towards cyber security. [Online]. Available at: https://europa.eu/eurobarometer/surveys/detail/2249, [Accessed 06.2021.].

Spiegel. 2009. Conficker-Wurm. Bundeswehr kämpft gegen Viren-Befall. [Online], Available at: https://www.spiegel.de/netzwelt/web/conficker-wurm-bundeswehr-kaempft-gegen-viren-befall-a-607567.html, [Accessed 07.2021.].

Štitilis, D. Pakutinskas, P. and Malinauskaitė. I. 2017. EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal*, 30(4), pp.1151–1168.

Sweet, A.S., Sandholtz, W. 1997. European integration and supranational governance. *Journal of European Public Policy*, 4(3), pp. 297–317.

Sweet, A.S., Brunell, T.L. 1998. Constructing a Supranational Constitution: Dispute Resolution and Governance in the European Community. *American Political Science Review* 92, pp. 63–81. doi:10.2307/2585929.

The Baltic Times. 2008. Lithuania cyber attacks: Round two. [Online]. Available at: https://www.baltictimes.com/news/articles/20897/, [Accessed 06.2021.].

Treaty on European Union. 2012. Consolidated Version of the Treaty on European Union. *Official Journal of the European Union*. [Online]. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF, [Accessed 06.2021.].

Tsebelis, G. and Garrett, G., 2001. The Institutional Foundations of Intergovernmentalism and Supranationalism in the European Union. *International Organization*, 55(2), pp.357–390.

Wessel, R. A. 2015. Towards EU cybersecurity law: Regulating a new policy field. *Research Handbook on International Law and Cyberspace,* 19, pp. 403-425.