

### The European Cybersecurity Competence Centre - One More Step towards Supranationalism

Suciu, Sebastian; Cirjan, Andreea-Larisa

Veröffentlichungsversion / Published Version

Zeitschriftenartikel / journal article

#### Empfohlene Zitierung / Suggested Citation:

Suciu, S., & Cirjan, A.-L. (2022). The European Cybersecurity Competence Centre - One More Step towards Supranationalism. *Perspective Politice*, 15(1-2), 57-73. <https://doi.org/10.25019/perspol/22.15.4>

#### Nutzungsbedingungen:

Dieser Text wird unter einer CC BY-NC-SA Lizenz (Namensnennung-Nicht-kommerziell-Weitergabe unter gleichen Bedingungen) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier: <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.de>

#### Terms of use:

This document is made available under a CC BY-NC-SA Licence (Attribution-NonCommercial-ShareAlike). For more information see: <https://creativecommons.org/licenses/by-nc-sa/4.0>

**How to cite this paper:**

Suciu, S.; Cîrjan, A. L. (2022). The European Cybersecurity Competence Centre – one more step towards supranationalism. *Perspective Politice*. XV (1-2), pp. 57-73.

DOI: 10.25019/perspol/22.15.4.

Received: November 2022.

Accepted: November 2022.

Published: December 2022.

**Copyright:** © 2022 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license.

*Article*

# The European Cybersecurity Competence Centre – One More Step towards Supranationalism

---

**Abstract:** *The evolution of the European Union has been influenced by many social, economic, technological, political or even climate factors since its creation in 1957. The supranational character of the Union has been questioned over the years by many authors focused on the study of European integration due to the changes that occurred within the EU. Over the last century, the rapid pace of technology development, especially digitalization, directly influenced EU and the integration theories related to it. The COVID-19 pandemic showed everyone that digitalization does not represent an option anymore, it is a necessity. In regard to this matter, the European Union adopted over the last years several policies, strategies and normative acts that aim to ensure a higher level of digitalization at EU and Member States level. A key factor in the digital transformation is represented by cybersecurity, therefore, EU took important steps into protecting itself and the Member States from cyber threats: it established specialized institutions, developed two strategies and adopted compulsory normative acts for the Member States. This paper focuses on the new established European Cybersecurity Industrial, Technology and Research Competence Centre, emphasizing its supranational features with the purpose of proving that development of such institutions sustain the supranational theory of European integration, as well as EU's supranational character.*

**Keywords:** *cybersecurity; digital policies; European Union; supranationalism; technology*

## 1. Introduction

The European Union (EU) was established 64 years ago, as a supranational economic community that aimed to help 6 states in their economic activities. Since

then, EU has become an important international actor, which represents the interests of 27 Member States and has a significant role in the international arena. Its supranational character is defined by its structure, as well as its actions in relation with third-parties or Member States. EU developed specific policies and strategies in order to achieve its goals, as a supranational entity. Due to the societal evolution and the technology development, EU defined clear objectives that aimed to keep the Union up to

date towards the latest global challenges, while striving to become a global leader in some areas.

---

### **Sebastian SUCIU**

Independent researcher;  
mr.sebastian.suciu@gmail.com

### **Andreea-Larisa CÎRJAN**

Independent researcher;  
c.larisa1998@yahoo.com

---

Nowadays, the great majority of EU's population use digital technologies as an integrated part of their lives. In regard to this matter, the European Union took several steps in assuring a higher level of digitalization at both EU and Member States levels. Moreover, the COVID-19 pandemic proved that digitalization must represent a priority for the EU, as people, businesses and public institutions need to be able to stay connected and conduct their activities efficiently. At the same time, digitalization cannot be achieved without considering the possible threats coming from the cyber space. Cybersecurity has a pivotal role in this process, due to the fact that it ensures the well-functioning of digital activities, by protecting ICT infrastructure, data consumed within the process and users. The European Union understands that cybersecurity represents such an important element and approaches this matter throughout specific policies, strategies for the future and specialized institutions that focus their activity on protecting EU from cyber threats.

The purpose of this paper is to analyse the supranational theory of European integration, as well as EU's supranational character throughout the lens of the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC). In order to achieve this, it is mandatory to have a comprehensive approach over what supranationalism means for the European Union, while focusing on EU's objectives in regard to digitalization. The final objective of this paper is to prove that EU's supranational character is sustained by institutions like the ECCC, which encourage Member States to gather expertise and resources in order to ensure EU's resilience.

## **2. What is supranationalism?**

The theoretical framework is one of the most important parts that needs to be addressed in order to have the full perspective of the puzzle. So, in this case, in order to know how the specific characteristics of the European Cybersecurity Competence Centre comply with the supranational concept it is necessary to explain the meaning of supranationalism.

Supranationalism is one of the multiple theories, along with intergovernmentalism, multi-level governance or constructivism that can be used to describe EU's mechanisms. Supranationalism can be described as a process of decision-making in the international organizations in which states transfer a part of their power to entities or officials, elected by the Member States (Arcas, 2007). In other words, supranationalism changes relations between states from a cooperative perspective beyond an integration one, during this process losing a part of their national sovereignty.

With a long and robust background, Europe faced a lot of changes throughout the history, moving from supranational empire times to decentralized international systems. Thus, supranationalism may represent the antithesis of the Westphalian paradigm or a consequence of a so challenged situation. The idea of forming governance beyond the state implies much more than a normative support. A supranational community that stands for living in a peaceful, secure and free environment with economic trades (United States of Europe) is considered to be the idea of W. Churchill, who mentioned it in his famous speech hold at the University of Zurich in 1946 (Zaharia and Pozneacova, 2020).

Interdependence is the key factor of the supranational theory. As long as the expansion of interdependence continues to grow, states, governments and entities are pushed to cooperate in order to have a better and clearer governance in the region. This interdependence does not

require a specific domain, as it can be economic, digital, financial, environmental or even security related (Telo and Weyembergh, 2020).

Supranationalism in the European Union has its origins from diverse perspectives, dating back to the end of World War II. There were different causes that influenced the idea of governance beyond the state. On one hand, it is the idea of a defeated nationalism, while on the other hand it is the idea that even if they win, they lose their colonial territories. At that moment, the level of states' internal or external implications was very low due to various reasons, including the memory of the past and also decline of the sovereignty concept in the Western Europe (Telo and Weyembergh, 2020).

As it can be seen, the supranational theory was established through several stages, but the so-called crystallization event was the adoption of The Schuman Declaration in 1950. The Minister of Foreign Affairs of France, Robert Schuman was the promoter of creating the "European Federation", a supranational entity. Along with this idea, he also proposed France and Germany as the engine of the European Coal and Steel Community. It represented a supranational body that aimed to integrate more states from the European Community, which was meant to be under the control of a High Authority. Jean Monnet, an important figure in the process of creating the nowadays European Union, came to the conclusion that it was necessary to have an economic common ground, similar to a huge market, where states could make economic trades (Zaharia and Pozneacova, 2020). Starting with 1950s, the process of integration has already begun and increased when it came to the numbers of policy areas covered. That was the point where the Member States have agreed on transferring power to a supranational level (exclusive competences) and also share the sovereignty in other areas (shared competences). All these new created competences had the role to boost the cooperation and interdependence between the Member States.

Starting with the Treaty of Rome and all throughout the years, European Union has grown drastically. In terms of legislation, a series of treaties were adopted, consolidated versions of the original that have the role of creating a better image and structure of the Union. The Brussels Treaty (also known as the Merger Treaty) entered into force in 1967 and changed the institutions' structure, creating only one Commission and one Council for all of the European Communities (EEC, ECSC, Euratom). Single European Act adopted in 1987 gave more influence on the European Parliament and also changes the system of voting in the Council. The so-called 'cross border' that changed the cooperation dynamics in EU was Maastricht Treaty, entered into force in 1993. It introduced the procedure of co-decision, in this way giving to the EP a substantial influence in decision-making. In 1999, the Amsterdam Treaty entered into force, which brought with it more transparency regarding the process of decision-making. The Treaty of Nice followed in 2003, which reformed the structure of the institutions, as the Commission composition and the Council system of voting (European Union, n.d.-a.).

Furthermore, the latest treaty that European Union adopted is the Treaty of Lisbon, 2009, which also brings dramatic changes in the institutional structures. For example, two institutional bodies, European Council and European Central Bank were brought to the stage of formal institutions, becoming directly linked to the stipulations of the treaties. At the same time, the Lisbon Treaty established two news posts, one for the President of the European Council and one for the High Representative of the Union for Foreign Affairs and Security Policy. The reason why these two posts were necessary is related to a European need of coherence in terms of institutional structures. Regarding the European Commission, the treaty stated that the in-

stitution needs to reduce its number of commissioners. This change was firstly mentioned in the Treaty of Nice, being stated that when the EU would reach the number of 27 MS, then the number of the commissioners should be reduced. This rule brought a lot of tension and disapproval especially from the Irish government. This occurred because reducing the number of the commissioners would be transposed in less international power for the Irish government at EU level (Laurent and Patrick, 2009).

Even though the number of the commissioners did not change, the EU representatives came to the conclusion that there is a necessity to increase the level of democratic legitimacy and transparency within the institutions of the Union. The Treaty of Lisbon also extended the Ordinary Legislative Procedure (the former co-decision) in order to sustain this need of democratic legitimacy (Peach, 2011).

Furthermore, people are starting to decrease their confidence toward the European Union system (Euractiv, 2010). Treaty of Lisbon produced a politicized and democratic Union, rather than an effective and stable function in decision-making, only by strengthening the EP power and the national parliaments influence in the process of decision-making.

### **3. Supranational elements of the European Union**

The academic sphere is divided into several approaches regarding the potential integration theory when it comes to the European Union system, but there are two of them that are also stated on the official sites of the Union: supranationalism and intergovernmentalism. Even though there can be applied more than two theories, the European Union can be considered an entity with mainly supranational features.

First of all, when it comes to a supranational entity, it is clearly stated from its theoretical framework that the entity itself is beyond the elements that are composing it. So, the decision makers, political leaders from the supranational entity, should comply with the organization as their primary affiliation (University of Groningen, 2013). Also, this represents one of the multiple supranational features that can be applied to the European Union, especially the European Commission. The President of the European Commission and also the other 27 commissioners are the perfect example due to the fact that the entire work corresponds to the European Commission. All the plans, reports and meetings that they conduct, are related to the well-being of the EU as a whole. Considering the supranational structure of the EU, the role of the European Commission is to promote EU's interests at international level.

In addition to this supranational matter of responding, the treaties represent the legislative norms that must be followed at EU level. Considering the fact that none of the treaties adopted by the European Union defined a determined territory of the EU, policies that are adopted at the EU Commission level underpin a vision orientated towards a non-national approach.

Also, on the international political scene, the European Union acts like a true supranational organism, being at the same time independent from the Member States and open to cooperation with third parties. Moreover, the European Commission as a promoter of EU's interests, is the entity that has the capability to interact with other supranational organizations. As an example, giving the international events, EU started implementing sanctions as a hard-power tool, even though there are shared views regarding the effectiveness of this method to the targeted states. So, EU as a supranational entity applied sanctions, like embargoes to those states that are involved in military confrontations. Moreover, most of the time, along with the em-



bargoes, the EU, had the possibility to impose asset freezes and even visa bans on the governments that were responsible with the violations of human rights. Iran, Russian Federation or Syria, are example of states in which EU established robust sanctions regimes (Lehne and Siccardi, 2020).

Among the main characteristics of supranationalism that can be found throughout the European Union there is to be mentioned the Treaty of Rome (EEC), signed in 1957. As it was stated in the treaty, the main ideas that were to be implemented, referred to the creation of common policies among states that signed it. The supranational feature of this treaty refers to the fact that only the EU has the capability to legislate, adopt, or even empower a member state in some specific domains. The specific areas in which the European Union has complete power are named exclusive competences and they refer to (European Union, 2016a):

- a) *“Customs union;*
- b) *the establishing of the competition rules necessary for the functioning of the internal market;*
- c) *monetary policy for the Member States whose currency is the euro;*
- d) *the conservation of marine biological resources under the common fisheries policy; common commercial policy”*

Along with the ratification of the treaty, new institutions were created, which had the role to ensure the completeness and correctness implementation of the treaty. Among them, the European Commission appeared as the promoter of EU's general interests. The supranational line that can be drawn regarding the European Commission is linked to its structure. Even though it consists of commissioners coming from every Member State, the role of the institution is to propose new laws on behalf of the EU interest overall. So, on a hypothetical note, even if a few Member States find a legislature proposal inefficient for their states, it does not mean that the proposal would not be implemented, because EU's interest is considered to be above all others (European Union, n.d.-b). Furthermore, the European Commission has another important role that emphasizes its supranational manifestations. The infringement procedure can be considered a supranational mechanism that gives the European Commission the absolute power to start investigating and apply financial penalties over the Member States that do not comply with the instructed rules. Every Member State is obliged to obey the EU laws, so if they do not act in accordance, the Commission has the obligation to start an investigation and apply specific sanctions (European Commission, n.d.-a.).

Apart from the institutional supranational character that was mentioned before, the EU's legislative structure contains a procedure called Ordinary Legislative Procedure, classified as supranational even by the European Parliament Fact Sheets. Along with the Ordinary Legislative Procedure, the EU classifies as supranational the quasi-constitutional procedures in which the proposal comes from the Commission, while the Parliament (implicit the Member States) has only a consultative role. Moreover, in this range of supranational procedures, there are also the budgetary and appointment ones, that completes EU's supranational character (European Parliament, 2021).

In addition to this, the European Union, in terms of its competences, has several agencies, which tend to adopt a supranational attitude. For example, EMA (European Medicines Agency) is the supranational entity that has to deal with evaluating and supervising the medicinal industry. Its role is to smooth out the work of national medicinal agencies from Member States

regarding different actions like approving a new medicine for the entire Union or even disapproving others (European Medicines Agency, n.d.).

As it was shown by the supranational characteristics previously mentioned, the European Union has most of its structure based on a supranational mentality. The areas in which this supranational theory has its mark are various. Starting from the medicinal sector to the economic area or even the digital one will have their own entities that will have to face a lot of challenges regarding nowadays conflictual dynamics.

#### **4. Digital sovereignty: a supranational objective for the European Union**

Nowadays, the European Union aims to keep up with any unpredictable events by focusing on two pillars: digitalization and climate change. These challenges are tackled differently, due to EU's capabilities regarding them. While climate change is a global phenomenon that needs to be addressed on a large scale, digitalization represents an objective of the European Union that strives to become a worldwide player in this area. In order to achieve this, EU representatives developed a Digital Agenda for future digital transformations.

Beside from being a plan for digitalization, EU's Digital Agenda also represents a key aspect in the European strategic autonomy. This does not mean that everything has to be produced within the borders of the European Union. In contrary, a strategic autonomy can sustain the transformation of EU in an international entity that can be independent and confident enough to have a greater contribution on the global stage (European Council, 2021).

The EU's Digital Agenda needs to be underpinned by many concepts in order to achieve its goals. In regard to this matter, digital sovereignty has a pivotal role in the future "Digital Europe", as it represents a necessity for the European community. Digital sovereignty can be defined as the capacity of an entity to have full control over its own digital means (data consumed, hardware and software products), without depending on third parties. In other words, the European Union aims to become autonomous in the digital sector by becoming an important player on the international stage.

Digital sovereignty has been approached by European entities for several years, as a necessity at the community level. In order to ensure evolution and excellence in this area, several policies were developed any many more would come in the following years. The main areas approached throughout a digital sovereignty perspective are (Huw 2021):

- Data governance – in order to ensure that citizens and private entities have a better control over their data, its governance represents a necessity not only for maximizing benefits generated by them, but also for guaranteeing infringements when individual privacy rights are violated. First step took by EU in this area dates back to 2016, when the *General Data Protection Regulation* – GDPR (European Union 2016b) was adopted. Since then, EU developed the *Single Digital Gateway Regulation* (European Union 2018), the *Open Data Directive* (European Union, 2019) and the *European Data Strategy* (European Commission, 2020e).
- Constraining platform power – increasing EU control over non-European companies (especially the ones that provide "platform" services) represents a priority area for ensuring EU's digital sovereignty. In regard to this matter, EU adopted in 2020 the *Digi-*

*tal Services Act* – DSA (European Commission, 2020d) and the *Digital Markets Act* – DMA (European Commission, 2020c) with the main objective of assuring that European rules and values are respected by any entity that invests, operates or bids in the EU.

- Digital infrastructure – reducing EU’s reliance on foreign entities by developing European digital infrastructure represents another key element of UE’s digital sovereignty. At the same time, developing this area facilitates EU citizen to access new digital opportunities. The European Commission, in cooperation with other Member States came up with *Gaia-X* project (Gaia-X, n.d.), that aims to cut EU’s dependency on cloud infrastructure developed by non-EU entities. Moreover, the *Connecting Europe Facility* – CEF (European Commission, n.d.-e.) includes an objective of developing digital projects on infrastructures.
- Emerging technologies – the future relies on new technologies that have the capacity of changing citizens’ daily activities, making the public systems more efficient or businesses more productive. Ensuring a constant development in this area impacts directly the sustainability of EU’s digital sovereignty in the future. In this matter, EU launched specific initiatives like the *European Alliance on Processors and Semiconductor Technologies* (European Commission, 2021b) and the *Electronic Components and Systems for European Leadership* – ECSEL (European Commission, 2021c) to encourage research and increase investments in this area. An important component of this area is Artificial Intelligence (AI), as EU aims to become a global leader in this field and developed a specific strategy to achieve this goal – *EU’s AI strategy* (European Commission, 2018).
- Cybersecurity – technology development and well-functioning cannot be ensured without security measures implemented by both producers and consumers in order to prevent the risks coming from the cyber space. This field strengthens EU’s digital sovereignty, as the supranational entity aims to set security standards in the cyber space. This is the reason why EU developed policies to increase Union’s resilience: *Network and Information Security Directives* – NIS 1 and NIS 2 (European Commission, n.d.-f.), *Cybersecurity Act* (European Commission, n.d.-c). In addition to this, two cybersecurity strategies were adopted at EU level, the most recent one in 2020, called *EU’s Cybersecurity Strategy for the Digital Decade* (European Commission, 2020f).

The current international situation makes digital sovereignty a necessity for the European Union. More exactly, 92% of data used in the western countries is hosted in the United States of America, which can be seen as a possible vulnerability for European citizens and businesses. In the same time, the European private sector has a significant deficit in comparison with its competitors at international level. In 2021, European companies that activate in the technology area could not be part of the first 20 tech companies around the world, because they were overreached by American and Asian companies (Huw, 2021). Even European representatives from the most digitalized countries in the European Union (Estonia, Germany, Denmark and Finland) underlined EU’s necessity of becoming digitally sovereign (Fleming, 2021).

Digital sovereignty can be considered a solid argument in defining EU’s supranational character, due to the fact that it represents the ability of the EU, as a supranational entity, to be digital autonomous and resilient. Once this objective is achieved, Member States can benefit



by gaining access to digital services and new technologies faster and cheaper. Moreover, some of the Member States representatives decided to step up and call the importance of EU's digital sovereignty, action that can be seen as an acceptance of the Member States towards a strong digital EU that is capable of representing their interests in international agreements. At the same time, EU's supranational character is sustained by the fact that it represents an entity that can get involved in international relations as an independent actor. Taking into account these arguments, digital sovereignty can be considered a supranational objective for the European Union.

## **5. Future perspectives of a digital European Union**

The international scene has dramatically changed over the years in every domain, from the political one to the economic and social. The dynamics of today's events is in a constant change since the digital era started to develop. Along the years, actors had to face a series of challenges that modified the ordinary structure of the systems. Digitalization became one of the main challenges that nowadays organisms need to encounter.

What is already accepted by most of the people is the fact that the digital domain is in a transformation process. The ambiguous part of this process refers not only to the capacity of the political and economic areas to face the unknown, but also how this transformation will take place and under what consequences. Also, there are a series of question that need to be addressed. For example: How the digital innovations will be managed? By whom? How will the states react to more and more challenges? Some of these questions have their obvious answer, but most of them are still in shadow.

The digital sphere, or maybe the digital transformation process can be considered provocative due to its uncertainties, but in order to understand it and change it into an advantage, there is a necessity to have a robust and flexible strategies. The key factor of this entire digital transformation is represented by the European Union, in cooperation with other important factors like public and private stakeholders. Encouraged by the Member States, the European Union has to face difficult times in terms of the rapid changing and adaptability of the digital field.

Furthermore, there is a stringent need to develop policies and strategies in order to have a reaction towards the dynamical evolution of areas like technology, economy, environmental, military and so on. The capacity of predicting the future trends and, at the same time, having the full spectre of the situation, represents an advantage that will help in creating adaptable strategies and policies into the future (Deloitte, 2019).

The current international context consists of many uncertainty, risks and also many opportunities. The European Union has to face delicate problems regarding the balance between uncertainties and opportunities. Considering the rapid changes that are taking places in nowadays societies and also the evolution of the digital world, it is extremely important for EU to take advantage of this digital transformation. By doing so, the new EU policies will act like guidelines for the lives of the citizens. Moreover, the initial and principal ideas in terms of the creation of EU have to live in a safe, healthy and free environment, but due to the digital transformation that is happening now, there are constant changes occurring. Taking into consideration the race in the process of implementing Artificial Intelligence as part of human lives, the everyday life will completely change resulting in a shifting percentage of the working and active people (GeSI, 2015).

It became very clear that digitalization affects every area of the world and implicit it will affect the European Union and its status against other international actors. In addition to this, representatives of the EU private sector conducted different studies on the matter of possible future digital scenarios. According to their research, the prerequisites of a strong digitalized EU are developing the concept of Internet of Everything, omnipresent future networks and re-making institutions. By creating and implementing these capabilities, European Union will be able to prosper and develop as a stronger actor on the international political scene (Accenture strategy, 2017).

In the first place, developing a concept like Internet of Everything comes with precious advantages regarding the value of EU. This concept consists of an enormous accessibility of data from various interoperable sources that are transmitted in a secured way. Also, taking into consideration having a digital and secured identity that allow exchanging data and store it in a safe marketplace, can strengthen the cooperation and cohesion between both individual users and supranational entities (Accenture strategy, 2017).

Moreover, with this continuously enhanced cooperation on the communication networks, the need of a pervasive and reliable communication system networks will grow. Connectivity is the key when it comes to creating such a network that can encapsulate various areas, from renewable energy to autonomous vehicles. Also, by creating these omnipresent networks, the chance of having real-time analytics of data will systematically grow (Accenture strategy, 2017).

Digitalization represents one of the biggest challenges that needs to be confronted and it is very important to have institutions that have the capabilities to respond in a firm and active mode to this transformation. According to some private representatives, there is a need in terms of readjusting the nowadays institutions in order to be able to establish elements like digital identification, transparent usage of personal data, transaction security and overall control (Accenture strategy, 2017).

As it was mentioned before, there is a stringent need of urgent policy action so that the European Union will have the chance to stand out in this digital transformation process. At the same time, there is also a need of supporting elements of the actual structure of the Union. For instance, by supporting the digital leadership, EU can grow the cooperation in the digital system and even achieve a Digital Single Market in order to encourage all the actors, including public and private stakeholders to take action. Furthermore, a key element of the entire process of digitalization and transformation refers to multiplying the European investment capabilities, by promoting competition fairness among the digital chain and also by having a long-term plan to upgrade the infrastructure (Accenture strategy, 2017).

## **6. Case Study:**

### **The European Cybersecurity Competence Centre**

When it comes to the research method chosen for this paper, case study is the most suitable due to the fact that it allows an in-depth analysis over a specific institution in order to prove the assumption of this article. The comprehensive character of this method is determined by the institution's details provided, like its role on the international stage, the context of its development as well as the reason why it is eloquent for this paper. All these aspects are presented in a logical and chronological way, in order to facilitate a better understanding of the as-

sumption. At the same time, using a case study provides a proper context to focus on a single point of interest.

The main focus of the following case study is The European Cybersecurity Competence Centre (also known as The European Cybersecurity Industrial, Technology and Research Competence Centre or ECCCC), emphasizing its role in the European Union ecosystem, as well as the reason why it represents a solid argument for the EU's supranational character.

### **6.1. ECCCC: key aspects and its role in the European ecosystem**

ECCC stands for The European Cybersecurity Industrial, Technology and Research Competence Centre and it represents a new framework for the European Union to develop industrial and innovation policies in the cybersecurity area. The focus of this Centre is to create an ecosystem where Member States can cooperate with the private entities and the academic sector in order to develop and implement technologies and digital policies that can ensure the EU's cybersecurity, especially at small and medium enterprises level (SMEs). In this way, the European Union aims to create a strong shield against threats that can be projected from the cyber space and can interfere in its process of achieving its objectives. At the same time, ECCCC will cooperate with the Network of National Coordination Centres (NCCs) in order to ensure a higher level of cybersecurity at Member State's level (European Commission, n.d.-d.). NCCs represents a mechanism for the European Union to increase the cooperation between Member States' stakeholders in the field of cybersecurity with the main objective of ensuring EU's digital sovereignty.

Taking into account the accelerated pace of technology development, EU developed several policies and strategies over the last years in order to integrate it into European citizens lives. Moreover, one of EU's main goals is to be a role model for the digital economy, at the international level. In regard to this matter, the European Commission developed a plan called *A Europe fit for the digital age*, which aims to strength EU's digital sovereignty, focusing on three key aspects: technology, data and infrastructure. The plan developed by the European Commission includes two strategies that have the role to enhance a constant evolution in the EU's digitalization process (European Commission, n.d.-b.):

- Shaping Europe's digital future. The main objective of this strategy is to facilitate the digital transformation to all actors in the European Union (citizens, businesses and public institutions), through three main pillars: technology that works for people, a fair and competitive digital economy and an open, democratic and sustainable society. This strategy aims not only to improve citizens' daily lives through technology, but it also aims to improve the environment by reaching climate neutrality through digital means (European Commission 2020b).
- Europe's Digital Decade. The European Commission developed this strategy in order to have a comprehensive view of what digitalization in the European Union has to look like in 2030. More exactly, within this document, a metaphorical compass is used to describe the coordinates of EU's digital transformation: improving citizens' digital skills, assuring a secure and sustainable digital infrastructure, improving digital integration into businesses and raise the digitalization level of public services (European Commission, 2021a).

A key component of the EU's process of digitalization is represented by cybersecurity. The main reason why this element constitutes such an important aspect is the need of secured ICT infrastructures, technologies and data managed within them.

Digitalization is a complex procedure that needs a solid foundation to be fully operational. In regard to this matter, ICT infrastructures has to be as secured as possible, due to the fact that they can represent a potential target of cyber attackers. EU conducts constant efforts to ensure a higher level of cybersecurity not only at the level of its ICT infrastructures, but also at Member States level. This is the reason why EU developed the two NIS Directives, which are compulsory laws for every Member State. The first one addresses national cybersecurity capabilities of the Member States through their own CSIRT (Computer Security Incident Response Team) institutions, cross-border collaboration between EU countries and National supervision of critical infrastructure (European Parliament and Council of the European Union, 2016a). In addition to this, the second NIS Directive was developed, focusing on the security of supply chains, streamline reporting obligations and new security requirements (Del Mar and Negreiro, 2021).

An important step towards the security of hardware and software products used at EU level has to be made by implementing the *security-by-design* concept (used to describe the integration of security measures on each development phase of a product), as well as setting specific security standards for technologies in order to be eligible. The European Parliament took measures in this regard by adopting The EU Cybersecurity Act in 2019. Its role is to set up a legal framework for The European Union Agency for Cybersecurity (ENISA) to create specific certification schemes that has to be respected in order to make a hardware or software product valid form a cybersecurity point of view (European Commission n.d.-c.).

The EU's digital transformation requires a strong security of data that is managed among European entities. In order to state that data is secured, it needs to fulfil three main characteristics: confidentiality, integrity and availability. This concept is known in the cybersecurity areal as the CIA triad, representing a model that guides development of policies for data security.

Nowadays, EU's cybersecurity is ensured by 22 actors (Fig. 1), which have different roles, but the same goal: making the European Union cyber resilient. In order to achieve this goal, each of them has to fulfil its role, but most important to cooperate with the aim of having a comprehensive approach into this area.

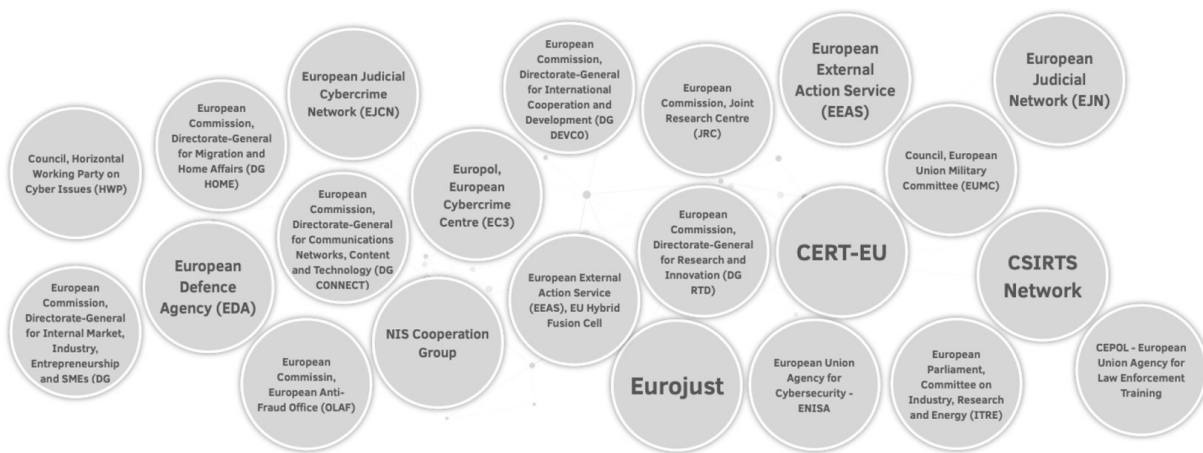


Figure 1. EU's entities in the cybersecurity field

The European Commission aims to develop a cyber-secured EU by implementing policies and strategies that can reduce the risks coming from the cyber space. In this matter, a new EU Cybersecurity Strategy was developed in December 2020, having a key role in *EU Security Union Strategy*, *Recovery Plan for Europe* and *Shaping Europe's Digital Future*. The strategy has 3 main objectives which have to be achieved in order to keep up with the digital development (European Commission, 2020a): “Trust and security at the heart of the EU Digital Decade”, “Cyber and physical resilience of network, information systems and critical entities” and “Securing the next generation of networks: 5G and beyond”. Among the actions that have to be taken for achieving these objectives, EU has to advance an open and global cyberspace by increasing cooperation between Member States. In this regard, the European Cybersecurity Industrial, Technology and Research Competence Centre aims to be a new actor in the EU’s cybersecurity landscape that encourages cooperation between states in order to develop a common agenda for research and technology development in this area.

Before the operationalization of ECCC, the European Union launched four pilot projects in 2019, that were meant to bring together private entities (both big companies and SMEs), cybersecurity research institutes and universities from 26 Member States in order to create a foundation for the new Competence Centre and the Network of National Coordination Centres (European Commission, 2019):

- **CONCORDIA**: represents a Cybersecurity Competence Network that provides high standards in research, technology development and services conducted to develop a comprehensive ecosystem for EU’s digital sovereignty.
- **ECHO**: it’s main focus is to ensure a secured European market by encouraging cooperation and development in this area. At the same time, it makes sure that European citizens are protected from threats coming from the cyber space.
- **SPARTA**: represents a community capable of identifying, projecting and developing technological solutions used to increase cybersecurity at EU level. It also involves a new way of approaching innovations, research programs and trainings in cybersecurity.

CyberSec4Europe: using the practice provided by previous initiatives, alongside the expertise provided by private partners, this project aims to project and develop governance structures that might be useful in a future European Cybersecurity Competence Network.

## **6.2. Supranational elements of the ECCC**

As it was previously presented in the theoretical framework, the European Union represents a supranational entity, due to its structure and its decision-making process. Over the years, it proved to be a real benefit for the Member States, as EU managed to improve cooperation, coherence and dialogue between them. Similarly, once it is operational, ECCC will act like a promoter of interoperability and cooperation between Member States in order to develop new technologies, cybersecurity policies and solutions for EU’s digital needs.

First of all, the European Cybersecurity Industrial, Technology and Research Competence Centre can be considered a supranational entity as its main role is to coordinate the Network of National Coordination Centres. In other words, it will gather expertise and resources in the cybersecurity field from each Member State in order to develop new ways of enhancing security at a supranational level.



Secondly, EU Regulation 2021/887, which represents the legal foundation of the ECCC sustains its supranational character even from the context of the current normative act. Thus, taking into account the quick evolution of cybersecurity and the evolution of cyber threats, EU's officials consider that ECCC must facilitate and coordinate projects that aim to consolidate Union's resilience (European Parliament and Council of the European Union, 2021). This aspect underlines the importance of the Centre for EU as a supranational entity.

Thirdly, projects related to cyber capabilities or ICT infrastructure at EU level, that are developed and coordinated by ECCC have to meet specific conditions imposed by EU. Even if it is only a particular phase of the project, the entities involved have to obey European regulations and standards. In this way, ECCC becomes not only a coordination entity for technology development, but also a guarantor of the supranational standards in term of cybersecurity at EU level.

Apart from its own supranational elements, ECCC support EU's supranational character, throughout its mission. The activities conducted under ECCC coordination sustain EU's supranational features in terms of (European Parliament and Council of the European Union 2021):

Strengthening strategic autonomy and EU's authority character in the field of cybersecurity, throughout retention and development of research, industrial and technological cybersecurity capabilities. These actions represent a necessity in order to ensure a high level of trust and security in the Digital Single Market.

Supporting EU's technological resources, capabilities and skills in terms of ICT infrastructure resilience and dependability. This aspect includes hardware and software components used in EU and critical infrastructure.

Increasing EU's cybersecurity industry's worldwide competitiveness, enforcing cybersecurity standards and measures across the Union and make cybersecurity an advantage when it comes to competitiveness for other EU industries.

## **7. Conclusions**

As it was stated in the beginning of this paper, its purpose was to prove EU's supranational characteristics throughout the lens of the European Cybersecurity Industrial, Technology and Research Competence Centre. In this matter, it was demonstrated that EU is aiming to achieve its objectives towards digitalization through supranational means, as it was the establishment of ECCC.

Even if the Treaty of Lisbon made the European Union more focused on its intergovernmentalism perspective, global challenges and societal evolution underpinned EU's supranational elements. Technology development also played an important role in EU's evolution as a supranational actor, due to the fact that it forced the Union to pay more attention on digital development as an independent actor in the international relations. Moreover, the gap between European tech companies and their competitors from the United States of America or Asia emphasized the need of urgent actions on behalf of EU towards a strategy focused on digital matters. Nevertheless, EU dependency on infrastructure provided by non-European third parties might represent a vulnerability for the Union in future negotiations. This fact proved once again that EU must take actions as a supranational entity in order to ensure its digital sovereignty.

As cybersecurity represents a necessity for the digitalization process, EU projected its supranational character into this area as well. The two strategies developed at supranational level proved that the cybersecurity of some Member States alone cannot assure the resilience of the entire Union. In this way, EU developed the NIS Directives in order to impose new cybersecurity measures that had to be taken by every member. At the same time, EU established new security standards that needed to be respected by entities that developed hardware and software products used within the Union.

The development of the European Cybersecurity Competence Centre was another step made by EU in order to strength one of its supranational features, digital sovereignty. As ECCC has the role of sustaining technology development within the European Union by gathering Member States resources and using them in order to ensure a higher level of cyber security at supranational level, it can be stated that EU projects its supranational character throughout ECCC. This statement is also sustained by Centre's mission, which focuses on strengthening strategic autonomy and EU's authority character in the field of cybersecurity, supporting EU's digital capabilities and increasing the competitiveness of EU's cyber security industry worldwide.

Taking everything into consideration, EU's supranational character remains a strong part of its mechanisms, due to the fact that even new challenges – as digitalization and cybersecurity – are addressed throughout supranational means, like the creation of the European Cybersecurity Industrial, Technology and Research Competence Centre.

## Conflicts of interest

The authors declare no conflict of interest.

## About the authors

Sebastian SUCIU – Master graduate of the Security & Technology Master Programme, Department of International Relations and European Integration from the National University of Political Studies and Public Administration

Andreea-Larisa CÎRJAN – Master graduate of the International Relations and European Integration Master Programme, Department of International Relations and European Integration from the National University of Political Studies and Public Administration

## References

- Accenture strategy (2017) *Lead or lose. A vision for Europe's Digital Future*. Available at: <https://etno.eu/library/reports/6-lead-or-lose-a-vision-for-europe-s-digital-future.html>. [Accessed 11 November 2022].
- Arcas, R. L. (2007) Theories of Supranationalism in the EU. *The Journal of Law in Society*, 8(1), pp. 8995.
- Del Mar, M. and Negreiro, A. (2021) *The NIS2 Directive: A high common level of cybersecurity in the EU*. Available at: [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS\\_BRI\(2021\)689333](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2021)689333). [Accessed 13 November 2022].
- Deloitte (2019). *Digital Transformation in the EU 2035. A Glimpse into the Future*. Available at: <https://www2.deloitte.com/content/dam/Deloitte/de/Documents/strategy/deloitte-future-of-digital-transformation-eu-2035.pdf>. [Accessed 11 November 2022].

- Euractiv (2010) *Europeans losing faith in EU*, August 27. Available at: <https://www.euractiv.com/section/public-affairs/news/europeans-losing-faith-in-eu/>. [Accessed 11 November 2022].
- European Commission (2019) *Four EU pilot projects launched to prepare the European Cybersecurity Competence Network*. Available at: <https://digital-strategy.ec.europa.eu/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network>. [Accessed 13 November 2022].
- European Commission (2020a) *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*. Available at: [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_20\\_2391](https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391). [Accessed 13 November 2022].
- European Commission (2020b) *Shaping Europe's Digital Future*. Available at: [https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020\\_en\\_4.pdf](https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf). [Accessed 13 November 2022].
- European Commission (2020c) *Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)*. COM/2020/842 final. Available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN>. [Accessed on: 11 November 2022].
- European Commission (2020d) *Proposal for a REGULATION of the EUROPEAN PARLIAMENT and of the COUNCIL on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC*. COM/2020/825 final Available at: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=COM:2020:825:FIN>. [Accessed on: 10 November 2022].
- European Commission (2020e) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data*. COM/2020/66 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>. [Accessed on: 13 November 2022].
- European Commission (2020f) *The EU's Cybersecurity Strategy for the Digital Decade*. Available at: <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>. [Accessed on: 9 November 2022].
- European Commission (2021a) *Europe's Digital Decade: digital targets for 2030*. Available at: [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en). [Accessed 13 November 2022].
- European Commission (2021b) *Alliance on Processors and Semiconductors technologies*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/alliance-processors-and-semiconductor-technologies>. [Accessed on: 13 November 2022].
- European Commission (2021c) *Electronic Components and Systems for European Leadership (ECSEL) Joint Undertaking Publication of a vacancy for the function of Executive Director (Temporary Agent – Grade AD 14)*. COM/2021/20067. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:C2021/365A/01&from=ES>. [Accessed on: 11 November 2022].
- European Commission (n.d.-a.) *Infringement procedure*. Available at: [https://ec.europa.eu/info/law/law-making-process/applying-eu-law/infringement-procedure\\_en](https://ec.europa.eu/info/law/law-making-process/applying-eu-law/infringement-procedure_en). [Accessed 12 November 2022].
- European Commission (n.d.-b.) *A Europe fit for the digital age*. Available at: [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en). [Accessed 13 November 2022].
- European Commission (n.d.-c.) *The EU Cybersecurity Act*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>. [Accessed 13 November 2022].
- European Commission (n.d.-d.) *Cybersecurity Competence Centre and Network*. Available at: [https://cybersecurity-centre.europa.eu/index\\_en](https://cybersecurity-centre.europa.eu/index_en). [Accessed 13 November 2022].
- European Commission (n.d.-e) *Connecting Europe Facility*. Available at: <https://ec.europa.eu/inea/en/connecting-europe-facility>. [Accessed on: 12 November 2022].
- European Commission (n.d.-f.) *NIS Directive*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/nis-directive>. [Accessed on: 10 November 2022].
- European Commission. (2018) *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and The Committee of the Regions. Artificial Intelligence for Europe*. COM(2018) 237 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN>. [Accessed on: 12 November 2022].

- European Council (2021) *Digital sovereignty is central to European strategic autonomy* – Speech by President Charles Michel at „Masters of digital 2021“ online event. Available at: <https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/>. [Accessed 11 November 2022].
- European Medicines Agency (n.d.) *EU partners*. Available at: <https://www.ema.europa.eu/en/partners-networks/eu-partners>. [Accessed 12 November 2022].
- European Parliament (2021) *Supranational Decision-Making Procedures*. Available at: [https://www.europarl.europa.eu/ftu/pdf/en/FTU\\_1.2.3.pdf](https://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.3.pdf). [Accessed 12 November 2022].
- European Parliament and Council of the European Union (2016) *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*. Available at: <https://eur-lex.europa.eu/eli/dir/2016/1148/oj?locale=en>. [Accessed 13 November 2022].
- European Parliament and Council of the European Union (2021) *Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*. Available at: <https://eur-lex.europa.eu/eli/reg/2021/887/oj>. [Accessed 13 November 2022].
- European Union (2016a) *Consolidated text: Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union*. s.l.:EUR-Lex.
- European Union (2016b) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. OJ L 119, 4.5.2016. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> [Accessed on: 15 November 2022].
- European Union (2018) *Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012*. OJ L 295, 21.11.2018. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2018.295.01.0001.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0001.01.ENG) [Accessed on 14 November 2022].
- European Union (2019) *Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast)*. OJ L 172, 26.6.2019. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024>. [Accessed on: 14 November 2022].
- European Union (n.d.-a.) *EU treaties*. Available at: [https://europa.eu/european-union/law/treaties\\_en](https://europa.eu/european-union/law/treaties_en). [Accessed 11 November 2022].
- European Union (n.d.-b.) *European Commission*. Available at: [https://europa.eu/european-union/about-eu/institutions-bodies/european-commission\\_en](https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en). [Accessed 12 November 2022].
- Fleming (S., 2021) *What is digital sovereignty and why is Europe so interested in it?* Available at: <https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/>. [Accessed 11 November 2022].
- Gaia-X (n.d.) *About Gaia-X*. Available at: <https://gaia-x.eu/what-is-gaia-x/about-gaia-x/>. [Accessed on: 8 November 2022].
- GeSI (2015) *#SMARTer2030 ICT Solutions for 21st Century Challenges*. Available at: [http://smarter2030.gesi.org/downloads/Full\\_report.pdf](http://smarter2030.gesi.org/downloads/Full_report.pdf). [Accessed 11 November 2022].
- Huw, R. (2021) Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet Policy Review*, 10(3).
- Laurent, P. and Patrick, G. B. (2009) Fixing a hole where the rain gets in: The Lisbon Treaty and the Irish „Legal Guarantees“. *Irish Journal of European Law*, 16(5).
- Lehne, S. and Siccardi, F. (2020) *Where in the World Is the EU Now?* April 29 Available at: <https://carnegieeu-rope.eu/2020/04/29/where-in-world-is-eu-now-pub-81658>. [Accessed 13 November 2022].
- Peach, L. (2011) *The institutional Development of the EU post- Lisbon: A case of plus ça change...?* UCD Dublin European Institute Working Paper, December. Volume 11-5.

- 
- Telo, M. and Weyembergh, A. (2020) *Supranational Governance at Stake: The EU's External Competences caught between Complexity and Fragmentation*. s.l.:Routledge.
- University of Groningen (2013) *Future Learn*. Available at: <https://www.futurelearn.com/info/courses/european-culture/0/steps/23521>. [Accessed 12 November 2022].
- Zaharia, V. and Pozneacova, V. (2020) Supranationalism vs. Intergovernmentalism in the Actual Organization of EU. *Logos University Mentality Education Novelty: Political Science and European Studies*, 6(2), pp. 47-61.