Border Crossing
November 2025
Volume: 15, No: 4, pp. 69 - 93
ISSN: 2046-4436 (Print) | ISSN: 2046-4444 (Online)
bordercrossing.uk

TRANSNATIONAL PRESS® LONDON

Received: 1 October 2025 Accepted: 9 November 2025
DOI: https://doi.org/10.33182/bc.v15i4.2941

European Union's Cyber Security Policies in the Context of A Developing and Changing Security Perception

Fatma Betül Korkmaz[1]

Abstract

Despite being a relatively recent development, cyberspace has become an integral part of human lives due to rapid technological advancements. It functions as a fifth dimension in addition to the four traditional domains where states exercise sovereign powers: land, air, sea, and space. Unlike these physical spaces, cyberspace lacks physical and geographical boundaries, displaying a dynamic and continuously evolving nature. This fundamental characteristic complicates the definition of sovereignty in cyberspace, posing unique challenges to the traditional concept of sovereignty. Another important point to consider is that cyber operations can be conducted anonymously, often without cost or risk to the perpetrators. This anonymity creates legal challenges because it prevents the attribution of these operations to a specific person, organization, or government. The cyber security strategies and policies developed by the EU both internally and in cooperation with other international organizations are important in overcoming the aforementioned legal difficulties. The main purpose of this study is to analyse in detail the EU's cybersecurity policies within the scope of the identified problems related to the new security perceptions that have emerged due to the latest technological developments.

Keywords: *European Union, cyberspace, cybersecurity, cybernetic, cybersecurity agreements, cyberattack*

Introduction

The 21st century world forces even international relations to keep up with the pace and requirements of technological developments. Increasing digitalization has not only affected the daily lives of individuals but also required international relations and international law subjects to adapt to the innovations brought about by the digitalizing modern age. Moreover, the rapid evolution of technology has dramatically changed the ways in which states interact, negotiate, and resolve conflicts, demanding a more agile and proactive approach to international governance.

National and international security perceptions have also been influenced and transformed by this change, leading to a shift in the classical understanding of sovereignty. In this context, the scope of traditional security understanding has expanded. Cyberspace, which has emerged as an additional domain to land, air, sea, and space where states exercise their sovereign powers, has become a subject of international law discussions on how these powers should be exercised. The lack of physical and geographical boundaries and the constantly evolving dynamic nature of cyberspace, which is added as a fifth domain to these four classical domains, make it controversial for states to exercise their sovereign powers in cyberspace in

[1] PhD Candidate, Department of Public Law, Marmara University, Institute of Social Sciences, Istanbul. Guest Researcher, University of Hamburg, Germany. E-mail: fatmabetul20@marun.edu.tr , https://orcid.org/0000-0001-7194-7099

the same way as in other domains. This shift necessitates not only new legal frameworks but also the continuous adaptation of existing laws to the unique challenges posed by cyberspace.

The emergence of cyberspace as a fifth domain where equal sovereign states exercise their sovereign powers has brought along many national and international security issues. The harmful activities conducted in cyberspace, emerging as another aspect of the changing security perception, combined with the difficulty of identifying those who perform these actions, have created the need for legal regulations in the field of cybersecurity. The anonymity, which means the challenge of attributing the attacks to specific actors, complicates the attribution of these activities to certain actors, creating legal challenges and hindering accountability in a legal sense. Furthermore, the cross-border nature of cyberspace has led to jurisdictional conflicts, where the actions taken in one country can have profound effects on another, complicating legal recourse and enforcement. In response to this situation, the European Union continues to be an effective subject in establishing international legal rules applicable in cyberspace with comprehensive cybersecurity strategies and policies implemented both through the domestic policies developed by its member states and in collaboration with other international organizations to overcome these challenges and enhance cyber resilience.

This study aims to analyse the EU's cybersecurity policies in detail, focusing on the contemporary security perceptions caused by digitalization. The definition and scope of cybersecurity, the role of the EU in developing cybersecurity policies, the effectiveness of these strategies, the relationship between the EU and NATO in cybersecurity, and the issues of sovereignty and responsibility in the context of cyber activities constitute the general scope of the study. Additionally, the study will explore the EU's role as a normative power in shaping global cybersecurity norms and its influence on other international actors and organizations.

In the second section, historical perspectives on the notion of security are provided to define it. The term cybersecurity is explained against the backdrop of security perception, establishing a link with the past. Subsequently, the concept of governance, intertwined with sovereignty, is examined, and the impact of cybersecurity governance activities on the process of forming binding international rules is addressed. This section also delves into the evolution of security governance in the digital age, highlighting how the need for collective action has transformed both national and international security strategies.

The third section pertains to the existing cybersecurity strategies and policies of the EU. The contribution of the EU in making the exercise of sovereign powers in cyberspace compatible with international law by demonstrating its normative power in the international arena is discussed within the framework of concrete legal regulations. The challenges and limitations faced by the EU in the process of forming cybersecurity strategies and developing policies are also presented in this context. The section further examines the role of the EU in fostering cooperation between member states and its efforts to harmonize cybersecurity standards across different jurisdictions, ensuring a unified and effective approach to emerging threats.

Section 4 examines the cybersecurity relationship between the EU and NATO, evaluating the strategies developed by both organizations to ensure security in the cyber domain within their historical contexts. The legal regulations and joint initiatives that emerged as a result of the development of these strategies are concrete outputs of the needed cooperation in the field of cybersecurity. The initiatives put forth by focusing more on the common points rather than

the differences of both organizations are accepted as successful examples of cooperation in the field of cybersecurity. The Ukraine-Russia war has once again highlighted the necessity for both states and international organizations to cooperate more in the field of cybersecurity. Moreover, this section will analyse how this cooperation can serve as a model for future alliances in addressing global cyber threats, illustrating the importance of interoperability and shared intelligence in countering sophisticated cyber operations. It is evident that any concrete step taken as a result of NATO and EU solidarity in the field of cybersecurity will help alleviate the global threat environment created by the war to some extent.

Section 5 generally addresses cybersecurity agreements and sovereignty issues. The challenges related to sovereignty encountered in cyberspace and how the EU overcomes these challenges within the framework of existing legal regulations are discussed. This section also explores the complex nature of sovereignty in the digital age, where traditional notions of territorial control are blurred, and the implications for state responsibility are profound. Furthermore, the section examines the legal implications of cyber sovereignty, including the right of states to regulate cyberspace within their borders, and the tension between national security and the free flow of information across borders. The section further considers how these dynamics influence international relations and the potential for conflict in cyberspace. The section also explores potential future developments in international law related to cyberspace sovereignty, such as the creation of new treaties or the adaptation of existing ones to better address the challenges posed by the digital age.

The final section examines the compensation mechanisms related to damages caused by wrongful acts of states. The conditions of attribution according to the rules of International Responsibility Law are addressed. The handling of damages resulting from cyber activities, the attribution of responsibility to state and non-state actors, and the EU's responsibility within the framework of international law are also evaluated under this heading. After examining the issue of attribution, the methods of compensation for the damage caused by the wrongful act attributed to the responsible state are explained. The section also investigates the EU's approach to the rules of responsibility law in the cyber domain and the challenges encountered in applying these rules. Additionally, the section will analyse case studies where state and non-state actors have been held accountable for cyber activities, providing insights into the practical application of these legal principles and the effectiveness of current mechanisms in achieving justice and deterring future violations.

As a New Security Perception: Cybersecurity

To understand the concept of cybersecurity, it is necessary first to define the notion of "cyber" and "security" individually. Given its broader scope, deep-rooted nature, and the modern perception evolved with globalization, it would be beneficial to define the latter first.

When we look at the lexical meaning of security, it is generally described as a condition of being safe from danger or threat (Oxford University Press, 2024). Security is considered an essential necessity for individuals, communities, and states, and the question of what constitutes security for these groups has been debated throughout history (Rogozińska, 2021:86). Thomas Hobbes focused on the requirement of a central authority to maintain order and prevent chaos, thereby imposing a stable society in his foremost work, Leviathan (1651). (Lloyd,1991: 363).

John Locke introduces another dimension of security by emphasizing individual rights to life, liberty, and property, along with the government's primary yet limited role in protecting these rights (Internet Encyclopedia of Philosoph, 2024). He asserted that the government`s responsibilities should be limited to safeguarding the lives, and property of its citizens. In a perfect anarchic state of nature, numerous problems would emerge, rendering life less secure than it would be with the protection of a minimal state. In the context of his profound philosophical insights on peace and republicanism, Imanuel Kant argued that the likelihood of achieving security among nations increases when democratic forms of government, which maintain the division of governmental functions and adherence to the rule of law, are in place (Fidler, 2022: 15).

As understood from the divergent views put forward, it is not possible to make a fixed definition of the notion of security, as ideas of human, national, and international security emerge from such diverse perspectives. Security, in its narrow definition, is the absence of any threat and ensuring the continuity of the subject's survival, while in its broad definition, it is about ensuring the integrity and freedom for the entity's development (Rogozińska, 2021: 88). Therefore, the process of defining the concept of security is dynamic and influenced by several factors such as changing environmental conditions, advancements in civilization, and the evolving needs of individual entities (Rogozińska, 2021: 88)

Following the Second World War, becoming the international system to bipolar, which is dominated by the USA and Soviet Union. This era marked by ideological rivalry, arms race and proxy wars. The collapse of the Soviet Union in 1991 led to a shift from a bipolar international system to a multipolar one. The transformation to a multipolar international order has also driven globalization and technological advancements, resulting in the decentralization of power. In this new order, power is shared among different actors, fostering both competition and coordination. This substantial alteration impacts global governance, diplomacy, and security, especially when major collaboration is needed to tackle transnational issues such as cyberattacks, transnational terrorism, and cross-border environmental hazards (Toje, 2010: 44). These examples can be labeled as instances of global insecurity, which are no longer perceived only as national issues in the 21st century, and have made it necessary to implement regulations in the field of cybersecurity (Geiss, 2021: 69). In this way, cybersecurity is a contemporary manifestation of the evolving traditional security concepts in this century and will be examined in more detail in the next section.

Definition of Cybersecurity

We have been acquainted with cybersecurity law, still in its early stages, for a little over two decades (Geiss, 2021: 661). Therefore, defining terms in this field is crucial for current and potential regulations. Furthermore, the ever-evolving nature of the cyber sphere constantly gives rise to new concepts, heightening the necessity for their identification. The term "cyber" comes from the abbreviation of "cybernetics" and refers to anything involving, using, or related to computers, particularly the internet (Rackevičienė, Mockienė, 2020) . When looking at the etymological origin of the term "cybernetics," it stems from the Greek word "kybernetes", meaning "steersman" or "governor." This term was first used by Norbert Wiener in 1948 to describe the study of control and communication in both animals and machines (Rackevičienė, Mockienė, 2020: 676)

As time goes by, the term "cyber" began to be considered independently of "cybernetics" in the context of evolving technology. With the advent of digitalization, various developments such as online book access, the proliferation of electronic messaging, and global internet access via satellites have transformed the internet into a versatile and widely participated technology (Fidler, 2022: 12). While the 1990s and 2000s were pivotal for the lexical evolution of the term,

they also saw an increase in activities such as cybercrime, cyberattacks and cyberterrorism conducted via the internet. Consequently, the term "cyber" has detached from its neutral context in e-formations, like e-mail, e-book, and e-currency, within the field of information technology and has acquired a negative connotation (Rackevičienė, Mockienė, 2020: 677).

Considering all the points mentioned, cybersecurity is the practice of protecting internet-connected systems, comprising hardware, software, and data, from cyberattacks. This parallels traditional security measures that protect physical assets and ensure the safety of individuals, properties, and entities (Ştefănescu; Papoi, 2020: 180). Just as traditional security aims to prevent unauthorized access and protect against threats, cybersecurity focuses on preventing unauthorized digital access and protecting data integrity, confidentiality, and availability.

Security in Cyberspace

The term "cyberspace" was first used by American author William Gibson in his 1984 novel "Neuromancer". In the novel, cyberspace is described as follows:

> *"Cyberspace: A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding…"* (Gourgey, Smith, 1996: 235).

Metaphorically, Gibson uses the term cyberspace to present the nature of entering a parallel dimension to the reader, implying that the digital world is a place where everyone interacts. The ranged lines of light and clusters of data in the "non-space of the mind" indicates that cyberspace is not a physical realm but exists and is perceived mentally.

Like cybersecurity, cyberspace has numerous definitions in the literature across different disciplines, including technical, social, legal, military and economic contexts. As research in this area progresses, the number of definitions increases. Rather than focusing on individual definitions, quoting Kuehl's definition, which treats cyberspace as a global domain, provides a comprehensive framework for understanding it (Kuehl, 2009: 26).

The dynamic nature of cyberspace has led to it being considered as a fifth domain, besides the four traditional domains of land, air, sea, and space, where states can exercise their sovereign powers (Wu et al., 2018: 1459).

However, the main feature that differentiates cyberspace from these four spaces is that it does not indicate a physical area. Therefore, it has no physical or geographical boundaries and continues to develop, unlike the other four more static domains. This fundamental feature makes it difficult to define sovereignty over cyberspace. Additionally, after the fall of the Soviet Union, the emergence of rival states increased the importance of traditional security concerns in military and technological terms.

Consequently, states have begun to perceive cyberspace as a competitive and dangerous domain of espionage, covert actions, and armed conflict among states (Fidler, 2022: 14). As a result, most states choose to establish national cyberspace strategies. These strategies typically emphasize common themes such as international cooperation on cyber issues and the strengthening of security in cyberspace. Because in today`s world, international security is synonymous with cybersecurity (Kleinwähter, 2021: 13).

Cybersecurity Governance within the Framework of Inter-state Relations

The evolving nature and diverse characteristics of cyberspace are redefining the theory, policies, and practices of inter-state relations. The modern understanding of cyberspace has shifted from being seen as a matter of low politics to one of high politics (Choucri, 2012: 3). Low politics addresses less critical and daily issues, such as societal issues and domestic affairs, which do not directly affect national security or the continuity of the state. In contrast, high politics concerns itself with issues that are crucial, especially for national security, such as military defence, foreign policy, and the fundamental values of the state. Thus, high politics is often prioritized and regarded as pivotal for the security and survival of the state.

Although cyberspace encompasses important elements of both low politics and high politics, its significance in national security and international relations is increasingly placing it in the realm of high politics. This shift in perception highlights the importance of developing robust frameworks for global and cybersecurity governance within the inter-state relations. As cyberspace increasingly influences national security and survival of states, comprehensive international cooperation and strategic policies are essential to tackle the complex challenges and threats that arise in this domain.

Governance stems from the ability to use governmental authority, but it can occur in the absence of a government or governmental mandate (Fidler, 2022: 17). In this regard, the meanings of governance and government do not refer to the same thing. Government refers to activities bolstered by formal authority, primarily supported by public power, to ensure the application of policies formulated according to certain rules. In contrast, governance is a broader concept that includes government institutions but also encompasses informal mechanisms. Governance activities do not necessarily rely on public power and can operate through shared goals and informal arrangements. Therefore, governance is a system based on ratified constitutions, regulations, and agreements, as well as intersubjective meanings. In this sense, while governments can continue to function despite substantial opposition to their policies, effective governance requires the consent of the majority or, at the very least, the most powerful individuals affected by it (Rosenau, 1992: 4). Relying on collective and mutual consent rather than coercive power, it is essential for managing today's interconnected and digitalized affairs.

In addition to states, the United Nations (UN), NATO (North Atlantic Treaty Organization), EU, and other international organizations have adopted declarations and binding agreements under international law to regulate data use and prevent misuse in cyberspace. These collaborations and efforts illustrate the hybrid nature of international cybersecurity regimes and are crucial for enhancing the effectiveness of cybersecurity governance and ensuring cyber deterrence (Fidler, 2022: 22).

Consequently, many cybersecurity governance activities focus on helping countries improve their national cybersecurity defences by providing technical assistance, alongside domestic efforts (Cavelty, Egloff: 2019: 49).

EU`s Cybersecurity Policies and Regulations

On a global scale, within the expanding framework of global governance, there is a need for a functioning international order to combat increasing global threats (Wessel, Odermatt, 2019: 42). At this point, the EU supports the discourse of a rule-based international order by bringing its founding values to the world stage, using its normative power more effectively in matters of foreign policy.

The protection of the EU's founding values must also be ensured in cyberspace. This argument is at the core of the EU Cybersecurity Strategy- An Open, Safe and Secure Cyberspace adopted in 2013 by the European Commission and the High Representative, which emphasizes both the internal and external dimensions of this new policy area (Tsagourias, Buchan, 2015: 403). At the same time, cybersecurity is an integral part of the Common Security and Defence Policy (CSDP), which forms the basis for the EU's external security action. Therefore, the EU has formulated various policies to secure its digital infrastructure and to establish international norms. In doing so, the EU contributes significantly to the global cybersecurity environment, fostering cooperation with states and other international organizations to address cyber threats.

The EU`s Role to Improve Cybersecurity Policies

Article 3(5) TEU delineates the principles and values that the EU shall follow on the international stage, aligning with the shared values on which the EU is founded according to Article 2 TEU, including the rule of law, democracy and the protection of human rights. The relevant article states that the EU will thereby contribute to peace and security. Furthermore, it emphasizes the commitment to protecting and developing international law, including respect for the principles of the UN Charter.

Article 21 TEU consolidates all the principles and goals of the EU's foreign activities for the first time, aiming to create coherence (Ramopoulos, 2024: 201) . This comprehensive approach underscores the need for consistency between internal and external policies. However, the apparent division between these policies within the European security policy framework undermines the EU's capacity to effectively respond to cyber threats (Tsagourias, Buchan:2015: 419).

EU cybersecurity represents a crucial area where global and bilateral policies are interconnected, requiring the EU to integrate various legal competences (Tsagourias, Buchan:2015: 404). The 2013 Strategy mentioned in the previous section aims to combine these legal competences while formulating wide-ranging regulations for the EU cybersecurity policies. In this strategy, public and private actors coordinate and operate within a multi-stakeholder framework. Notably, it is the first comprehensive policy document created to ensure the digital security of the EU (Joint Communication to the European Parliament, 2024). However, it should be noted and not ignored that various policy documents, which formed the basis of the Strategy document, were published before 2013. In this context, these documents hold varying degrees of importance in cybersecurity and combating cybercrime. They have contributed to developing a comprehensive approach in the 2013 Strategy by

increasing the EU's awareness and capacity in cybersecurity (Bergamasso et al., 2020, Chapter 4).

The roots of the EU Cybersecurity policy lie in the realm of information and computer security, which has been vital for the sustained growth of economies and the completion of the single market (Carrapico, Barrinha, 2017: 1259). Early policy efforts such as Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Directive 95/46/EC), Directive 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services (Directive 2002/21/EC) , Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures (ECI) and the Assessment of the Need to Improve their Protection (Council Directive 2008/114/EC, 2008) are some significant policy documents related to telecomunications, user privacy and critical infrastructure implemented by the EU before the 2013 Cybersecurity Strategy. As another early-stage policy effort, in the 2001 Commission Communication "Network and Information Security: Proposal for a European Policy Approach," the EU recognized that security had become a key priority due to the significant role of communications and information in economic and social progress. Thus, the EU took another step beyond efficiently operating the Single Market by recognizing for the first time that network and information security, cybercrime, and data protection are closely interrelated policy areas (Kasper, Vernygora, 2021: 47). In this regard, Article 114 TFEU is a crucial provision that stipulates the enactment of rules to eliminate existing obstacles to the functioning of the internal market. Given the critical importance of network and information systems in enabling the cross-border movement of goods, people and services, ensuring their resilience and stability is vital for the effective operation of the internal market. Pertaining to this, Article 114 TFEU provides the legal framework for harmonizing cybersecurity laws through adopted measures across the EU, enabling a unified internal market (Tsagourias, Buchan, 2015: 416).

The harmonization process was accelerated with the 2016 Network and Information System (NIS) Directive (Directive (EU) 2016/1148) which was incorporated into the national laws of all EU Member States. This directive aims to update and harmonize existing cybersecurity measures across Member States. It also enables the establishment of a new administrative structure for more effective implementation of cybersecurity policies and strategies.

In 2019, the EU introduced the Cyber Security Act, along with the NIS Directive, to further bolster its cybersecurity regulatory framework (Papakonstantinou, 2022: 78). In terms of strengthening the institutional and administrative structure, the Cybersecurity Act reinforces the EU Agency for Cybersecurity (ENISA) by establishing a permanent mandate for it, enhancing EU cybersecurity competences at both national and European levels by providing ENISA with more resources and an expanded authority (The EU Cybersecurity Act).

However, despite leading to significant changes in mindsets and institutional approaches, the existing NIS Directive has also shown its shortcomings (Proposal for directive on measures for high common level of cybersecurity across the Union). The societal digital transformation, accelerated by the COVID-19 pandemic, has altered the cybersecurity threat landscape and calling for innovative responses to the new challenges arising from these shortcomings. The NIS2 Directive (Directive 2022/2555) aims to rectify the shortcomings of the current NIS Directive by ensuring entities adopt a forward- thinking approach to resilience and risk

control. This modernization of the legal framework will make the EU better prepared to respond to and detect cyber threats (Repealing Directive (Eu) 2016/1148).

In this context, text of the NIS2 Directive is significantly more detailed than its predecessor. Every chapter specifically focuses on reducing the discrepancies caused by the original Directive due to its allowance for flexible implementation by the EU Member States (Papakonstantinou, 2022: 11).

Effectiveness of EU Cybersecurity Strategies in the Context of Relevant Institutions

As mentioned in the previous section, EU cybersecurity represents a significant area requiring the integration of legal authorities at different levels. This integration depends on the coherence and coordination between both the national practices of each member state and European institutions (Portela, Raube, 2012: 5).

Coherence generally refers to the alignment of goals and objectives, but from an EU perspective, it should be evaluated both horizontally and vertically. Vertical coherence involves the consistent interpretation and application of EU rules by all member states, ensuring alignment between EU and national policies. Horizontal coherence refers to the alignment among different policy areas within the EU (Carrapico, Barrinha, 2017: 1257). To reduce vertical incoherence and enhance coordination in cybersecurity policies, the first institution to consider is the ENISA.

ENISA was formed in 2004 by Regulation 460/2004 (Regulation (EC) No 460/2004) as an agency dedicated to strengthening network and information security across the EU. Until the last extension by Regulation 526/2013 (Regulation No 526/2013), it operated under a mandate that was periodically renewed. Subsequently, with the adoption of the EU Cybersecurity Act (Regulation 2019/881), namely Regulation 2019/881, ENISA has operated as a permanent agency starting from 27 June 2019. This act not only strengthened its cbersecurity measures but also established certification framework for Information and Communications Technology (ICT) products and services (Briefing Paper: 2019).

As part of the EU crisis management framework, another key entity for ensuring consistency and cooperation within the union is the European Cybercrime Centre (EC3), established by the European Police Office (EUROPOL). EC3's mission is to enhance law enforcement's ability to combat cybercrime in the EU, thereby safeguarding businesses, European citizens, and governments from online threats (European Cybercrime Center: 2024). EC3 targets cybercrime, including online fraud by organized groups seeking significant financial gains, online child sexual exploitation with severe impacts on victims, and cybercrimes that threaten critical infrastructure and information systems within the EU (Tsagourias, Buchan, 2015: 409).

Since 2010, Cyber Europe, coordinated by ENISA and the guided by European cybersecurity experts, has conducted several cyber incidents and crisis management practices featuring scenarios based on real-life events (Cyber Europe, 2024). Alongside this, the operations conducted within EC3 to combat cybercrime demonstrate the effectiveness of EU cybersecurity strategies in the context of relevant institutions.

Challenges and Limitations Stemming from Implementing Cybersecurity Policies and Strategies

Implementing cybersecurity policies and strategies is closely related to effective cybersecurity governance. Cybersecurity governance has become an international issue involving multiple stakeholders in both the public and private sectors. As a result, harmonization challenges have emerged, particularly for the EU, which plays a significant role in shaping international cybersecurity policies and strategies (Al Blooshi, Eksteen, 2022: 19).

One of these challenges is the imparity in cybersecurity maturity levels among member states, leading to inconsistent application and enforcement of regulations. The EU considers itself an important actor in the international system and argues that the complexity of cyber issues positions it well to act, support, and coordinate (Kasper, Vernygora, 2021: 69). However, the primary responsibility for cybersecurity still remains with the Member States. This, thereby, disrupts the fostering of coherent and harmonized strategies within the EU. At this point, the NIS directives are essential in this context, aiming to enhance cybersecurity across the EU and set standards for member states to develop and update their national cybersecurity strategies (Compact Committee of the Supreme Institutions of the EU, 2014-2020). The goal is to minimize implementation-related disparities and promote cooperation through these standards.

Particularly in combating cybercrime, the EU needs to be a stabilizing force, and the changing security environment dictates the necessity of greater EU security autonomy and clear rules for the sake of predictability and economic development. Efforts to improve cyber defences against cybercrime have not produced significant progress in international law. Domestic cyber defence falls within a state's sovereign authority, and governments can strengthen national cyber defences without treaties or customary international law (Fidler, 2022: 48). Given the necessity for states to increase cooperation and sign agreements to develop international law in the creation of cyber norms, addressing differences among EU member states is essential. This will also help shape international regulations in accordance with EU policies.

Another significant challenge is the variation in resource allocation and investment in cybersecurity across member states, which hampers the development of uniform and robust cybersecurity measures throughout the EU. In this regard, the role of the private sector is crucial, especially regarding public-private partnerships, as many critical infrastructures are operated by private entities. ENISA's reports show that by identifying good practices and common issues among member states in the implementation of the NIS Directive, steps are being taken to harmonize these practices (NIS Investment Report, 2023)

However, despite efforts to increase ENISA's funding and capabilities, the disparities in how different member states allocate budgets for cybersecurity create an uneven landscape. This inconsistency undermines the overall security posture of the EU, as some states lag in implementing necessary cybersecurity measures. Thus, while ENISA's enhanced funding and strategic collaborations are steps in the right direction, addressing the variations in national investments remains critical to achieving a cohesive and resilient cybersecurity framework across the Union (Digital Europe, 2024).

Last but not least, monitoring the implementation of strategies and policies can be stated as an another challenge. According to a report by the European Court of Auditors, one of the

significant hurdles in the EU's cybersecurity policy is the absence of effective monitoring and evaluation mechanisms, which leads to inconsistencies in the application and enforcement of cybersecurity measures across different member states (Briefing Paper, 2019).

Relationship Between the EU and NATO in Cybersecurity

The relationship between the EU and NATO has converted significantly over the years, with cybersecurity emerging as a key area of mutual interest.

The rhetoric that NATO was founded in response to the Soviet Union threat is not incorrect, but it is not the whole story. NATO was established not only to deter Soviet expansion but also to prevent the revitalization of nationalist militarism in Europe through a strong North American presence and to strengthen European integration (A Short History of NATO). Hence, by its nature, NATO is a political-military international organization. In contrast, the European Union is a supranational organization with an economic basis and operates through institutions to which the member states transfer some of their sovereign powers. The two organizations have shared values, compatible strategic interests and many member countries in common. In this sense, the general approaches adopted by them complement each other and avoiding unnecessary duplication (Kutlu, 2023: 35)

The end of the Cold War and the transition from a bipolar international order to a multipolar one, along with the rise of digital technologies over time, led both organizations to reassess their strategic priorities. For NATO, the turning point was in 2007 when Estonia was subjected to a coordinated cyberattack for three weeks, which targeted news outlets, ministries, government and parliamentary portals, major banks, internet service providers and small businesses (2007 Cyber Attacks on Estonia). For the EU, it was the 2014 annexation of Crimea by Russia. Following these events, both NATO and the EU intensified their initiatives in the cyber sphere (Lété, Pernik, 2017: 2).

In 2003, the Berlin Plus Agreement marked a significant milestone, allowing the EU to draw on NATO's military assets for its operations, establishing the foundation for closer collaboration in various security domains, including cybersecurity (Tardy, Lindstrom, 2019: 10). This agreement was built on the earlier NATO-EU Declaration on European Security and Defence Policy (ESDP), which opened the door to such cooperation (Cooperation with NATO). As cyber threats have grown in complexity and scale, the EU and NATO have increasingly acknowledged the importance of a coordinated approach, leveraging their respective strengths to enhance overall cyber resilience and defence capabilities.

The EU and NATO share common values, strategic interests, and many mutual members. Despite having overlapping qualifications, they have different focus areas, which help maintain their indispensable partnership in international crisis management and especially in combating growing hybrid threats.

NATO's main efforts are focused on military defence. While it acknowledges the importance of civilian networks and the risks they face through its work on hybrid threats, it does not have the legal or policy tools to directly address these issues. At this point, the EU steps in (Ilves et al., 2016: 130). The linkage between the EU's internal and external security provides it with an advantage in effectively combating both internal and external security threats (Tardy, Lindstrom, 2019: 9). The EU's regulatory role and its authority in home affairs make it a

significant threat management actor, particularly in areas counterterrorism, hybrid threats, cyber defence, and military mobility.

The importance of the EU-NATO partnership was formalized in the 2016 and 2018 Joint Declarations, which laid the groundwork for enhanced cooperation in several key areas. The 2016 Declaration was signed at NATO`s Warsaw Summit, focusing on seven strategic areas: cybersecurity, defence capabilities, hybrid threats, operational cooperation in maritime domain, industry and research, exercises and resilience of partners. It was a pivotal moment, marking the beginning of a structured and strategic partnership. Building on the 2016 Declaration, the 2018 Brussels Joint Declaration further expanded the scope of cooperation. This declaration highlighted the progress made since 2016 and set ambitious goals for future joint efforts. Moreover, the parties pledged to rapidly advance in areas like counter-terrorism, military mobility and encouraging the peace, women and security agenda (The Third Joint EU-NATO Declaration).

Commitments to cooperation are not limited to joint declarations but are also reiterated in reports published separately by both organizations. In 2022, the EU's Strategic Compass, an action plan aimed at strengthening its security and defence policy until 2030, was published (Strategic Compass for Security and Defence).This plan emphasizes the importance of maintaining the transatlantic bond in the scope of Russia's military aggression against Ukraine for Euro-Atlantic security and investing in more technologies to reduce dependencies in the defence sector. In the same year, NATO's Strategic Concept, which outlines its core tasks to enhance cooperation in areas of common interest like emerging disruptive technologies, military mobility and hybrid and cyber threats, was also published (NATO 2022 Strategic Concept).

The third Joint Declaration signed by NATO and the EU in 2023 aims to further strengthen and expand the strategic partnership, building on the previous declarations of 2016 and 2018. This declaration emphasizes the need for NATO and the EU to act together in response to increasing geostrategic competition. For the first time, China is featured in a joint declaration, with the statement that "China's growing assertiveness and policies present challenges that need to be addressed" (Joint Declaration on EU-NATO Cooperation). The Joint Declaration aims to enhance cooperation in emerging disruptive technologies. Additionally, it highlights that Russia's war against Ukraine poses the greatest threat to Euro-Atlantic security and underlines the prominence of NATO-EU collaboration in addressing this issue. The declaration reaffirms the complementary and mutually reinforcing roles of NATO and the EU in supporting international peace and security.

Challenges and Opportunities in the EU- NATO Cooperation

While the EU-NATO cooperation mechanism, implemented through legal instruments like the Berlin Plus Agreement and the Joint Declarations, has facilitated the sharing of tasks and responsibilities between the two organizations with differing founding purposes, it has been criticized for largely remaining on paper (Akgül et al.,2014: 133).

The development of the CFSP in the EU and the movement towards an autonomous structure in conducting external relations are, in fact, an extension of the Europeanist perspective that views the presence of the US in Europe as a threat. In contrast, Atlanticists support the US military presence in Europe and emphasize that NATO is not only a collective

defence organization but also the primary institution responsible for ensuring European security (Akgül et al.,2014: 161).

Twenty-six years ago, when the EU's desire for greater autonomy in security and defence was introduced at the St. Malo summit, Secretary of State Madeleine Albright pointed out the three "D"s in response to the discussions that arose from it (Press Conference by US Secretary of State Albrigh). These are: the decoupling of European decision-making from NATO decision-making; the duplication of NATO efforts by European security anddefence initiatives; and the EU's discrimination against European NATO members who are not part of the EU. Albright emphasized that these issues could have negative impacts on Europe's security architecture and stressed the importance of maintaining alignment with NATO (European Strategic Autonomy). This difference in understanding led to different interpretations of NATO's prioritization of crisis management operations in Europe by the US and the EU, which led to a division between the two organizations rather than their complementarity (Akgül et al.,2014: 161).

An example of this can be seen in the difficulties faced in coordinating actions between NATO and the EU for the peacekeeping operation in the Darfur region. Both organizations aimed to assist the African Union troops in different capacities, but the lack of a unified command and control structure resulted in inefficiencies and delays (NATO and the EU: lending a helping hand in Darfur).

NATO and the EU typically focus their cooperation on political matters. However, to enhance collaboration, particularly in the cyber domain, it is necessary to prioritize technical cooperation while maintaining the distinct institutional structures of both organizations (Sarcià, 2024). Despite having common participants, there are EU member states that are not NATO members and vice versa. This situation creates de facto discrimination against non-EU NATO members, as the EU is often reluctant to share operational information or include these countries in operations.

To address these issues and improve cyber cooperation, it would be beneficial to concentrate technical collaboration and refrain from ideological conflicts for the advantage of both organizations and their respective member states and allies. Concentrating on enhancing cooperation infrastructure and capacity rather than problems would be more functional. In this context, instead of duplicating each other's capabilities and acting separately, the two organizations should strive to be complementary and take responsibility according to their capabilities in planned operations, paving the way for more effective cooperation (Akgül et al.,2014: 165).

Cybersecurity Agreements and Sovereignty Issues

Similar to the concept of security, there is no consensus on a universally accepted definition for the term "sovereignty". While the origin of the concept focused on the relationship between the individual and the sovereign, its development in the scope of international law was shaped by the international role of the state and subsequently became the subject of discussions on the relations between equal sovereign states (Brand, 2002: 280). Therefore, developments in international law necessitate the reassessment of the meaning of sovereignty. This necessity diversifies the definitions related to the concept (Brand, 2002: 280).

Sovereignty has historically been synonymous with the authority of the state. State sovereignty has traditionally been regarded as the right to exercise supreme political authority (legislative, executive and judicial) over a geographical area, a group of people, or itself. This definition actually refers to internal sovereignty, which involves the state`s political authority and control over its territory and people (Synman-Ferreira, 2006: 2).

Additionally, sovereignty has an external or international aspect, which encompasses the rights a state possesses in its relations with other states. In this regard, sovereignty also refers to the state's recognition as an independent entity in the international arena and its possession of equal rights. The International Court of Justice (ICJ) affirmed this interpretation of sovereignty in its 1928 Island of Palmas decision as follows:

> *"Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State"(Island of Palmas Reports of International Arbitral Award: p.838).*

As evident from the decision, this definition reflects the dual nature of sovereignty: firstly, as "the authority to govern a territory" and secondly, as "the exclusion of any external interference".

Although cyber sovereignty is an ambiguous concept often associated with state power and independence in cyberspace, in its broadest definition, it is the implementation of the principles of state sovereignty to cyberspace (Baezner, Robin, 2018: 6). Thus, states have sovereignty over any cyber infrastructure and related activities within their territory. In addition, as a prerogative of their sovereign authority, they can exercise jurisdiction over certain infrastructure and activities outside their territory, and over the persons involved in those activities (Jensen, Talbot, 2014: 277).

Nevertheless, the incidents and activities related to cyber infrastructure experienced daily raise significant questions about the conduct of these activities and the associated responsibilities of states. These questions, ranging from the source of the activities to who is carrying them out, will be addressed in the subsequent sections.

Sovereignty- related Challenges in Cyberspace and How the EU Navigates Them Through Legal Framework

Cyberspace, while emerging as the fifth dimension in which states exercise their sovereignty, is inherently non-physical and lacks geographical boundaries. Traditional sovereignty is exercised in physical and well-defined areas, whereas the virtual nature of cyberspace makes it difficult for nation-states to exercise such sovereignty in the same way.

Additionally, the rapid sharing of information and data in cyberspace and the anonymity with which cyber activities can be carried out hinder states' ability to intervene in the negative consequences of these actions. Furthermore, it is necessary to determine whether states are responsible for cyber acts committed especially by non-state actors, and to what extent they are held accountable if they neglect their responsibilities regarding these activities, in other words, the issue of attribution and its degree.

In response to these challenges, including a major 2007 attack on Estonia, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn initiated a multi-year project, resulting in the Tallinn Manual, which provides expert opinions on applying

international law to cyber activities. It is a legally non-binding academic work on how existing international law norms can be adapted to the digital age and how international law should be interpreted as part of cyber activities. In this sense, it serves as an important resource for states and international organizations in developing strategies and policies in the field of cyber defence.

The first edition of the Manual (Tallinn Manual 1.0), introduced in 2013, focused primarily on the international rules applicable to cyber operations during armed conflict. The second edition released in 2017, expanded the scope to include peacetime cyber operations (Jensen, Talbot, 2017). It also addressed a wide range of related topics in international law, encompassing sovereignty, state responsibility and human rights. In 2021, the Tallinn Manual 3.0 Project was launched as a five-year initiative to revise the sections from previous editions and to research new topics of importance for states (The Tallinn Manuel).

The EU, as part of its foreign security policy, has developed numerous cybersecurity strategies and implemented them through various legal regulations. However, the war in Ukraine has dramatically impacted the EU's foreign and defence policy, including its cyber dimension, and has highlighted the need for new approaches to strengthen cyber resilience (SEDE: p.19). Since February 2022, the ongoing invasion of Ukraine by Russian armed forces has been accompanied by destructive cyberattacks, clearly demonstrating the trend of using cyberattacks as a means of warfare. According to the CyberPeace Institute report, a total of 2776 cyber incidents against critical infrastructure and civilian objects in Ukraine and the Russian Federation, conducted by 106 different threat actors between January 2022 and September 2023, have been documented (Cyber Dimensions of the Armed Conflict in Ukraine).

To leverage common EU preparedness, detection, and situational awareness for these attacks, the EU Cyber Solidarity Act introduced the Cybersecurity Alert System. The Act also establishes the Cybersecurity Incident Review Mechanism to evaluate and overview specific cyber incidents. Through these mechanisms, the EU aims to support its members and offer mutual cooperation among them (The EU Cyber Solidarity Act).

What has been mentioned so far concerns the strategies developed to eliminate cyberattacks and minimize their negative effects, as well as the regulations put in place for this purpose. However, the conditions under which responsibility law rules can be applied to cyberattacks are also a substantial issue. Concerning this, attacks carried out by state and non-state actors should be examined individually, and the question of their attributability should be addressed. Moreover, how the state responsibility rules will be applied for cyber damage caused by any EU member state requires a separate assessment.

Compensation mechanism for Cyber Damages: Attribution and Responsibility

As previously stated, Tallinn Manual 2.0 serves as a comprehensive guide on how states should act within the framework of international law regarding cyberspace, and Article 6 specifically addresses the responsibilities of states in this respect. Article 6 provides:

> *"A State bears international legal responsibility for a cyber operation attributable to it, and which constitutes a breach of an international obligation".*

This provision is largely taken from the International Law Commission's (ILC) Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) and reflects customary rules on state responsibility. ILC was established in 1947 by the UN General Assembly to codify existing international rules and bring clarity and consistency to the legal principles that govern international relations (International Law Commission)

Although the Commission designed the articles as the text of an international agreement, the aim of the work is to strengthen the binding force of the rules in this sensitive area of international law. Therefore, ARSIWA is not an international agreement, but a guide aimed at codifying and formulating the basic rules of international law regarding the responsibility of states for their internationally wrongful acts (A/56/10 Report of the International Law Commission). With respect to this, one of the main features of the relevant work is that it adopts the distinction between primary rules, which set out norms of behaviour requiring states to 'do' or 'not do' certain actions, and secondary rules, which are applied in case of violation of these norms, focusing particularly on the latter (Pirim, 152).

Article 6/2 of the Tallinn Manual 2.0 states that holding a state responsible for an action is a fundamental principle of international law and stipulates state responsibility for cyber operations under two conditions. These conditions, which are drawn up in parallel with Article 2 of ARSIWA, are as follows:

> *1) "the act in question is attributable to the State under international law; and,*
>
> *2) it constitutes a breach of an international legal obligation applicable to that State (whether by treaty or customary international law)"* (Schmitt, 2017: 29)

It is also stated in the continuation of the relevant provision that such a breach may consist of an act or an omission.

There are many difficulties encountered in the investigation, prosecution, and adjudication of actions directed at the cyber domain or carried out using cyber weapon systems. In particular, the borderless and distanceless nature of the cyberspace makes it hard to determine who is responsible for an action and under what conditions (Şafak, 2020: 142). In other words, the absence of a common understanding among states regarding what evidence is sufficient for attribution and the absence of legal rules to limit such behaviours render the responses to these types of actions ineffective (Banks, 2021: 1040). Sanctions are also a type of response, which is why the discussion of effectiveness is important. The legal system asserts its existence through the rules of responsibility that regulate issues such as the nature of rights, the structure of obligations, and the definition of sanctions to be applied in case of violations of these obligations.

The responsibility law of the international legal system is of more vital importance compared to the responsibility law in domestic legal systems. This is because, in international law, which is exempt from the principle of compulsory jurisdiction, sanctions that can overcome arbitrary actions of states must be established to maintain the legal order (Pirim, 150).

Attribution is a matter that needs to be evaluated separately in each case, depending on the subject of the relevant action and other conditions. Responsibility is a consequence of the violation, not the resulting damage. Although damage is not sought as an element of responsibility, it is important in determining the type and form of reparation (Erkiner, 2022: 7).

Every international wrongful act entails the responsibility of the state that commits the act. This responsibility imposes certain secondary obligations on the state concerned. If the international wrongful act that gives rise to responsibility is ongoing, the responsible state is obligated to cease this act. Additionally, the responsible state must take reasonable measures to ensure that the violation does not continue, and, if necessary, provide assurances that the violation will not be repeated.

The most important secondary obligation arising from the rules of state responsibility law is reparation. According to the obligation of reparation, the responsible state is required to remedy all adverse damages caused by the wrongful act. Essentially, the state's obligation of reparation arises automatically with the occurrence of damage (Erkiner, 2022: 7). This obligation begins not from the moment the damage is identified, but from the moment it occurs. In international doctrine and practice, three different forms of reparation are envisaged for the remediation of damage. These are restitution, compensation, and satisfaction. Full and proper reparation of damage is achieved by using one or several of these forms. In some cases of damage, completely eliminating the adverse consequences of the wrongful act may require the application of multiple forms. Theoretically, restitution is the primary form of reparation to be considered first. Restitution aims to restore the material and legal situation to what it was before the damage occurred. However, in cases where restitution is impossible, or it is determined that it does not provide a benefit worth preferring over compensation under the principle of proportionality, the form of compensation will be resorted to. When restitution or compensation is not feasible, and to the extent that they are not feasible, the form of satisfaction is resorted to. The form of satisfaction includes the acknowledgment of the international wrongful act and violation, the official expression of apologies, and any suitable declarations and practices. In this context, satisfaction is a subsidiary form, applied only after restitution and compensation have been considered. Reparation through the form of satisfaction becomes possible in cases where the damage caused by the wrongful act cannot be remedied through restitution or compensation. According to Article 37(3) of ARSIWA, satisfaction must be proportional to the damage and provided in a manner that does not humiliate the responsible state.

Governing Cyberattack Damages: Attribution of Responsibility to State and Non-State Actors

There are various situations in which a state's responsibility may be invoked. The scope of these situations is very broad and may include actions such as breaching an international agreement, violating another state's territorial integrity, or damaging another state's property, as well as omissions, such as failing to take necessary measures (Shaw, 2021: 684)

The ICJ's 1949 Corfu Channel judgment is one of the most important examples of international responsibility arising from omission. In its judgment, the Court stated that the Albanian government could not be held responsible for the illegal act of mine- laying in its territorial waters and the subsequent sinking of British warships based solely on knowledge or the presumption that it should have known about the mine- laying. However, Albania's failure to inform other states about the mines in its territorial waters was considered an omission that invokes responsibility (ICJ, Corfu Channel Case).

Article 4 of the ARSIWA stipulates which conduct should be regarded as an act of state under international law. According to it, the conduct of any state organ, regardless of its functions,

legislative, executive, or judicial, its position within the state's organization, and whether it is an organ of the central government or a territorial unit of the state, is considered an act of the state. In a similar vein, Rule 15 of the Tallinn Manual 2.0 sets forth the corresponding principle as follows, specifically applied to cyber operations executed by a state:

> *"Cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State".*

Therefore, any cyber activity carried out by intelligence, internal security, military or other state agencies engages state responsibility if it violates an international legal obligation binding on that state (Schmitt, 2017: 87). Nevertheless, attributing an act that constitutes a violation of international law to a state is particularly challenging, especially considering the difficulty in identifying such acts in the cyber domain.

There are two main difficulties in attributing cyber activities to states. The first is the hesitation of states to accept responsibility for acts conducted in cyberspace, and the second is the challenge of determining the origin and timing of any cyber act. The nature of cyber domain inherently provides anonymity. Therefore, this feature makes it attractive to those who wish to conduct harmful activities. The difficulty in timely detecting and intervening in such activities

also complicates the acceptance of responsibility by states for acts originating from within their own territories. Additionally, the internationalization of activities in cyberspace means that unless the perpetrators accept responsibility, the mechanisms of accountability cannot be effectively enforced. The Stuxnet virus is a prime example in this regard; despite numerous allegations, neither the United States nor Israel has officially accepted responsibility for the attack. This situation is, in fact, exploited by states and complicates the application of responsibility rules, particularly for actions carried out through proxies, such as non-state actors (Jensen, Talbot, 2017: 279).

The conditions under which a cyber operation conducted by non-state actors may be attributed to a state are outlined in Rule 17 of the Tallinn Manual 2.0 as follows:

> *"Cyber operations conducted by a non-State actor are attributable to a State when:*
>
> *(a) engaged in pursuant to its instructions or under its direction or control; or*
>
> *(b) the State acknowledges and adopts the operations as its own".*

This provision is essentially the version of Article 8 of ARSIWA adapted for cyber operations. Article 8 of ARSIWA states that actions carried out by an individual or a group of individuals under the instructions, direction, or control of a state are considered actions of that state. The meaning of the term "instruction" was clarified by the ICJ in the Bosnian Genocide case. The Court stated that instructions must be given "in respect of each operation in which the alleged violations occur, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations" (Amerasinghe, 2008: 427).

Besides instruction, the relevant article also refers to responsibility arising from a state's "control" over a private entity. There are two main criteria focusing on different aspects of the term "control". In the Nicaragua case, the ICJ stated that for a state to be held responsible for the actions of another state or armed group, it must have direct and effective control over the actions in question. In the Tadić case, the International Criminal Tribunal for the former

Yugoslavia (ICTY) discussed the "overall control" criterion and found that it is sufficient for a state to have general control over a specific armed group or organization. This control includes influence over the group's strategy, planning, and general operations. Therefore, direct control over each individual action is not necessary (Crawford, 2013: 147).

The distinction between effective control and overall control emphasizes the varying degrees of state involvement required for attributing responsibility under international law. While the effective control criterion necessitates that a state directly manages the specific actions of another entity, the overall control criterion allows for a broader scope, where general influence over an entity's strategies and actions is sufficient. This distinction is also crucial for cyber operations, as the extent and nature of control may significantly impact the attribution of responsibility.

Given these nuances, it is important to assess whether the level of state control over non-state actors involved in cyber activities meets the required criteria for attribution. In light of these considerations, it can be said that, according to international law, cyber activities conducted by non-state actors under the effective control of a state are attributable to that state. Merely encouraging or supporting these actions is not sufficient for attribution (Tsagourias, 2016: 472).

Assessing the EU`s Responsibility in International Law

As an influential international actor, when the EU interacts with states and other international organizations, it must abide by the norms that form the international order. This acknowledgment raises the question of the extent to which the EU may be held accountable by its international allies for violations of international law and the degree of responsibility it bears in such situations. This question might arise with regard to all of the EU's international obligations; however, it is particularly significant in terms of the CFSP (Wessel, Larik, 2020: 168).

In 2011, the International Law Commission (ILC) adopted a series of provisions concerning the responsibility of international organizations, known as the Draft Articles on the Responsibility of International Organizations (ARIO). According to Article 2 (a) of the ARIO, the term of international organization should be understood "an organization established by a treaty or other instrument governed by international law and possessing its own international legal personality". There is no doubt that the EU is an international organization that meets these criteria, and thus it may be held responsible for any internationally wrongful act.

rom this point, another important question that needs to be answered is which acts may be attributed to the EU. According to Article 6(1) ARIO states that any actions by an organ or agent of an international organization, performed in their official capacity, are considered acts of the organization under international law, regardless of their specific role within the organization. However, what sets the EU apart from other international organizations is its supranational nature.

Consequently, both its internal functioning and the distribution of competences in the conduct of external relations differ from those of other international organizations. Article 6(2) ARIO stipulates that "the rules of the organization" shall apply when determining these "organs and agent"". Therefore, it must be determined whether, in the case of any

internationally wrongful act, the member states should be held individually responsible, or the EU should be held responsible as an organization (Wessel, Larik, 2020: 169).

The EU is an indispensable part of the international legal order, and thus there are many connections between the EU and international law. However, the EU's position as an autonomous entity in relation to international law leads to tensions when it needs to establish relationships with other global actors in accordance with international law (Wessel, Larik, 2020: 171). A concrete example of this tension can be seen in the Kadi case (Judgment of the Court -Grand Chamber, 2024) by the European Court of Justice (ECJ). The court asserted the autonomy of the EU legal order and maintained that all EU actions, including those implementing UN Security Council (UNSC) resolutions, must comply with fundamental rights as protected by the EU.

In conclusion, the interdependence of the EU's internal and external competences, along with its supranational nature that distinguishes it from other international organizations, makes the application of rules on responsibility for internationally wrongful acts more difficult.

State Responsibility in the Cyber Realm: EU Approaches and Difficulties

Although the general understanding is that traditional state responsibility rules apply in the cyber realm, the implementation of these principles to the cyberspace is debatable. As mentioned in the previous section, the applicability of state responsibility rules to international legal subjects other than states is not yet clear. Moreover, the evolving nature of the cyber domain, driven by technological advancements, makes the application of these principles even more challenging.

Due to the increase in malicious cyber activities, the EU has been prompted to take necessary measures against cyber-attacks and to develop mechanisms aimed at deterring such activities. One such regulation is CFSP Decision 2019/7973 (Council Decision- CFSP, 2019/797 of 17 May 2019), which enforces restrictive measures against cyber activities that pose a substantial potential threat to the EU or its Member States. This decision is a part of the broader EU framework known as "Cyber Diplomacy Toolbox", which encompasses a range of measures and strategies address and respond to cyber threats, including sanctions and other restrictive measures (Cyber Diplomacy Toolbox).

Decision 2019/7973 covers cyber-attacks that represent an external threat to the EU or its member states, as well as attempted cyber-attacks that could have a significant impact. According to Article 2 of the decision, cyber-attacks posing an external threat include those which:

> *"a) originate, or are carried out, from outside the Union;*
>
> *(b) use infrastructure outside the Union;*
>
> *(c) are carried out by any natural or legal person, entity or body established or operating outside the Union; or*
>
> *(d) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union".*

In response to these malicious cyber activities, the EU may impose sanctions on individuals, entities, or bodies responsible for or attempting such actions. These sanctions may include asset freezes and visa bans. However, they are intended to respond to and deter malicious cyber activities rather than to serve punitive purposes. Thus, these sanctions are designed more for deterrence and reducing the frequency of malicious cyber activities rather than for enforcing accountability through traditional responsibility rules.

Overall, the EU has both the interest and capacity to develop an autonomous attribution mechanism for malicious cyber activities. However, differences in the capacity to attribute a cyber-attack to a specific third country among EU members even hinder the implementation of current responsibility rules. In other words, discrepancies in capacity among member states lead them to focus on deterrent measures rather than on the application of responsibility rules. An EU member that is not affected by the cyber-attack and lacks the ability to authenticate the forensic evidence provided by the targeted state often chooses not to activate the state responsibility mechanism (Poli, Sommario, 2023: 528).

t is evident that more specific rules for the attribution of internationally wrongful acts in the cyberspace need to be developed. The difficulty in adapting traditional state responsibility rules to activities in the cyber domain also provides a legitimate justification for states not applying the existing rules. Ultimately, the idea of initially concluding more limited but binding agreements to govern state behaviour in the cyber domain should remain a priority. These agreements could replace deterrent measures with binding rules of accountability, thereby increasing responsibility and providing reparations for the damages. Although a multilateral treaty containing general rules of conduct may not be very likely under current conditions, developing mechanisms for prohibiting or controlling specific areas, such as cyber espionage or malicious cyber activities against critical infrastructure, could be an important step.

Conclusion

In the modern world, the competences derived from the sovereignty of states have expanded. This enables them to exercise their authority not only over their sovereign territories but also in cyberspace. The exercise of rights and competences derived from sovereignty in cyberspace, where there are no physical boundaries, complicates the application of traditional concepts of sovereignty. States and numerous international organizations, notably the EU and NATO, are developing various strategies and policies to more effectively use their rights and these competences emanate from sovereignty in cyberspace.

The EU plays a significant role in establishing international customary rules in this field through its cybersecurity strategies, which include both as internal policies of its member states and as part of its foreign policy. The EU, leveraging its normative power, projects its founding values into the international arena. The transfer of these founding values to the international stage is crucial in establishing international legal rules that bind all subjects in a policy area. The inseparable nature of the EU's internal and external security policies facilitates the transfer of founding values and especially paves the way for strategies developed by both member states and the EU to evolve into multilateral international agreements in areas related to foreign policy.

In developing joint cybersecurity strategies, NATO stands out as the EU's strategic and most important partner. Despite having different characteristics in nature and founding purposes,

both organizations complement each other due to their many common members and values. These two significant organizations take important steps towards enhancing global cooperation in the field of international security, both through the security policies they develop and implement separately and through the joint declarations they put into effect. This cooperation enhances the effectiveness of both the EU and NATO in cybersecurity and ensures a stronger stance against global cyber threats. Such collaborations between states and international organizations are vital for ensuring the security of cyberspace and protecting sovereign rights in this domain.

One of the fundamental challenges in cyberspace is identifying the perpetrators behind malicious activities conducted in cyberspace. The anonymous nature of cyber operations and the constantly evolving technological landscape perpetuate this challenge. The draft articles prepared by the ILC regarding the responsibilities arising from states' wrongful acts govern the traditional rules of responsibility. This draft, which also forms the basis of the regulations in the Tallinn Manual, establishes the rules of responsibility law for wrongful acts committed in cyberspace. When interpreting the rules of responsibility for activities conducted in cyberspace, these two draft articles are considered together.

The EU has introduced many legal regulations to increase accountability for such activities conducted in cyberspace. However, the differences in competence and capacity among member states in attributing the responsibility of a cyber-attack to a third state complicate the application of responsibility law rules. Although the EU is an international entity capable of developing and implementing an autonomous cybersecurity responsibility mechanism, for now, the priority is to take steps to enhance the validity and effectiveness of existing rules.

The attribution of such cyber activities conducted by one of its members to the EU as an international organization is another topic of discussion. The articles on the responsibility of international organizations for wrongful acts are much more recent, and the limited functionality of organizations compared to states, constrained by their founding purposes, makes the application of responsibility law rules to such activities debatable.

The issue of attributing cyber-attacks conducted not only by states but also by non-state actors is equally important and complex. The conditions under which actions by non-state actors can be attributed to states have been the subject of numerous international court decisions and advisory opinions. The applicability of traditional international responsibility law rules to such actions is evaluated within the criteria of effective and overall control. It has been observed that discussions on the application of responsibility rules for such actions conducted in cyberspace are also conducted based on these two criteria.

Every international wrongful act gives rise to state responsibility. With the emergence of responsibility, a new legal relationship is established between the responsible state and the injured state. This legal relationship regulates the scope and consequences of the responsibility arising from the international wrongful act. It also imposes secondary obligations on the responsible state. If the international wrongful act that gives rise to the responsibility continues, the responsible state is obliged to put an end to this act. Additionally, the responsible state must take reasonable measures to ensure the non-repetition of the violation, if conditions require. As a rule, the responsible state is obliged to remedy all adverse consequences caused by the international wrongful act. Most of the time, all adverse consequences of the violation cannot be remedied. Therefore, it is intended to restore the

situation, in the best possible way, to that which existed before the violation. Three forms of reparation are accepted in international doctrine and practice to remedy the damage. These are "Restitution," "Compensation," and "Satisfaction." In cases and to the extent that restitution or compensation cannot be applied, the form of satisfaction is resorted to. Satisfaction includes the acknowledgment of the international wrongful act and violation, the formal apology, and any appropriate declarations and applications. In this context, satisfaction is a secondary form of reparation, following restitution and compensation.

In conclusion, the idea of concluding more limited but binding agreements to govern state behaviour in cyberspace should remain on the agenda. Such agreements could enhance accountability and provide reparation for damages, thereby strengthening the overall cybersecurity framework. Although a comprehensive multilateral treaty may not be feasible under current conditions, progress in specific areas, such as prohibiting cyber espionage or protecting critical infrastructure, would be beneficial.

The EU's efforts in cybersecurity reflect a commitment to adapting to the challenges of the digital age and ensuring the security and resilience of its member states. Continuous cooperation, innovation, and legal development are essential to addressing the complexities of cyberspace and enhancing global cybersecurity.

Acknowledgements:

This article was supported by the Jean Monnet Scholarship Programme, implemented by the Directorate for EU Affairs in collaboration with the Ministry of Treasury and Finance, the Central Finance and Contracts Unit, and the Delegation of the European Union to Türkiye. I sincerely thank the programme for its support, which also enabled the completion of my master's thesis, from which this article is adapted. I would also like to express my gratitude to Prof. Dr. Markus Kotzur for his valuable guidance and support throughout this research.

Funding Statement:

This article was funded by the Jean Monnet Scholarship Programme and is adapted from the author's master's thesis completed as a Jean Monnet scholarship holder.

References

Al Blooshi, B., & Eksteen, A. (2022). Cyber governance in the EU. In L. Martino & N. Gamal (Eds.), European cybersecurity in context: A policy-oriented comparative analysis (Techno Politics, Vol. 3, pp. 19–27). European Liberal Forum.

A/56/10 Report of the International Law Commission on the work of its fifty-third session (2001). Retrieved from https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf (Accessed 5 Aug 2024).

Akgül Açıkmeşe, S., & Dizdaroğlu, C. (2014). NATO-AB ilişkilerinde işbirliği ve çatışma dinamikleri. International Relations Journal, 10(40), 131–163. Retrieved from https://dergipark.org.tr/tr/pub/uidergisi/issue/39288/462652 (Accessed 1 Aug 2024).

Amerasinghe, C. F. (2008). The Bosnia Genocide Case. Leiden Journal of International Law, 21(2), 411–428. https://doi.org/10.1017/S0922156508005001 (Accessed 7 Aug 2024).

Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence (2024). Retrieved from https://www.eeas.europa.eu/sites/default/files/documents/2024/Strategic Compass_2ndYear_ Report_0.pdf(Accessed 31 Jul 2024).

Baezner, M., & Robin, P. (2018). Cyber sovereignty. Cyberdefense Trend Analysis, Center for Security Studies (CSS), ETH Zürich.

Banks, W. (2021). Cyber attribution and state responsibility. International Law Studies, 97, 1039–1068.
Bergamasco, F., Cassar, R., Popova, R., & Scott, B. I. (2020). Cybersecurity: Key legal considerations for the aviation and space sectors (Ch. 4). Kluwer Law International.
Brand, R. A. (2002). Sovereignty: The state, individual, and the international legal system in the twenty-first century. Hastings International and Comparative Law Review, 25, 279–301. Retrieved from https://scholarship.law.pitt.edu/fac_articles/39 (Accessed 2 Aug 2024).
Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor. JCMS, 55(6), 1254–1272.
Cavelty, M. D., & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. St Antony's International Review, 15(1), 37–57.
Challenges to Effective EU Cybersecurity Policy (2019). Briefing Paper, European Court of Auditors. Retrieved from https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf (Accessed 28 Jul 2024).
Choucri, N. (2012). Cyberpolitics in international relations. MIT Press.
Crawford, J. (2013). Direction or control by the state. In State responsibility: The general part (pp. 141–165). Cambridge University Press
Compact Committee of the Supreme Institutions of the EU (2020). Supreme audit institution reports relating to cybersecurity 2014-2020. Retrieved from https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EN.pdf (Accessed 29 Jul 2024).
Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008L0114 (Accessed 26 Jul 2024).
Crawford, J. (2013). Direction or control by the state. In State responsibility: The general part (pp. 141–165). Cambridge University Press.
Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj (Accessed 27 Jul 2024).
Directive 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022L2555 (Accessed 27 Jul 2024).
Fidler, D. P. (2022). Cybersecurity law. Edward Elgar Publishing.
Erkiner, H. H., & Kavak, M. H. (2022). Uluslararası sorumluluk hukukunda devletlerarası zararlara yönelik tazminatın belirlenmesi. Yıldırım Beyazıt Law Review (YBHD), 1, 1–30.
European Cybercrime Center (2024). Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Accessed 28 Jul 2024).
Geiss, R., & Melzer, N. (2021). The Oxford handbook of the international law of global security. Oxford University Press.
Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), Cyberpower and national security. National Defense University Press.
Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European Union and NATO global cybersecurity challenges: A way forward. Prism, 6(2), 126–141. Retrieved from https://www.jstor.org/stable/26470452 (Accessed 31 Jul 2024).
Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and insights. Georgetown Journal of International Law, 48, 735–760. https://ssrn.com/abstract=2932110 (Accessed 3 Aug 2024).
Kasper, A., & Vernygora, V. (2021). The EU's cybersecurity: A strategic narrative of a cyber power or a confusing policy for a local common market? Deusto Journal of European Studies, 65, 29–71. https://doi.org/10.18543/ced-65-2021pp29-71 (Accessed 26 Jul 2024).
Kutlu, F. B. (2023). A new field between two old allies: Cybersecurity approaches of EU and NATO (2016–2020). Journal of Diplomatic Research, 5(1).

Lété, B., & Pernik, P. (2017). EU–NATO cybersecurity and defence cooperation: From common threats to common solutions. Policy Brief No. 38, The German Marshall Fund of the United States.
Lloyd, H. A. (1991). Sovereignty: Bodin, Hobbes, Rousseau. Revue Internationale de Philosophie, 45(179), 353–379.
Papakonstantinou, V. (2022). The need to introduce a new individual right to cybersecurity. In L. Martino & N. Gamal (Eds.), European cybersecurity in context: A policy-oriented comparative analysis (Techno-Politics Series, Vol. 3, pp. 77–83). https://doi.org/10.53121/ELFTPS3 (Accessed 27 Jul 2024).
Pirim, Z. C. (2020). Uluslararası sorumluluk hukukunda devletlerin ağırlaştırılmış sorumluluğu: Kuramsal bir değerlendirme. Public and Private International Law Bulletin, 32(2), 147–182.
Poli, S., & Sommario, E. (2023). The rationale and the perils of failing to invoke state responsibility for cyber-attacks: The case of the EU cyber sanctions. German Law Journal, 24, 522–536. https://doi.org/10.1017/glj.2023.25 (Accessed 7 Aug 2024).
Rogozińska, A. (2021). Theoretical aspect of modern security threats definition, typologies, evolution. Scientific Journal of the Military University of Land Forces, 53(1), 199.
Rosenau, J. N. (1992). Governance, order, and change in world politics. In J. N. Rosenau & E.-O. Czempiel (Eds.), Governance without government: Order and change in world politics (pp. 1–29). Cambridge University Press.
Shaw, M. N. (2021). International law (9th ed.). Cambridge University Press.
Snyman-Ferreira, M. P. (2006). The evolution of state sovereignty: A historical overview. Fundamina, 12(2), 1–28.
Schmitt, M. N. (2017). State responsibility. In Tallinn Manual 2.0 on the international law applicable to cyber operations (p. 29). Cambridge University Press. https://doi.org/10.1017/9781316822524 (Accessed 5 Aug 2024).
Ştefănescu, D.-C., & Papoi, A. (2020). New threats to the national security of states: Cyber threat. Scientific Journal of Silesian University of Technology, Series Transport, 107, 177–182.
Steger, M. B. (2013). Globalization: A very short introduction. Oxford University Press.
Şafak, E. (2020). Uluslararası hukukta değişen güvenlik algısı ve saldırı suçu bağlamında siber saldırılar. Selçuk Law Review (SÜHFD), 28(1), 127–160.
Tardy, T., & Lindstrom, G. (2019). The scope of EU-NATO cooperation. NATO Defense College. Retrieved from http://www.jstor.org/stable/resrep19964.6 (Accessed 30 Jul 2024).
Toje, A. (2010). The European Union as a small power. JCMS: Journal of Common Market Studies, 49(1), 43–60.
Tsagourias, N., & Buchan, R. (2015). Research handbook on international law and cyberspace. Edward Elgar Publishing.
Tsagourias, N. (2016). Non-state actors, ungoverned spaces and international responsibility for cyber acts. Journal of Conflict & Security Law, 21(3), 465–488. https://doi.org/10.1093/jcsl/krw020 (Accessed 8 Aug 2024).
Wessel, R. A., & Larik, J. (2020). EU external relations law (2nd ed.). Hart Publishing.
Wessel, R. A., & Odermatt, J. (2019). Research handbook on the European Union and international organizations.Edward Elgar Publishing.
Wu, J., Li, J., & Ji, X. (2018). Security for cyberspace: Challenges and opportunities. Frontiers of Information Technology & Electronic Engineering, 19(12), 1459–1461. https://doi.org/10.1631/FITEE.1840000 (Accessed 18 Jul 2024).