

SECURITIZING SABOTAGE IN THE EUROPEAN UNION'S SECURITY STRATEGY: INSTITUTIONAL TRANSFORMATION FROM COUNTER-TERRORISM TO HYBRID THREATS

Selçuk KÖMCÜ (Ph.D. Student)* 

Asst. Prof. Alptekin MOLLA (Ph.D.)** 

ABSTRACT

This study analyzes how sabotage is defined, positioned, and addressed within the European Union's (EU) security strategies through the lens of securitization theory. Unlike classical terrorism, sabotage is framed as an existential security threat, particularly targeting critical infrastructure, digital systems, and hybrid threats. Distinct from cyber-terrorism, which is ideologically driven, sabotage focuses on systematic infrastructure disruption, necessitating a multi-layered security regime involving institutions such as Europol, European Network and Information Security Agency (ENISA), and the Hybrid Fusion Cell. The study examines key EU documents, including the 2005 Counter-Terrorism Strategy, the European Programme for Critical Infrastructure Protection (EPCIP), and ENISA reports, alongside case studies such as the 2022 Nord Stream pipeline sabotage, attacks on France's energy infrastructure, and cyber-sabotage campaigns during the Russia-Ukraine war. Findings indicate that while the EU has developed an advanced institutional framework to counter sabotage, challenges persist due to national sovereignty issues, limited intelligence sharing, and gaps in democratic oversight. Recommendations include enhanced intelligence coordination, AI-based early warning systems, mandatory private sector compliance, and reforms focused on human rights.

Keywords: EU, Sabotage, Fight Against Terrorism, Hybrid Threats, Securitization.

Jel Codes: F50, F52, F53.

* Bandırma Onyedi Eylül University, Graduate School of Education, Department of International Relations, E-mail: selcukkomecu@gmail.com

** Bandırma Onyedi Eylül University, Faculty of Economics and Administrative Sciences, Department of International Relations, E-mail: amolla@bandirma.edu.tr

Makale Geçmişi/Article History

Başvuru Tarihi / Date of Application : 25 Ekim / October 2025

Düzeltilme Tarihi / Revision Date : 20 Kasım / November 2025

Kabul Tarihi / Acceptance Date : 1 Aralık / December 2025

1. INTRODUCTION

One of the fundamental functions of states is to ensure national security. Establishing security has become increasingly complex, particularly in recent decades, due to evolving threat perceptions and the rise of asymmetric threats. While terrorism remains one of the most prominent elements of this complex threat landscape, acts of sabotage have emerged as an increasingly significant method of terrorism. Sabotage has become central to modern security policies, not only because of its potential to damage physical infrastructure but also due to its impact on information systems, public services, and social psychology (Galtung, 1990; Waldmann, 2005). In this context, the EU is restructuring its security strategy to address not only traditional terrorist threats but also acts of sabotage targeting infrastructure, information systems, and economic structures. Unlike cyberterrorism, sabotage focuses on systematic disruption of infrastructure and prioritizes operational disruption over ideological violence. This has necessitated the development of distinct management mechanisms within the EU, involving agencies such as Europol (terrorism-related sabotage) and European Network and Information Security Agency (ENISA) for cyber sabotage.

The study analyzes this transformation within the framework of securitization theory, examining the role of sabotage in the EU's security architecture and its institutional and legal implications. Cases such as the sabotage of the Nord Stream pipeline (2022), physical attacks on energy infrastructure in France, and cyber-sabotage attempts related to the Ukrainian War are examined to assess how these threats are constructed and the EU's capacity to respond. The study argues that sabotage is not merely a technical issue but also a strategic challenge to the EU's political integration, democratic oversight, and the protection of human rights.

2. RESEARCH DESIGN

2.1. Research Question

The central research question of this study is how acts of sabotage are defined within the EU's counter-terrorism strategies, the contexts in which they are situated, and the preventive mechanisms developed to address these threats. Sabotage is framed as an existential security issue within EU security policies, distinct from classical terrorism, particularly concerning critical infrastructures, cyber systems, and hybrid threats (Borchert & Pankratz, 2004). Moreover, within the EU's security strategy framework, acts of sabotage are assessed through a holistic, multi-layered approach, especially in areas such as critical infrastructure protection, cybersecurity, energy supply security, and countering hybrid threats. This study aims to understand how sabotage is constructed as a threat at both conceptual and operational levels and how this construction is reflected in the EU's institutional and legal frameworks. It also examines the distinctions between sabotage and cyberterrorism—focusing on system disruption versus ideological violence—and how the EU operationalizes this threat (e.g., through the roles of ENISA and Europol), analyzing the impact of securitization processes on institutional transformation.

2.2. Purpose and Empirical Scope of the Research

This study aims to analyze the EU's approach to sabotage within its counter-terrorism strategies by examining institutional and policy documents. In this context, the role of sabotage within the EU security architecture is explored from both conceptual and practical perspectives. Sabotage has been reconceptualized within the EU's security framework, distinguishing it from classical terrorism, particularly in areas such as the protection of critical infrastructure, cybersecurity, energy supply security, and the fight against hybrid threats. The study seeks to assess how this reconceptualization has influenced the EU's institutional transformation and security policies, focusing on the roles of institutions such as Europol, ENISA, EU Intelligence and Situational Awareness Centre (INTCEN), and the Hybrid Fusion Cell. The empirical scope includes the EU's core normative documents and case studies. The review process draws on key sources such as the Council of Europe's 2005 Strategy (European Council, 2005), the 2009 Security Strategy (Council of the EU. General Secretariat of the Council., 2009), technical reports published by the ENISA, sectoral security initiatives like the European Programme for the Protection of Critical Infrastructure (EPCIP), and strategic documents based on NATO-EU cooperation. These documents systematically illustrate how the EU defines sabotage, the threat categories under which it is classified, and the preventive or intervention mechanisms developed in response.

2.3. Method

This study employs documentary review and case analysis techniques within the framework of qualitative research methods. The research is classified as a "disciplined-configurative case study" according to Lijphart's typology. By structuring the cases within the framework of securitization theory, this approach aims to derive conclusions that extend beyond individual instances and offer broader analytical insights (Lijphart, 1971). These methods were selected because they facilitate a multi-layered analysis of the EU's counter-sabotage strategies through both normative documents and practical applications. Documentary review was used to uncover the EU's security priorities and structural transformations by examining institutional sources such as strategy documents, legal regulations, and policy reports. The case study method was employed to evaluate the real-world implications of the strategies outlined in these documents; cases such as the Nord Stream pipeline sabotage, attacks on energy infrastructure in France, and cyber sabotage in Ukraine were analyzed (Yin, 2009). This approach enables the examination of both the discursive and operational impacts of security policies. Furthermore, securitization theory, which forms the theoretical foundation of the study, provides an appropriate framework for analyzing how these threats are constructed as "existential" security issues (Buzan et al., 2013). Critical security studies, meanwhile, offer a complementary perspective for assessing the impact of this process on rights and freedoms.

2.4. Theoretical Framework

This study examines the EU's security policies concerning acts of sabotage, grounding its theoretical framework in securitization theory. Developed by Barry Buzan, Ole Wæver, and Jaap de Wilde within the Copenhagen School, securitization theory posits that the designation of a phenomenon as a "security issue" depends less on its objective characteristics and more on its discursive framing as an "existential threat" by political actors, coupled with public acceptance of this framing (Buzan et al., 2013). This process aligns with J.L. Austin's concept of illocutionary acts, wherein an actor's discourse persuades a specific audience of the threat's seriousness, thereby prompting political and operational responses (Austin, 1962). Once securitization is achieved, legal, political, or administrative measures that would otherwise be unacceptable become legitimate. Consequently, security is understood not only as a military and physical concern but also as a process of political and discursive construction.

The securitization process encompasses physical (e.g., Nord Stream pipeline attacks), cyber (e.g., cyber attacks during the Ukraine War), and hybrid (e.g., disinformation campaigns concurrent with infrastructure attacks in France) dimensions of sabotage. However, this process is also examined from a critical perspective. Balzacq (2011) argues that securitization is shaped not only by discourse but also by contextual and institutional practices (Balzacq, 2011). Therefore, the EU's sabotage policies are analyzed through a combination of discourse (e.g., the Commission's emphasis on the “existential importance of critical infrastructures”) and practices (e.g., the EPCIP guidelines), and by engaging with the literature on hybrid threats (e.g., Hybrid CoE, 2023) to illuminate the multidimensional nature of sabotage—cyber, physical, and psychological—and the integrated manner in which the EU addresses these threats..This framework provides an analytical perspective for understanding the role of sabotage within the EU security architecture and its institutional transformation.

In the context of the EU, acts of sabotage are regarded not only as technical or operational threats but also as existential challenges that jeopardize the integrity of the democratic order, economic stability, and societal security. Threats to energy infrastructure, digital systems, and transportation networks, in particular, are identified in EU security documents as risks not only to public order but also to the political continuity of European integration (European Council, 2005). Consequently, the securitization of acts of sabotage plays a critical role in legitimizing supranational decision-making mechanisms and in aligning the private sector and member states with shared security priorities.

In the Turkish literature on this issue, Sinem Akgül-Açıkmeşe has examined the EU's foreign and security policies through the lens of securitization theory, demonstrating in detail how the EU legitimizes extraordinary measures through discursive strategies, particularly in areas such as migration, border management, and counterterrorism (2015). Similarly, this study employs securitization theory as the primary theoretical framework to analyze how acts of sabotage are defined at the EU level, as well as the institutional and legal implications of this definition.

Finally, the study adopts a critical security studies perspective to address long-standing critiques regarding the securitization of freedoms and rights. In this context, the analysis examines how cyber sabotage and digital surveillance shape democratic oversight, individual privacy, and freedom of expression (Balzacq, 2011).

2.5. Importance of Research

The EU's (EU) counterterrorism strategies have evolved rapidly since the 2000s and have become a prominent area of academic interest. This body of literature addresses topics such as the transformation of the EU's security architecture, intelligence sharing, inter-institutional cooperation, and external threat perception (Bures, 2006; Kaunert, 2009; Monar, 2015). Sinem Akgül-Açıkmeşe (2015, 2023) provides an important contribution by examining EU foreign and security policies through discursive strategies within the framework of securitization theory.

However, studies with systematic and theoretical depth specifically addressing sabotage remain quite limited. In the literature, sabotage is often treated as a technical issue within the broader context of cybersecurity or is indirectly incorporated into discussions of critical infrastructure security. For example, Carrapico and Barrinha analyze the EU's cybersecurity policy in terms of institutional integrity and inter-actor cohesion but address the threat of sabotage only at the digital level (Carrapico & Barrinha, 2017). Similarly, Christou focuses on the principles of "flexibility" and "adaptability" in the EU's cybersecurity governance but does not directly explore the intersection of sabotage and terrorism (Christou, 2016).

To address this gap in the existing literature, this study analyzes, both theoretically and through the use of case studies, how the EU defines, securitizes, and attempts to manage acts of sabotage. It examines how sabotage is constructed as an "existential threat" through securitization theory and evaluates the institutional implications of this discourse using contemporary cases such as the Nord Stream attack.

In this context, the study views sabotage not merely as a technical or sector-specific issue but as a multidimensional security threat central to the EU's counter-terrorism strategy. It provides a theoretical and practical framework for evaluating the balance among security, politics, and rights.

2.6. The Role of Sabotage in EU Security Policies

The EU's counter-terrorism strategy addresses sabotage as a security issue encompassing both traditional and cyber threats. EPCIP, in particular, has identified the protection of infrastructure in sectors such as energy, water, transport, and communications as a priority (European Commission, 2006). In this context, acts of sabotage are not only criminal offenses but also systematic threats to collective security.

In recent years, the digital aspect of sabotage, specifically cyber sabotage, has gained prominence. The EU Cyber Security Strategy (2025) calls for coordinated action among member states to address cyber sabotage threats, with institutions such as ENISA playing a central role (ENISA, 2025). These strategies aim not only to prevent attacks but also to enhance post-incident response capabilities.

Sabotage is a multifaceted threat central to the EU's counter-terrorism strategy. A wide range of policies—ranging from ensuring the physical security of critical infrastructure to protecting digital networks from cyber attacks, as well as intelligence cooperation and legal regulations—have been developed to address this threat. This multilayered approach elevates the role of sabotage in EU security policies from a merely technical issue to a strategic one, with significant implications for political integration, economic stability, and social trust. This study examines these institutional distinctions and the impact of the securitization of sabotage on the EU's security architecture in detail through case studies. However, democratic oversight of these policies, their compatibility with human rights, and the capacity for coordination among member states remain contentious. In this context, the following sections of the study will provide an in-depth analysis of counter-sabotage strategies specific to the EU.

3. CONCEPTUAL FRAMEWORK

3.1. Definition of the Concept of Sabotage

The concept of sabotage has a multifaceted historical and functional context. The term originates from the French word "sabot" (wooden shoe) and was first used in the 19th century to describe workers deliberately damaging machinery (Carlisle, 2004). In its modern sense, sabotage refers to any intentional action taken to disrupt or damage the functioning of an organization, system, or infrastructure. Such actions can occur at physical, digital, psychological, or economic levels.

In the context of the EU, sabotage is specifically addressed through threats to critical infrastructures such as energy, water, transportation, communications, and information systems. EPCIP, adopted by the EU in 2006, defines sabotage as "deliberate interference targeting the continuity of critical services." Furthermore, preventing such acts is considered not only within the scope of criminal law but also as part of protecting collective security, necessitating the development of multi-actor strategies (European Commission, 2006).

In this context, sabotage is not merely an operational threat but also the subject of a political and institutional construction process. When analyzed through the lens of securitization theory, acts of sabotage are elevated from technical issues to the status of "existential threats" through the discourse of political actors (Buzan et al., 2013). This framing of the threat legitimizes extraordinary security measures and broadens the crisis management capabilities of the state or supranational entities. The EU's characterization of sabotage as a systemic threat linked to terrorism exemplifies this securitization process.

3.2. Types of Sabotage

Sabotage actions can be categorized into different types based on their target, method, motivation, and impact. One major type is physical sabotage, which occurs through direct attacks on tangible infrastructure such as industrial facilities, transportation networks, and power plants; for example, attempts to explode natural gas pipelines fall into this category (Waldmann, 2005). Another significant form is cyber sabotage, which targets information systems to disrupt critical services or compromise data integrity; the EU Cyber Security Strategy identifies these attacks as “elevated priority threats” (ENISA, 2025). A third category is psychological or information sabotage, involving the manipulation of information systems or media platforms to mislead the public, erode trust in institutions, or generate a sense of crisis and instability (Neocleous, 2022). Finally, economic sabotage focuses on undermining macroeconomic stability by disrupting financial systems or production chains, and the EU includes such actions within the broader framework of hybrid threats (Olech, 2025).

3.3. Differences and Overlaps Between Sabotage and Terrorism

Sabotage often shares characteristics with terrorism, as both involve violence, fear, and asymmetry. However, there are important distinctions between the two. The primary goal of terrorism is to influence large populations and achieve political objectives in the name of an ideology (Buzan et al., 2013). In contrast, sabotage is typically a more technical, systematic, and operational form of action.

According to Waldmann (2005), acts of sabotage are often covert and reveal their effects gradually rather than immediately. In contrast, terrorist acts involve overt violence intended to attract public attention. However, sabotage targeting critical infrastructure, such as energy systems, causes both direct damage and influences public opinion by instilling fear. Sabotage can have widespread effects only through the disruption of infrastructure, public services, or economic processes. Consequently, EU security documents classify acts of sabotage as "systemic threats with terrorist aims" (European Council, 2005).

From the perspective of securitization theory, this overlap is crucial. Associating acts of sabotage with terrorism makes these threats vulnerable not only to security forces but also to extraordinary interventions in legal, intelligence, and public policy domains (Buzan et al., 2013). Thus, sabotage is incorporated into security discourse as an existential threat not only to physical infrastructure but also to the continuity of political order and public authority.

3.4. Critical Infrastructure and Security Perception

The EU addresses the concept of sabotage within the framework of critical infrastructure security (European Commission, 2006). According to the EPCIP program, critical infrastructure comprises "assets and systems that are indispensable to the health, security, economy, or public order of a state or

society." Therefore, sabotage represents not only a physical threat but also a challenge to the integrity and stability of societal functioning.

This approach is directly related to the EU's securitization strategies. According to Buzan et al. (2013), when an issue is defined as a "security issue," it becomes possible to legitimize extraordinary measures. By framing acts of sabotage in this manner, the EU justifies the use of extraordinary powers in both border security and intelligence sharing.

3.5. The Position of Sabotage in the European Security Strategy

The 2005 EU Counter-Terrorism Strategy treats sabotage as a deliberate act directly linked to terrorism, addressing its prevention explicitly under the "Protect" pillar and outlining measures for safeguarding critical infrastructures (European Council, 2005). By contrast, the 2009 European Security Strategy does not identify sabotage as a standalone threat; instead, it subsumes sabotage-related risks under broader categories such as cyber attacks, energy security, and the protection of critical infrastructures, all framed as "asymmetric threats" (Council of the EU, 2009). This shift indicates that, by 2009, sabotage is conceptualized less as an intentional, discrete act and more as part of wider systemic vulnerabilities affecting the EU's security environment.

For example, under the heading "Protect," measures include the protection of critical infrastructure, securing energy supply chains, and monitoring public spaces. In contrast, the heading "Prevent" focuses on stopping radicalization processes and organizations through digital platforms.

Sabotage is not merely a technical or legal issue; it also constitutes a strategic security threat to the EU. This threat targets both digital systems and physical infrastructure, aiming to undermine the economic and psychological resilience of societies. The EU's approach to sabotage has evolved beyond traditional security perspectives into a systemic security doctrine.

4. THE EUROPEAN UNION'S COUNTER TERRORISM STRATEGY

With the transformation of the security environment following the Cold War, the EU has evolved from a mere economic union into a political actor developing common foreign and internal security policies. In this context, combating terrorism has become a key priority on the EU's internal security agenda (Monar, 2015). The evolution of the terrorist threat—extending beyond traditional acts of violence to include digital sabotage, hybrid threats, and attacks on critical infrastructure—has compelled the EU to develop a more comprehensive and multi-layered counterterrorism architecture.

4.1. The EU's Approach to the Fight Against Terrorism: Key Strategic Documents

The EU's most fundamental document in the fight against terrorism is the "EU Counter-Terrorism Strategy," published in 2005. This strategy is structured around four main objectives: prevent, protect, pursue, and respond (European Council, 2005). This four-pronged approach aims to address the root causes of terrorism and develop the capacity to respond quickly and effectively to incidents.

Subsequently, the 2009 "European Security Strategy" document defined the EU's approach to security, addressing terrorism alongside emerging threats such as weapons of mass destruction and failed states (Council of the EU. General Secretariat of the Council., 2009). The document emphasized that the EU must act as a global security actor and adopt a strategy that considers the security of not only its member states but also its neighboring regions.

These documents facilitated the development of a holistic security approach that was not only defense-focused but also incorporated diplomatic, economic, legal, and intelligence-based strategies (Bures, 2006).

4.2. Institutional Structure of The EU in the Fight Against Terrorism

The EU's counter-terrorism framework is supported not only by strategic documents but also by a robust institutional structure that ensures coordination, intelligence sharing, and operational efficiency across member states. Europol, serves as the primary agency coordinating police cooperation within the EU in the fight against terrorism. Through the European Counter-Terrorism Centre (ECTC), which began operations in 2013, Europol provides analytical and intelligence support on issues such as preventing terrorist financing, radicalization, and terrorist travel (Europol, 2025). Eurojust, the EU's judicial cooperation body, coordinates the work of judicial authorities across member states and plays an especially active role in terrorism-related criminal investigations with cross-border dimensions (Weyembergh & Brière, 2018). Frontex, the EU's border and coast guard agency, supports counter-terrorism efforts by managing the security of the Union's external borders and conducting risk analyses to prevent terrorist movements across frontiers (Carrera et al., 2018). Finally, INTCEN, operating within the European External Action Service (EEAS), functions as the EU's civilian intelligence analysis hub, producing strategic threat assessments and facilitating intelligence exchange among member states (Occhipinti, 2017). Together, these institutions enhance transnational cooperation and reinforce the EU's collective resilience and solidarity in combating terrorism.

4.3. Joint Intelligence and Threat Assessment Mechanisms

Information sharing in the fight against terrorism and intelligence cooperation are among the EU's top priorities. Following the 2004 Madrid and 2005 London attacks, the European Counter-Terrorism Coordinator was established. This coordinator oversees counter-terrorism policies, ensures coherence among national strategies, and publishes annual threat assessment reports (European Council, 2005).

SIENA (Secure Information Exchange Network Application) and the Terrorist Finance Tracking Programme (TFTP), developed within the EU, facilitate the rapid and secure sharing of sensitive data among member states (Monar, 2015).

4.4. Multi-Layered Approach and Hybrid Threats

The EU's counter-terrorism policy is founded on a multi-layered framework. This framework encompasses not only intergovernmental cooperation but also the private sector, local governments, and civil society actors. These stakeholders are encouraged to collaborate in combating acts of sabotage targeting critical infrastructure (Olech, 2025).

Furthermore, the EU recognizes that terrorist acts, when combined with other tactics such as cyber attacks, disinformation campaigns, and energy manipulation, constitute multifaceted threats encompassed by the concept of hybrid threats. Consequently, cybersecurity strategies and energy policies are implemented in an integrated manner alongside the counter-terrorism strategy (ENISA, 2025).

4.5. Evaluation: Strengths and Challenges

The EU's counter-terrorism strategy, shaped by its multi-level governance model, is particularly robust in several respects. Normative documents, such as the EPCIP, provide a comprehensive framework for systematically addressing sabotage within the context of hybrid threats. At the institutional level, the coordination efforts of Europol against terrorist-related sabotage, ENISA against cyber-sabotage threats, and the Hybrid Fusion Cell against hybrid threats demonstrate that the EU has established a multi-layered response capacity. Joint threat assessments, intelligence sharing, border security mechanisms, and coordination systems for the protection of critical infrastructure are among these strengths (Bossong, 2008).

However, member states' reluctance to share intelligence—stemming from concerns about national sovereignty, disparities in resource allocation, and weak democratic oversight mechanisms—stands out as a significant challenge (Kaunert, 2009). The EU's counter-sabotage strategy faces substantial structural and operational obstacles. Concerns over national sovereignty make member states hesitant to cooperate fully, especially in sensitive areas such as intelligence sharing and crisis management. For instance, reservations about intelligence sharing following the Nord Stream sabotage in 2022 delayed a coordinated response. Inequities in resource allocation, particularly the insufficient investment in cybersecurity infrastructure by smaller member states, impede the establishment of a comprehensive protection regime at the EU level. Additionally, the slow pace of legal harmonization and inconsistent implementation—such as the incomplete adoption of EPCIP guidelines by some member states—undermine the strategy's effectiveness. Collaboration with the private sector is essential, given that critical infrastructure is predominantly privately owned; however, the absence of mandatory legal harmonization and the influence of market-driven priorities limit this cooperation. These challenges obstruct the full integration of sabotage securitization at both institutional and normative levels. Overall, while the EU has developed an advanced institutional framework to combat sabotage, significant operational and normative challenges persist.

5. ADDRESSING SABOTAGE ACTS IN THE EU STRATEGY

The EU's counter-terrorism strategy addresses sabotage within the context of systematic, technical, and infrastructure-focused threats, distinguishing it from traditional terrorist acts. The EU's policies—particularly those designed to protect critical infrastructure, combat cyber sabotage, enhance energy security, and strengthen resilience against hybrid threats—demonstrate that sabotage is understood within a holistic security framework (Olech, 2025). This section will examine in detail how sabotage actions are structured along four fundamental axes within the EU strategy.

5.1. Protection of Critical Infrastructures

Critical infrastructures include energy, transportation, water, healthcare, and communication systems that are essential for the functioning and security of society. The European Commission has identified the protection of these infrastructures as a key priority in EU security policies. EPCIP, developed within this framework, provides a systematic security approach to guard against acts of sabotage (European Commission, 2006).

The primary objective of EPCIP is to classify critical infrastructure across the EU according to common definitions and to develop risk assessments, security protocols, public-private partnerships, and crisis management plans in these sectors. EPCIP provides binding guidelines not only for member states but also for cross-border infrastructure projects. In this context, natural gas pipelines, nuclear power plants, and integrated transport networks throughout Europe are considered priority targets for sabotage, and specific security measures are being developed for these areas (Bures, 2006).

The Critical Infrastructure Warning Information Network (CIWIN), established as a supplement to the EPCIP program, is a digital platform that enables member states to share information and experiences related to infrastructure security. CIWIN also functions as an early warning system against potential sabotage threats and enhances post-incident response capabilities (Bossong, 2008).

5.2. Cyber Sabotage and Digital Security

In the 21st century, with the rapid expansion of digitalization, a significant portion of sabotage threats has shifted to the cyber domain. These threats include disruptions to public institutions' internet systems, infiltration of energy management software, attacks on banking systems, and disinformation campaigns. The EU regards cyber sabotage not only as a technical issue but also as a strategic threat to national security (ENISA, 2025).

The EU's most comprehensive framework in this area is the European Cyber Security Strategy. Developed under the leadership of the ENISA, this strategy aims to strengthen the national cybersecurity capacities of member states, protect critical digital infrastructures, establish cyber incident response teams, and enhance civil-military cooperation (ENISA, 2025).

CERT-EU (Computer Emergency Response Team for the EU Institutions), established as part of the EU's cybersecurity strategy, analyzes cyber-sabotage attempts targeting EU institutions, recommends preventive measures, and responds immediately to incidents. Furthermore, the Network and Information Security (NIS) Directive regulates cyber incident reporting obligations, making information sharing mandatory between both the private sector and public institutions (Farrand & Carrapico, 2022).

5.3. Energy Security and Sabotage Threat

Energy supply security is a strategic priority for the EU. The EU's dependence on energy imports, combined with the transboundary nature of its energy resources, makes this sector a high-risk target for sabotage. Pipelines, LNG terminals, power plants, and nuclear facilities are particularly vulnerable to both physical and cyber attacks (Kuzemko et al., 2016).

The EU is implementing measures to counter this threat within the framework of its "Energy Security Strategy," including diversifying energy infrastructure, establishing alternative routes, and testing energy crisis scenarios. However, the significant involvement of private companies in controlling critical energy infrastructure leads to fragmentation in the implementation of security strategies and, in some cases, results in insufficient coordination (Scholten & Bosman, 2016).

The Nord Stream sabotage in 2022 is a notable example in this context. Although the perpetrator has not been definitively identified, the incident has raised awareness within the EU that sabotage of energy infrastructure must be taken seriously (Olech, 2025).

5.4. Hybrid Threats and Sabotage

The EU also considers acts of sabotage within the context of hybrid threats. Hybrid threats are multifaceted challenges that involve the simultaneous use of unconventional tools such as cyber attacks, disinformation, and economic pressure. In this context, sabotage has evolved into a strategy employed not only to cause physical damage but also to manipulate public opinion, create political instability, and influence foreign policy processes (NATO, 2024).

The EU has enhanced its institutional capacity to counter hybrid threats through the establishment of the Hybrid Fusion Cell in 2016 and the adoption of the EU Strategic Compass documents in 2021. These documents advocate for an integrated assessment of sabotage activities across various domains, including intelligence, communications, infrastructure, and foreign relations (European External Action Service, 2024).

6. INSTITUTIONAL TRANSFORMATION AND OPERATIONAL RESPONSE: CASE STUDIES

To evaluate the field-based response of the EU's strategic and institutional framework to acts of sabotage, relying solely on discursive documents and institutional structures is insufficient; it is also essential to demonstrate how these structures operate in real-world scenarios. In this regard, the case study method is vital both for testing the EU's practical responses to sabotage threats and for assessing the field-based applicability of theoretical approaches. As Yin (2009) emphasizes, case studies provide an effective means of understanding the practical limitations and capabilities of normative approaches, especially in complex and contextually rich security issues.

The three cases selected for this study—the Nord Stream pipeline sabotage (2022), physical attacks on energy infrastructure in France, and cyber-sabotage attempts targeting EU countries during the Ukrainian War—were deliberately chosen because they represent a variety of sabotage types, actor structures, and institutional response styles. Three key criteria guided the case selection:

Each case illustrates different forms of sabotage—the Nord Stream incident exemplifies a direct attack on cross-border physical infrastructure; the French case involves infrastructure-targeted actions by domestically based extremist groups; and the Ukrainian context highlights the impact of state-sponsored cyber attacks on Europe.

The selected cases have mobilized the EU's institutional capacity at multiple levels. The Nord Stream incident underscored NATO-EU coordination; the French example emphasized the integration of national security institutions with CIWIN and Europol; and the cyber sabotage during the Ukraine war highlighted mechanisms such as ENISA, CERT-EU, and the NIS Directive.

Taken together, all three cases illustrate how, within the framework of securitization theory, a situation is redefined as an existential threat, the policy instruments such a discourse legitimizes, the actors it mobilizes, and how these actors operate during moments of acute stress.

These examples are timely, highly impactful, and coincide with critical moments when vulnerabilities in EU security became evident. The Nord Stream sabotage highlighted energy dependency and infrastructure security issues at the forefront of the European agenda; the events in France demonstrated that threats to internal security are not exclusively external; and the cyber attacks in Ukraine illustrated how conventional defensive measures can be insufficient in the cyber domain.

Therefore, the selected cases provide a comprehensive overview, both in terms of analytical diversity and in assessing how EU strategies function under stress. This section will first introduce each case within its context, then analyze the EU's response, the operation of institutional mechanisms, and the resulting policy outcomes. It will examine the extent to which sabotage is not merely a theoretical threat but also its manageability during concrete moments of crisis.

6.1. Nord Stream Pipelines Sabotage (2022)

The Nord Stream 1 and 2 natural gas pipelines, which connect Germany and Russia through the Baltic Sea, were the sites of explosions. This incident, occurring amid a deepening energy crisis in Europe, had widespread repercussions not only economically but also in geopolitical and security terms. Investigations conducted by Sweden, Denmark, and Germany indicate that the incident was most likely an act of sabotage (Geropoulos, 2024).

EU Commission President Ursula von der Leyen described the incident as "a provocation of the highest order" and announced that measures to protect energy infrastructure would be strengthened. Following this event, the EU Energy Council convened an extraordinary meeting, and the security of energy infrastructure began to be addressed not only as an energy policy issue but also as a matter of common defense (Euronews, 2022).

The most significant outcome of this incident was the enhanced integration of civil-military cooperation and cyber-physical threat awareness into EU security strategies. Simultaneously, infrastructure security analyses conducted by the Hybrid Threats Centre, in coordination with NATO, were intensified in the Baltic and North Seas (European Commission, 2023).

From a securitization perspective, the Nord Stream sabotage illustrates how the EU frames attacks on its energy infrastructure as an existential threat. The Commission's rhetoric (the actor) aimed to persuade member states (the audiences) to adopt extraordinary measures. However, the effectiveness of this discourse was limited, and intelligence sharing remained inadequate due to concerns over national sovereignty. This case highlights shortcomings in the institutional integration of the EU's securitization processes.

Nord Stream incident, while underscoring the geopolitical implications of physical sabotage, prompted a broader international response—specifically NATO-EU cooperation—compared to other incidents. However, it is important to note that it offered less operational clarity than cases involving cyber sabotage.

6.2. Actions Concerning Electricity Infrastructure in France

Numerous electrical substations in France were deliberately damaged in 2020 and 2021. These incidents were interpreted as systematic sabotage attempts by certain radical groups, triggering security alerts at both the national and EU levels. The French Ministry of the Interior classified the attacks as "infrastructure terrorism" and analyzed the incidents in coordination with institutions such as Europol and INTCEN (European Parliament, 2021).

These incidents demonstrate that threats to the physical security of critical infrastructure can originate not only from external sources but also from domestic extremist groups. Under the EU's EPCIP program, France has revised its security protocols for energy infrastructure, and the French Internal Security Agency (DGSI) has enhanced information sharing with other member states through the EU-wide CIWIN network (Olech, 2025).

Furthermore, French judicial authorities have decided to investigate acts of sabotage under anti-terrorism laws. This decision is one of the rare instances that solidify the legal connection between sabotage and terrorism (Waldmann, 2005).

This case exemplifies the securitization of internal threats. The French authorities' rhetoric regarding "critical infrastructure security" has persuaded the public and EU institutions to adopt extraordinary measures, such as increased surveillance. However, this securitization is problematic due to its lack of democratic oversight. Additionally, the case highlights the limited central coordination within the EU in addressing internal threats.

Compared to the Nord Stream case, the French case has a more localized focus and involves fewer hybrid elements than cyber sabotage incidents. However, the perception of internal threats has underscored the tension between national security and EU security within the EU's securitization processes.

6.3. The Ukraine War and Cyber Sabotage Attempts Targeting EU Systems

The Russia-Ukraine war, which began in 2022, has significantly increased cyber threats to the EU. In the early months of the conflict, coordinated cyber-sabotage attacks targeted public institutions, banks, and media outlets in EU member states (EUA Agency for Cybersecurity, 2022). Most of these attacks involved Distributed Denial of Service (DDoS), data exfiltration, and email chain attacks.

ENISA identified state-sponsored actors as the source of the attacks and announced that the CERT-EU and NIS Directive mechanisms, within the framework of the European Cyber Security Strategy, had been activated in response. Critical public services were temporarily disabled in countries such as Poland, Estonia, and Lithuania, while data breaches occurred in Germany and Italy (Farrand & Carrapico, 2022).

The EU's response was twofold. In the first stage, crisis management systems were activated, and cyber incident reporting was accelerated. In the second stage, joint cyber defense exercises and hybrid threat scenarios were conducted in collaboration with NATO. These cases demonstrate that cyber sabotage affects not only IT systems but also social psychology and public order, indicating that these areas are being targeted (Olech, 2025).

This case exemplifies the securitization of hybrid threats. The EU's rhetoric on "cyber resilience" has persuaded member states and the public to invest in cyber defense. However, the effectiveness of this rhetoric has been constrained by the limited capacity of some member states. This case clearly highlights the need to integrate hybrid threats into the EU's security architecture.

Compared to the Nord Stream and French cases, this case stood out due to its cyber and hybrid dimensions. The EU's institutional response to cyber sabotage was more advanced; however, the issue of national capacity gaps persisted.

6.4. Comparative Assessment

These three cases illustrate the practical implications of the strategic framework developed by the EU to counter the threat of sabotage. The Nord Stream incident revealed the vulnerability of energy infrastructure and underscored the necessity of NATO-EU cooperation. The events in France emphasized the severity of domestic threats and the critical importance of infrastructure security policies at the local level. Meanwhile, the war in Ukraine highlighted the borderless nature of cyber sabotage and the urgent need to develop comprehensive nationwide cyber defense strategies.

Nord Stream incident demonstrated that addressing geopolitical and physical sabotage requires international coordination between NATO and the EU. The French case highlighted the national-EU tensions related to internal threats, while the Ukraine case revealed the challenges of integrating cyber and hybrid threat responses.

Common to all three cases is that the EU's institutional response can be mobilized quickly; however, implementation is hindered by differences at the national level. This is a direct consequence of the EU security structure being based on a multi-level, consensus-driven governance model rather than a federal one (Bossong, 2008).

In terms of securitization, the Commission's rhetoric regarding Nord Stream received the strongest acceptance. However, deficiencies in intelligence sharing are a common issue across all cases. Theoretically, these cases confirm that the success of securitization depends on the relationship between the actor and the audience, as well as institutional capacity.

In today's world, where sabotage threats are becoming increasingly complex, it is imperative for the EU to develop not only technological solutions but also political and social cohesion strategies.

7. CRITICAL ANALYSIS

The EU's security strategies addressing sabotage have undergone a significant transformation in institutional capacity, normative frameworks, and practical implementation. Policy instruments such as EPCIP, ENISA, the NIS Directive, and hybrid threat documents have reframed sabotage as a strategic threat encompassing geopolitical, cyber, and societal dimensions, rather than merely a technical risk (Bures, 2006). However, despite this multi-layered security model, the EU continues to face several structural challenges related to both institutional coordination and democratic legitimacy. This section evaluates the strengths and weaknesses of this strategy, drawing on relevant theoretical perspectives.

7.1. Limits of Institutional Coordination

The EU's counter-sabotage strategy depends on the collaborative efforts of multiple institutions. Organizations such as Europol, Eurojust, Frontex, ENISA, and INTCEN perform security functions at various levels. However, this multi-actor structure does not always guarantee effective coordination. Challenges include member states' failure to fully integrate their national security policies at the EU level, reluctance to share information, and conflicts of authority between institutions (Kaunert, 2009; Monar, 2015).

INTCEN's mandate, especially concerning intelligence sharing, is limited, and national intelligence agencies are reluctant to share data due to concerns over sovereignty (Occhipinti, 2017). This reluctance adversely affects the early detection and rapid response capabilities for sabotage risks to critical infrastructure.

7.2. The Problem of Securitization and Democratic Control

The EU's classification of sabotage as a terrorism-related security issue aligns with securitization theory. According to Buzan et al. (2013), when an issue is framed within the security domain, extraordinary measures become legitimate. Within this framework, EPCIP, the NIS Directive, and hybrid threat strategies have expanded security regimes by employing the language of "existential threat."

However, this process also raises concerns regarding democratic oversight. Data monitoring and early warning systems, especially those designed to counter cyber sabotage, may conflict with individuals' right to privacy and the principles of personal data protection (Farrand & Carrapico, 2022). The European Data Protection Supervisor (EDPS) has noted that certain ENISA policies inadequately address human rights issues (Neocleous, 2022).

In this context, the search for a balance between security and freedom has become an increasingly prominent dilemma in the EU's anti-sabotage policies. While technological solutions to the threat of sabotage are being developed, further efforts are needed to ensure the democratic legitimacy and oversight of these tools.

7.3. National Sovereignty and Harmony Issues

The effectiveness of the EU's anti-sabotage security strategy largely depends on the compliance of member states with its implementation. However, the perception of sabotage threats varies across member states. For instance, the Baltic states prioritize sabotage threats from Russia, whereas Western European countries view domestic extremism as the primary concern (Olech, 2025).

These differences make it difficult to agree on common minimum standards for strategy implementation and limit the applicability of policy instruments developed at the EU level (Bossong, 2008). This is particularly evident in the fact that national action plans envisioned by ENISA to combat cyber sabotage risks remain unimplemented in some countries.

7.4. Collaboration with the Private Sector and Security Vulnerabilities

In Europe, a substantial portion of critical infrastructure in sectors such as energy, transportation, and communications is controlled by the private sector. This underscores the need for a multi-stakeholder approach to managing sabotage risks. However, the private sector cannot always implement security strategies due to several constraints. High security investment costs, the need to protect trade secrets, and a lack of institutional transparency hinder effective collaboration with private entities (Scholten & Bosman, 2016).

This issue became more pronounced following the electrical sabotage in France and the Nord Stream attack. In response, the European Commission issued recommendations in 2023 mandating crisis scenarios and joint exercises with the private sector. However, these weakly binding recommendations have had limited practical impact.

7.5. Lack of Strategic Alignment in Addressing Hybrid Threats

Hybrid threats are not limited to sabotage actions involving physical or digital attacks; they also encompass economic and social dimensions and are defined as multidimensional operations supported by political instruments. The EU has developed significant awareness in this area through its 2022 Strategic Compass document (European External Action Service, 2024). However, a comprehensive strategy to combat hybrid threats has not yet been fully implemented at the institutional level.

Particularly in cases where cyber sabotage and disinformation campaigns occur simultaneously, the response of EU institutions is often fragmented. Cybersecurity falls under ENISA, media monitoring under ERGA, and counter-disinformation under the External Affairs Service. This fragmented structure makes it difficult to provide a rapid and integrated response to hybrid attacks (European Commission, n.d.).

7.6. Alternative Approaches and the Need for Reform

Despite existing challenges, several key areas for reform stand out to enhance the EU's capacity to combat sabotage more effectively.

Joint Intelligence Mechanism: The capacity of INTCEN should be enhanced to ensure trust-based information sharing with national intelligence institutions (Occhipinti, 2017).

Democratic Oversight Mechanisms: The European Parliament's oversight powers over institutions such as ENISA, Frontex, and Europol should be strengthened.

Mandatory Compliance in the Private Sector: Legal regulations requiring the implementation of security protocols in critical infrastructures should be established, with sanctions applied for non-compliance.

Hybrid Threat Centralization: An integrated institution that evaluates cyber, economic, and psychological sabotage under a single framework should be established.

8. CONCLUSION AND RECOMMENDATIONS

Since the early 2000s, the EU has expanded its concept of security beyond border protection and combating traditional terrorism to include acts of sabotage, cyber attacks, threats to critical infrastructure, and hybrid threats. This concept has been redefined within a multidimensional framework. Consequently, institutional capacity in the security sector has grown, strategic documents have diversified, and intelligence-sharing and crisis management systems have been restructured (Bures, 2006; Olech, 2025). However, despite these structural advancements, the EU's measures against sabotage have had limited effectiveness due to factors such as lack of coordination, challenges in democratic oversight, and inconsistencies in implementation.

Within the framework of securitization theory, the EU's framing of sabotage as an existential threat has legitimized extraordinary measures, such as cyber defense exercises and investments in energy infrastructure. However, this process poses risks to democratic oversight and human rights. The study reveals that the EU has developed an advanced institutional framework to combat sabotage but faces both operational and normative challenges. Inadequate cyber defense capacity in smaller member states and insufficient cooperation with the private sector undermine the strategy's effectiveness.

The main findings of this study are summarized as follows:

- **Comprehensive Institutional Structure:** The EU has established numerous institutional bodies to counter acts of sabotage, including Europol, ENISA, INTCEN, Frontex, and Eurojust. These institutions evaluate sabotage in the context of both internal and external security and develop policies aligned with strategic documents (ENISA, 2025; European Council, 2005).

· **Critical Infrastructure-Focused Approach:** Infrastructure security has been prioritized in sectors such as energy, transportation, healthcare, and communications through programs like EPCIP and CIWIN. Sabotage is recognized as a multifaceted threat to these infrastructures, with all stakeholders, including the private sector, assigned specific roles (European Commission, 2006).

· **Emphasis on Cyber Security:** With increasing digitalization, cyber sabotage has become a prominent concern. Preventive and intervention mechanisms to counter these threats have been developed, utilizing tools such as ENISA, CERT-EU, and the NIS Directives (Farrand & Carrapico, 2022).

· **Awareness of Hybrid Threats:** The simultaneous evolution of threats such as disinformation, energy crises, and cyber attacks has demonstrated that sabotage strategies can no longer be managed using traditional security approaches. The EU has integrated this awareness into its policy documents through frameworks such as the Strategic Compass and the Hybrid Fusion Cell (European External Action Service, 2024).

· **Implementation Gap:** While these strategic documents and institutional structures function effectively in some member states, they remain largely nominal in others. Additionally, challenges to intelligence sharing arising from concerns over national sovereignty limit the effectiveness of early warning systems (Kaunert, 2009).

To develop a more effective, flexible, and inclusive security framework against acts of sabotage, the EU should consider the following recommendations:

INTCEN's institutional authority should be expanded to establish a structure that integrates both civilian and military intelligence analysis while fostering trust-based data sharing among member countries. This structure must also be sufficiently flexible to transform into a joint operations center during times of crisis (Occhipinti, 2017).

AI-powered attack recognition algorithms should be integrated throughout the EU under the coordination of ENISA. Detection times for attacks should be reduced, and alerts should be delivered to public institutions in real time and in multiple languages (ENISA, 2025).

Compliance with minimum security standards should be mandatory in contracts with infrastructure providers. Administrative sanctions must be imposed in cases of non-compliance, and EU-level oversight mechanisms should be established for high-risk sectors (Scholten & Bosman, 2016).

Individuals' rights to privacy, freedom of expression, and digital rights must be respected when addressing the threat of sabotage. Institutions such as ENISA and Europol should be mandated to conduct human rights impact assessments of their activities. EDPS should play an active role in overseeing this process (Neocleous, 2022).

European Hybrid Threat Analysis Center should be established to provide integrated analyses of cyber attacks, disinformation, economic sabotage, and social manipulation. This center should operate in coordination with NATO and the United Nations and serve as a rapid decision-making mechanism during times of crisis. The Hybrid CoE can be considered a step toward achieving this goal (Hybrid CoE, n.d.).

Given the limitations of this study, it would be beneficial to examine the EU's anti-sabotage strategies in greater detail from the following perspectives:

- The level of compliance of candidate countries such as Türkiye should be examined, particularly regarding the extent to which they are integrated into the sabotage strategies employed by countries involved in the enlargement process.
- Critical analysis of AI-based securitization processes: The ethical dimensions of technology-centric security solutions must be addressed, particularly from the perspective of data rights.
- Socio-psychological effects: The impact of sabotage threats on security perception through media, social resistance capacity, and psychological security warrants further investigation.

While the EU's strategy for combating sabotage is structurally sophisticated, its implementation remains fragile due to national differences, institutional fragmentation, and a lack of democratic oversight. In this context, enhancing technical capacity and aligning security policies with the principles of human rights, democratic legitimacy, and participatory governance are both critical. The threat of sabotage is not only a security issue but also a legal, political, and sociological challenge.

REFERENCES

- Akgül-Açıkmış, S. (2015). Avrupa Birliği'nin dış ve güvenlik politikaları. In B. Akçay (Ed.), *Türkiye-AB ilişkileri: Yeni açılımlar* (pp. 79–90). Seçkin Yayıncılık.
- Akgül-Açıkmış, S. (2023). Güvenlik, güvenlik çalışmaları ve güvenlikleştirme. In *Küresel siyasete giriş: Uluslararası ilişkilerde kavramlar, teoriler, süreçler* (pp. 241–257). İletişim Yayınları.
- Austin, J. L. (1962). *How to do things with words*. Harvard University Press.
- Balzacq, T. (Ed.). (2011). *Securitization theory: How security problems emerge and dissolve*. Routledge.
- Borchert, H., & Pankratz, T. (2004). Homeland security aus europäischer Perspektive. In H. Borchert (Ed.), *Weniger Souveränität – mehr Sicherheit: Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte* (pp. 17–38). Mittler.

- Bossong, R. (2008). The action plan on combating terrorism: A flawed instrument of EU security governance. *JCMS: Journal of Common Market Studies*, 46(1), 27–48. <https://doi.org/10.1111/j.1468-5965.2007.00766.x>
- Bures, O. (2006). EU counterterrorism policy: A paper tiger? *Terrorism and Political Violence*, 18(1), 57–78. <https://doi.org/10.1080/09546550500174905>
- Buzan, B., Wæver, O., & de Wilde, J. (2013). *Security: A new framework for analysis*. Lynne Rienner Publishers.
- Carlisle, R. P. (2004). *Scientific American inventions and discoveries*. John Wiley & Sons.
- Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber)security actor? *JCMS: Journal of Common Market Studies*, 55(6), 1254–1272. <https://doi.org/10.1111/jcms.12575>
- Carrera, S., Marco, S., Chun Luk, N., & Vosyliūtė, L. (2018). *The future of the Schengen area: Latest developments and challenges in the Schengen governance framework*. European Parliament. [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604943/IPOL_STU\(2018\)604943_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604943/IPOL_STU(2018)604943_EN.pdf)
- Christou, G. (2016). *Cybersecurity in the EU*. Palgrave Macmillan.
- Council of the European Union, General Secretariat of the Council. (2009). *European security strategy: A secure Europe in a better world*. Publications Office.
- ENISA. (2025, February 27). *A trusted and cyber secure Europe – ENISA strategy*. <https://www.enisa.europa.eu/publications/a-trusted-and-cyber-secure-europe-enisa-strategy>
- Euronews. (2022, September 28). “Sabotage” and “deliberate acts” suspected in mysterious Nord Stream leaks, EU says. <https://www.euronews.com/my-europe/2022/09/28/sabotage-and-deliberate-acts-suspected-in-mysterious-nord-stream-leaks-eu-says>
- European Commission. (n.d.). *Hybrid threats*. https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en
- European Commission. (2006). *European programme for critical infrastructure protection (EPCIP)* (COM(2006) 786 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33260>
- European Commission. (2023, June 29). *EU-NATO task force: Final assessment report on strengthening our resilience and protection of critical infrastructure*. https://ec.europa.eu/commission/presscorner/api/files/document/print/mt/ip_23_3564/IP_23_3564_EN.pdf

- European Council. (2005). *The EU counter-terrorism strategy*.
<https://data.consilium.europa.eu/doc/document/ST%2014469%202005%20REV%204/EN/pdf>
- European External Action Service. (2024, March). *Annual progress report: On the implementation of the Strategic Compass for security and defence*.
https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2ndYear_Report_0.pdf
- European Parliament. (2021). *Strategic or critical infrastructures, a way to interfere in Europe: State of play and recommendations*.
[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU\(2021\)653637_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU(2021)653637_EN.pdf)
- European Union Agency for Cybersecurity. (2022). *ENISA threat landscape 2022: July 2021 to July 2022*. Publications Office of the European Union.
- Europol. (2025). *European Counter Terrorism Centre (ECTC)*. <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc>
- Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, 31(3), 435–453.
<https://doi.org/10.1080/09662839.2022.2102896>
- Galtung, J. (1990). Cultural violence. *Journal of Peace Research*, 27(3), 291–305.
<https://doi.org/10.1177/0022343390027003005>
- Geropoulos, K. (2024). *The plot thickens again for Nord Stream sabotage*. New Europe.
<https://www.neglobal.eu/the-plot-thickens-again-for-nord-stream-sabotage/>
- Hybrid CoE. (n.d.). *What is Hybrid CoE?* <https://www.hybridcoe.fi/who-what-and-how/>
- Kaunert, C. (2009). The external dimension of EU counter-terrorism relations: Competences, interests, and institutions. *Terrorism and Political Violence*, 22(1), 41–61.
<https://doi.org/10.1080/09546550903409551>
- Kuzemko, C., Keating, M. F., & Goldthau, A. (2016). *The global energy challenge: Environment, development and security*. Palgrave Macmillan.
- Lijphart, A. (1971). Comparative politics and the comparative method. *American Political Science Review*, 65(3), 682–693. <https://doi.org/10.2307/1955513>
- Monar, J. (2015). The EU as an international counter-terrorism actor: Progress and constraints. *Intelligence and National Security*, 30(2–3), 333–356.
<https://doi.org/10.1080/02684527.2014.988448>

- NATO. (2024, May 7). *Countering hybrid threats*.
https://www.nato.int/cps/en/natohq/topics_156338.htm
- Neocleous, M. (2022). *Critique of security*. Edinburgh University Press.
- Occhipinti, J. D. (2017). Still moving toward a European FBI? Re-examining the politics of EU police cooperation. In J. Argomaniz, O. Bures, & C. Kaunert (Eds.), *EU counter-terrorism and intelligence* (pp. 234–258). Routledge. <https://doi.org/10.1080/02684527.2014.988449>
- Olech, A. (2025). Hybrid threats to critical infrastructure in the EU. *Terrorizm, 2025*(Special Issue), 133–158.
- Scholten, D., & Bosman, R. (2016). The geopolitics of renewables: Exploring the political implications of renewable energy systems. *Technological Forecasting and Social Change, 103*, 273–283.
<https://doi.org/10.1016/j.techfore.2015.10.014>
- Waldmann, P. (2005). *Terrorismus: Provokation der Macht* (2., vollständig überarbeitete Aufl.). Murmann.
- Weyembergh, A., & Brière, C. (2018). The future cooperation between OLAF and the European Public Prosecutor's Office. *New Journal of European Criminal Law, 9*(1), 62–82.
<https://doi.org/10.1177/2032284417743820>
- Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Sage.

KATKI ORANI / CONTRIBUTION RATE	AÇIKLAMA / EXPLANATION	KATKIDA BULUNANLAR / CONTRIBUTORS
Fikir veya Kavram / <i>Idea or Notion</i>	Araştırma hipotezini veya fikrini oluşturmak / <i>Form the research hypothesis or idea</i>	Selçuk KÖMCÜ Asst. Prof. Alptekin MOLLA (Ph.D.)
Tasarım / <i>Design</i>	Yöntemi, ölçeği ve deseni tasarlamak / <i>Designing method, scale and pattern</i>	Selçuk KÖMCÜ Asst. Prof. Alptekin MOLLA (Ph.D.)
Veri Toplama ve İşleme / <i>Data Collecting and Processing</i>	Verileri toplamak, düzenlenmek ve raporlamak / <i>Collecting, organizing and reporting data</i>	Selçuk KÖMCÜ Asst. Prof. Alptekin MOLLA (Ph.D.)
Tartışma ve Yorum / <i>Discussion and Interpretation</i>	Bulguların değerlendirilmesinde ve sonuçlandırılmasında sorumluluk almak / <i>Taking responsibility in evaluating and finalizing the findings</i>	Selçuk KÖMCÜ Asst. Prof. Alptekin MOLLA (Ph.D.)
Literatür Taraması / <i>Literature Review</i>	Çalışma için gerekli literatürü taramak / <i>Review the literature required for the study</i>	Selçuk KÖMCÜ Asst. Prof. Alptekin MOLLA (Ph.D.)

Hakem Değerlendirmesi: Dış bağımsız.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

Teşekkür: -

Peer-review: Externally peer-reviewed.

Conflict of Interest: The author has no conflict of interest to declare.

Grant Support: The author declared that this study has received no financial support.

Acknowledgement: -
