Eastern Journal of European Studies
DOI: 10.47743/ejes-2025-0203 • December 2025 • VOLUME **16**, ISSUE **2**

Toward a systemic framework for evaluating the European Union's resilience to hybrid threats

Edina Lilla Mészáros✉, **Constantin Vasile Țoca**
University of Oradea, Romania

Abstract: Recognizing the rapid advancement and heightened intricacy of hybrid threats, EU and Hybrid CoE experts devised a new framework to address these challenges. Given that non-conventional hazards can affect all aspects of life and society, implementing countermeasures that focus solely on certain areas is inadequate. The present article proposes a systemic framework for evaluating the EU's response to hybrid threats, as resilience is the foundation of the Comprehensive Resilience Ecosystem model. Initiatives aimed at fostering resilience against hybrid threats were classified into five principal areas, which include an assessment of political and legal frameworks, institutional measures, inter-institutional collaboration, regulatory actions, and societal strategies, reflecting a comprehensive approach that engages the entire society. This analysis will examine the Community's resilience-building initiatives against hybrid threats over the past two decades, while also illustrating that the Union can play a vital supplementary role in assisting Member States to address the unconventional threats of the 21st century.

Keywords: hybrid threats, hybrid warfare, resilience, Comprehensive Resilience Ecosystem Model, whole-of-society approach

Introduction

Acknowledging the swift progress and increased complexity of hybrid threats targeting the European Union prompted experts from the Joint Research Centre (JRC) of the European Commission and the Hybrid CoE to jointly develop a new framework for tackling hybrid menaces. Since non-conventional risks can impact all domains of life and parts of society, coming with counter-measures targeting only certain individual areas does not suffice, thus demanding the employment of a *systems-thinking* or a *comprehensive ecosystems approach* to hybrid threats. The proposed Comprehensive Resilience Ecosystem (CORE) model enables policymakers to assess the methods that various actors use to implement hybrid threats, so as to influence democratic decision-making processes in the EU. While it underscores the critical importance of anticipation in the timely detection of hybrid

✉ PhD Lecturer, Department of International Relations and European Studies, University of Oradea, Romania; e-mail: edina_lilla@yahoo.com.

threats, the CORE model permits the oversight of dependencies and their subsequent ramifications, by illustrating the gradual challenges that democratic systems face as a result of hybrid threat operations. These hybrid threat activities alter the prevalent status quo by generating different kinds of stress. The CORE model was developed to comprehensively represent democratic society, while focusing on the evaluation and mitigation of hybrid threats that seek to undermine the integrity and functioning of democracies. The proposed CORE is three layered, covering the local, national and international levels, comprising three main sectors of society: the civic, governance and services spaces. The CORE model hierarchy comprises 13 fields subordinate to the aforementioned spaces, including information, social/societal, culture, political, public administration, legal, intelligence, diplomacy, military defence, infrastructure, economy, space, and cyber domains. These 13 domains serve as gate-keepers against malevolent third-party activity. Overall, CORE functions as a dartboard, allowing decision-makers to outline the methods of operation of adversaries and observe their impact on the specific layers, spaces and domains, thus enabling the determination of possible responses and counter-measures (Jung Wirth et al., 2023, pp. 8-12).

The article builds on the CORE model by proposing a systemic framework for evaluating the EU's resilience to hybrid threats. Instead of conducting a direct empirical assessment, the paper develops a multilayered framework that positions resilience-building initiatives within five main categories: political and legal frameworks, institutional measures, inter-institutional cooperation, regulatory actions and societal approaches.

The main research question the study aims to address is: how effectively can resilience-building measures developed at Community level support Member States in the prevention and management of hybrid threats, and what systemic framework most accurately encapsulates these endeavours? By situating the CORE model within the broader literature on hybrid threats and resilience, the paper advances a more comprehensive understanding of how resilience can be conceptualized and enhanced across multiple layers of governance and society. The subsequent section delineates the methodology employed in the development and implementation of this framework.

Methodology

This study employs qualitative content analysis to examine the EU's resilience-building measures in response to hybrid threats. The research is not intended to explicitly assess resilience outcomes, but to systematically map and classify EU-level responses into the five resilience-building dimensions described above. The analysis is interpretive in nature, emphasizing the significance, context and development of EU policies and strategies related to the prevention and management of hybrid challenges rather than relying on quantitative indicators. The

collection of documents analysed includes official EU strategies, communications, directives and joint frameworks elaborated in the past two decades. This period was selected because it captures the progression of Community responses from early initiatives on critical infrastructure protection from 2006 to the most recent, the Strategic Compass from 2022 and the Security Union Strategy for 2020-2025.

Selection of materials and coding

EU level documents that expressly addressed hybrid threats, resilience or associated domains (like cyber, energy, disinformation) were included in the analysis. Texts were coded into five categories (political/legal, institutional, inter-institutional, regulatory and societal) based on the domains proposed in the CORE model. The coded material was examined to discern patterns, gaps and redundancies in resilience-building measures, emphasizing the evolution of the EU's role over the past two decades. No specialized software was employed, the authors performing coding and categorization manually in order to facilitate interpretive depth and contextual sensitivity.

The main added value of the research paper consists in the authors developing a multilayered (five-level model) analysis, examining resilience building against hybrid threats in five distinct categories.

The research has its limitations, as due to constraints related to time and paper length it does not cover resilience-building measures against hybrid threats across all 13 domains of the CORE model. Nevertheless, the framework provides a structured foundation for future empirical research.

The following section brings forth a comprehensive literature review that contextualizes the CORE model within the wider scholarly debate on hybrid threats and resilience. By comparing Western and non-Western conceptualization of hybridity in warfare, the review situates the EU's systemic approach as both a response to external influence and an advancement in security governance. This transition guarantees consistency between the conceptual foundations and the methodological approach presented above.

1. The conceptual foundations of hybrid threats and of hybrid warfare. A brief literature review

1.1. Western perceptions of hybridity in warfare

Several scholars emphasize the old notion reinvented in a new cloak approach while evaluating the emergence of the concept of hybrid threat. At the same time, Fiott and Parkes argue that the term previously referred to as 'unconventional threat' during the Cold War has reemerged in the new Millennium as 'hybrid threat', indicating a notable resurgence. Conversely, experts highlight the presence of

disagreements and uncertainties regarding the precise meaning of the term under inquiry, underlining two significant reservations associated with it. (Costa, 2021, pp. 1-2; Fiott & Parkes, 2019, p. 4; Wilkie, 2009, p. 13). To begin with, according to EUISS specialists, the concept of 'hybrid threat/warfare' does not offer a comprehensive and operational theory. In contrast, concerning its theoretical framing, other authors appear to adopt an alternative perspective. For instance, while Brin Najzer recognizes the limitations of developing an absolute theory of war, he does not dismiss the potential for creating a set of theoretical characteristics that may signal the onset of a particular type of conflict. Additionally, Najzer proposes a unified theory of hybrid warfare. This theory is designed to identify the factors that contribute to the emergence of hybrid threats and the critical indicators that lead to their occurrence (Fiott & Parkes, 2019, p. 4; Najzer, 2020, pp. 2, 18, 82-87). Furthermore, Fiott and Parkes contend that alternative terms such as 'irregular warfare', 'non-linear combat', 'compound warfare' or 'grey zone' may provide a more precise description of the asymmetric or hybrid-like threats of the 21st century (Fiott & Parkes, 2019, p. 4). Secondly, in their view, too much attention rendered to hybrid threats and to non-traditional forms of warfare might lead to neglecting conventional military threats, thus hindering the efficiency of their prevention and management (Ibidem, p. 5).

There's no unison among the pundits concerning the origins of the concept under investigation either. The vast majority of them attribute its development to former US Marine officer, Lieutenant Colonel Frank G. Hoffman, (Bērziņš, 2020, p. 357; Pulido Gragera, 2019, p. 104; Renz, 2016, p. 287) frequently overlooking the influence of other scholars on Hoffman's work, despite the author's own acknowledgment of the significant impact that several savants had on shaping his theory. Nonetheless, we must stress, that without neglecting the pioneering work in this field of experts such as William J. Nemeth, the coining of the most widely known definition of 'hybrid warfare' is attributed to Frank G. Hoffman (Fridman, 2018, pp. 10-15; Giannopoulos et al., 2021, pp. 9, 22-23; Najzer, 2020, pp. 26-27; Rinelli & Duyvesteyn, 2018, p. 19.).

While one of the most prominent military strategists of all times, Prussian General Carl von Clausewitz described war in the 19th century as a political instrument, a continuation of political intercourse by other means, Frank G. Hoffman argued that in modern times there exist various types of war and distinguishing between them can be a very arduous task. In his opinion, the blurriness of forms of war, belligerents and of the used weapons and technologies is what produces the anomaly called hybrid warfare (Clausewitz, 2007, pp. 28-2). Thus, Hoffman understands by hybrid warfare "a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder", warfare, which can be conducted by both state and non-state entities (Hoffman, 2007, p. 14). Based on the observations drawn from analysing the modus operandi of hybrid actors (proto-states), such as Hamas and Hezbollah in their

conflict with Israel, Hoffman has already forecasted the convergence of various challengers and their divergent methods into multi-modal or hybrid conflicts. In the author's view, their hybrid nature is being reflected not just in their methods of operation, but also in their organizational style, thus revealing a polymorphous character (Hoffman, 2007, pp. 28-29).

Whenever attempting to identify the particularities of 'hybrid threats' and of 'hybrid warfare', authors frequently perceive them as a combination and use of divergent tools and methods by various actors. As regards the definition of hybrid threats, Hoffman understands by them "any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behaviour in the battle space to obtain their political objectives" (Hoffman, 2009a, p. 15; Hoffmann, 2009b). Other specialists, such as Rasmus Hindren, besides drawing attention to the malevolent nature of actors employing hybrid tactics, highlight the seemingly infinite panoply of tools and methods that are at their disposal. The scholar's predictions indicate that technological advancements will significantly influence the growth of both the variety of threats and their portfolio (Hindren, 2021, p. 7).

1.2. Non-Western perceptions of hybridity in warfare

In analysing hybridity in warfare, it is crucial to acknowledge that non-Western state actors, such as Russia and China, have a different understanding of these concepts, hence intensifying even more the ambiguity surrounding the topic. It is rather polemical that while the European Union, NATO and their Member States talk about the imperativeness of tackling hybrid threats originating from Russia and boosting resilience, concurrently, Moscow also perceives itself as a target of Western hybrid hostility (Galeotti, 2019, p. 1). Concerning the introduction of the notion of hybridity into EU strategic documents, several scholars, politicians and military leaders highlight the trailblazing role of the Russian intervention in Ukraine, perceiving the annexation of Crimea as a prototype of contemporary hybrid warfare (Mészáros & Țoca, 2023, p. 7). However, while them labelling Russia's actions in Ukraine as 'a new form of hybrid warfare', other experts like DeBenedictis dispute such assertions. In his view, Russia's actions in Ukraine do not represent some novel form of warfare, but rather a modern implementation of political practices already used by the Soviet leadership. The author argues that the informational, political and military tools recently applied by Russia in Ukraine are similar, if not the same as those deployed by the U.S.S.R. decades ago, thus demonstrating that even though the times, technology and leaders have changed, the mindset and the methods have remained the same (DeBenedictis, 2022, pp. 1-20).

With respect to conceptualization, the majority of academics label the term 'hybrid warfare' as a Western construct, not necessarily having a precise match in the relevant Russian literature. *Gibridnaya voyna* is considered the closest Russian

term to the Western concept of hybrid warfare (Fridman, 2018). Indisputably, when discussing about the Russian perception of hybrid warfare, General Valery Gerasimov's tenets are of a major point of reference. However, the so called 'Gerasimov Doctrine' is not without flaws, critics pointing out its elusive, even 'mythical' or fictional character, many contesting the corporeality of such a tenet (Galeotti, 2019, pp. 27-28; Fox, 2023). When Gerasimov presented his ideas, he posited that the fundamental nature of armed conflict was evolving and subsequently introduced the notion of hybrid warfare as a characterization of the manner in which great powers would engage in competition in the future (Fox, 2023). Several scholars argue, that instead of coming up with a groundbreaking blueprint for a future type of combat, the so called 'new generation warfare', Gerasimov did nothing but acknowledge the altered essence of warfare itself. Nonetheless, the changing dynamics of warfare that prioritizes non-kinetic instruments over kinetic ones, seldom represent a significant deviation from the conventional Russian military doctrine (Fox, 2023; Galeotti, 2019, p. 28; Rácz, p. 36). Comparing the Russian scholarly work on *gibridnaya voyna* with the Western theoretical harvest, reveals a stark contrast in its comprehension and implementation. While the Western interpretation concentrates on tactical military and operational activities "directed and coordinated within the main battlespace to achieve synergistic effects" the Russian perception is more abstract, embracing all domains of public life, from politics to economy, social development, and culture. Namely, in contrast to Hoffman's view, describing hybrid warfare as a mix of combat modalities, encompassing conventional capabilities, irregular tactics and formations, terrorist activities etc. executed by both state and non-state actors, the Russian *gibridnaya voyna* focuses on an abstract combat zone, even targeting to break the social and cultural bonds of their opponents while preserving their own (Fridman, 2018). This indicates that, whereas the West perceives hybridity in warfare as an amalgamation of regular and irregular forces employing a mix of operational and tactical methods, Russia is unreserved in its willingness to engage all spheres of public life to attain specific political and military objectives.

The subsequent section represents the main analysis of the paper, the authors elaborating a five-layered framework for evaluating the EU's resilience to hybrid threats.

2. Developing a systemic framework for evaluating the European Union's resilience to hybrid threats

Even though governments have the main responsibility of countering hybrid challenges as these threaten vital national security interests, are endowed with skills and dispose of the necessary tools for their governance, precisely the borderless character of contemporary threats is what demands "a critical complementary role to

be filled by the EU in support of Member States' efforts" (Kalniete & Pildegovičs, 2021, p. 25).

At Community level resilience is described as the ability of various societal levels-individuals, households, communities, nations, or regions - to endure, adapt to, and swiftly recuperate from stresses and shocks, including natural disasters, violence, or conflict (European Parliament, 2016, p. 2; Ostárková & Staníčková, 2021, p. 13).

In the following lines, we shall divide resilience building measures against hybrid threats at Community level in five major categories, briefly assessing: the political/legal, institutional, inter-institutional cooperation, regulatory and societal measures (whole-of-society approach).

2.1. The political/legal framework of countering hybrid threats at EU level

Political will, resources and capacity to act are essential for a coherent response at Community level to counter unconventional security challenges. Concrete steps taken in this field, such as the establishment of a political and legal framework signals the existence of such a will, while capacity building has been forming over the years. Although we acknowledge that a range of EU legislation specifically targeting the countering of hybrid threats has emerged mainly since 2014, the Russian annexation of Crimea and the consolidation of the terrorist group, Da'esh, unconventional threats related initiatives were developed at EU level even before (Kalniete & Pildegovičs, 2021). Since specialists in the field include physical operations against infrastructure, creating and exploiting infrastructure dependency or of economic dependencies, foreign direct investment, industrial espionage, undermining the opponent's national economy, leveraging economic difficulties, cyber espionage, cyber operations, airspace violation, territorial water violation, weapons proliferation, paramilitary organizations, military exercises, engaging diasporas for influencing, financing cultural groups and think thanks, exploitation of socio-cultural cleavages, promoting social unrest, manipulating discourses on migration to polarize societies, promoting and exploiting corruption, intelligence and clandestine operations, infiltrations, creating confusion or a contradictor narrative, using migration as a bargaining chip, discrediting leaders and/or candidates, exploiting immigration for political influencing, media control and influencing, disinformation campaign and propaganda, electronic operations etc. in the palette of tools used within hybrid threat activities, then we reach the conclusion that previously elaborated legislation could also fit within the label of initiatives countering hybrid threats (Giannopoulos et al., 2021, pp. 33-34). Earlier documents, such as the "Communication on the European Programme for Critical Infrastructure Protection" from December 2006, the Green Paper on bio-preparedness from 2007, the "Communication on critical information infrastructure protection" from March 2009 or the "Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection"

from December 2008, could be perceived as one of the first steps in establishing the EU's legal framework aimed at countering unconventional or hybrid challenges (Fiott & Parkes, 2019, p. 14). The multiplication of security related incidents occurring within cyberspace prompted the elaboration of a "Cybersecurity strategy of the EU: an open, safe and secure cyberspace" in 2013, which put forward concrete actions and best practices for the prevention and tackling of all cyber disruptions and attacks, having the final objective of achieving a cyber resilient Community (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013, pp. 4-5). The "European Energy Security Strategy", the "EU Maritime Security Strategy", the "EU Maritime Security Strategy Action Plan" and the "The European Agenda on Security" developed in 2014, respectively 2015, are also meant to enhance the EU's response capacity and resilience to unconventional risks within the energy, maritime and security sectors (Fiott & Parkes, 2019, p. 14).

The "Global Strategy for Foreign and Security Policy" from 2016 also highlights the importance of countering hybrid challenges, recognizing their impending and borderless character; however, it renders more attention to the concept of resilience building, dedicating an entire chapter to describing the tools and methods with which the Community wishes to contribute to the establishment of state and societal resilience in its Eastern and Southern neighbourhood (Cusumano & Corbe, 2018, p. 146; European Union External Action Service, 2016, pp. 18, 20, 23-28, 37). The development of a Joint Framework for countering hybrid threats in 2016 signifies a pivotal moment in the EU's recognition of the significant alterations in its security landscape and the necessity for a unified response to hybrid threats. While acknowledging the inherent role of Member States in countering hybrid threats, primarily because the majority of national vulnerabilities are country-specific, the European Commission argues that hybrid menaces can be more successfully mitigated through a coordinated response at the EU level, employing EU policies and mechanism to strengthen European solidarity and mutual help. The Joint Framework has provided the conceptual basis of hybrid threats, at the same time showcasing the EU's collective response to tackling them, emphasizing key components such as enhancing awareness, fostering resilience, conflict prevention, effectively responding to crises, and facilitating recovery. In Community understanding, hybrid threat is a concept that seeks to encompass the amalgamation of coercive and subversive actions, employing both conventional and unconventional strategies (such as diplomatic, military, economic, and technological) that can be orchestrated by state or non-state entities to attain particular goals while remaining below the level of formally recognized warfare. (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2016). In 2018 was put forward a Joint Communication, specifically designed to confront hybrid challenges by enhancing resilience at both the national and EU levels. Within the joint communication, the importance of

cultivating resilience to counter hybrid threats was highlighted and broadened to encompass sectors such as Chemical, Biological, Radiological and Nuclear and cyber threats as well (Joint Communication, 2018, pp. 1-11).

Because nowadays disinformation has become one of the most insidious tools employed by both violent state and non-state actors, the European Commission's Action Plan from 2018 had signified a quantum leap in its handling (Action Plan, 2018, p. 2). The document not only acknowledges the potential of disinformation turning into a handy tool in a hybrid warfare waged against the European Community but proposes 10 targeted actions for its successful countering within a four-pillar framework.

In June 2019, the European Council came forward with "A New Strategic Agenda" for 2019-2024, assessing the enhanced role that the EU can play in a rapidly changing, complex international security environment. This document also aligns with the previously analysed papers, as it puts emphasis on the importance of countering hybrid threats, cyber incidents and disinformation generated by hostile state and non-state actors. According to the agenda, their prevention and management is possible only through the implementation of an all-encompassing approach that requires a more enhanced cooperation, coordination, technological capacities and the use of additional resources. As regards resilience, no concrete reference is made to resilience building to hybrid threats, the strengthening of resilience being mentioned only in the context of tackling natural and man-made disasters (European Council, 2019).

On the same note, indisputably, one of the biggest innovations of the Lisbon Treaty was the introduction of a solidarity clause under the auspices of Art. 222. This clause represents a major landmark in the history of the European Community, as it places within a legal framework the act of showing solidarity among EU states and of combining efforts in order to give a prompt, efficient and consistent response in the event of terrorist attacks, natural or man-made disasters. Namely, article 222 stipulates the possibility of Member States assisting each other, in case one of them experiences serious shocks and stresses, such as terrorist attacks, or various types of disasters (EUR-Lex, n.d.). In this regard, the Council of the European Union Conclusions from December 2019 is also worth mentioning, as it extended the situations in which Member States can enhance their collaboration with each other, enabling them to invoke the 'the all for one and one for all'(solidarity) clause even in the case of an emergency/crisis stemming from a hybrid type of activity (Council Conclusions, 2019, p. 6; Kalniete & Pildegovičs, 2021, p. 26).

The "Strategic Compass" was elaborated in 2022, expected to strengthen the EU's security and defence policy by 2030. Both hybridity and resilience occupy a central position within the paper. Despite the return of a conventional type of war to the European continent, the document acknowledges the large array of unconventional methods and instruments that are being used within the current international security landscape by both governmental and non-governmental

entities. The EU's response to these threats is divided in four priority actions: act, secure, invest and partner. The countering of hybrid threats and actors generating such threats, appears in the second priority action, secure, the 'Compass' stipulating the creation of an EU Hybrid Toolbox**,** gathering a wide range of tools for the early detection and response to all kinds of unconventional hazards (Strategic Compass, 2022, pp. 4-62).

Resilience building is included in the second priority action, the document highlighting the utter necessity of boosting resilience at Community level in order to offset "[...] hybrid threats, cyberattacks and foreign information manipulation and interference" (Strategic Compass, 2022, pp. 4-62). The bolstering of societal, economic and of cyber resilience is conceived as an essential part of the EU Hybrid Toolbox. Countering hybrid threats and resilience building occupies a major role in the EU Security Union Strategy for 2020-2025 as well. In this regard, special attention is given to the protection and bolstering the resilience of the EU's critical infrastructure. This strategy is of paramount significance, since it pioneered the Community's new holistic approach to managing hybrid threats, encompassing measures from "early detection, analysis, awareness, resilience building, and prevention to crisis response and consequence management", thus including hybrid considerations into all policymaking efforts (European Commission, 2020).

2.2. The EU's institutional resilience building measures to tackling hybrid threats

In addition to establishing a legal framework that allows the EU to play a complementary role in countering unconventional security threats, the joint communications and strategic papers have also established the legal foundation for the setup of a variety of supranational agencies and institutions. The EU Agency for Cybersecurity (ENISA) founded in 2004, could be considered as one of the first in the long list of agencies established at supranational level meant to tackle various forms of non-linear threats. The achievement of a high level of common cybersecurity at EU level is the most important rationale behind the establishment of ENISA. On the other hand, besides keeping EU citizens, institutions and agencies digitally safe, it is also charged with assisting the Community and MS in preparing for future cyber challenges (ENISA, n.d.; Fiott & Parkes, 2019, p. 14). In the same vein, the Computer Emergency Response Team (CERT-EU) established in 2012 and the EUROPOL's European Cybercrime Centre (EC3) set up a year later, were designed in order to reinforce protection against cyberattacks at Community level. The mandates of these two agencies are complementary to each other, as while the first has been set up to efficiently respond to information incidents and cyber threats in both the private and public sectors, the second acts as a sentinel, guarding EU citizens, governments and businesses from crime committed within cyberspace, by enforcing the law (Europol, EC3).

The necessity to effectively map and contain disinformation originating from the Eastern Neighbourhood, mainly following the Russian intervention in Ukraine in 2014, has led to the creation of the East StratCom Task Force in 2015. This special unit created under the umbrella of the European External Action Service has a double role (Hedling, 2021, pp. 841-845):

- Firstly, it is designed as a 'myth-buster', mandated with identifying and containing disinformation, namely, deconstructing 'fake news' coming from the Eastern vicinity;
- Secondly, it is responsible for projecting a positive narrative and a genuine picture about the European Union and its policies to the citizens and governments from the Eastern Neighbourhood.

According to the EEAS portal, by 2021, the number of full-time experts working for the Task Force had increased to 16, all recruited by EU institutions or seconded by EU Member States. Besides organizing information campaigns targeting discrediting operations, the Eastern StratCom elaborates on a weekly basis the *Disinformation Review*, its flagship product, containing valuable data and analysis about disinformation to both specialists and laymen (East StractCom Task Force).

One of the most important institutional innovations with respect to the countering of hybrid threats was established in 2016, by the "Joint Framework on Countering Hybrid Threats". The document foresaw the creation of an EU Hybrid Fusion Cell under the guidance of the EU Intelligence and Situation Centre (EU INTCEN), aimed at providing a real assessment of the hybrid threats targeting the EU and its MS. The task of the Cell is to identify, gather, analyse and share open-source information concerning indicators related to hybrid threats. The Cell, besides informing competent authorities at both supranational and intergovernmental level about potential unconventional challenges and challengers, also provides valuable inputs for the elaboration of security risk assessments. All EU Member States are expected to set up National Contact Points in order to have as a constructive and efficient liaison with the Hybrid Fusion Cell as possible (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2016, p. 4). Furthermore, given the example of the NATO Centres of Excellence, the framework paper recommends Member States to consider the possibility of establishing similar National Centres of Excellence, specifically targeting hybrid threats. These Centres are envisaged as research hubs, enabling the thorough examination of the phenomenon and thus, "the development of new concepts and technologies within the private sector and industry to help Member States build resilience" (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2016, p. 5).

Although not a self-standing EU agency, but an autonomous network-based think tank, the European Centre of Excellence for Countering Hybrid Threats also deserves to be included in the selective list of institutions boosting resilience against hybrid threats. Moreover, it could also fit in the following part of the study assessing

inter-institutional cooperation measures, as the Hybrid CoE inaugurated in 2017, in Helsinki, could be perceived as the embodiment of a more enhanced cooperation between the EU and NATO, endorsed during the NATO Warsaw Summit from 2016. It acts as a hub of expertise, promoting a 'whole-of-government' and 'whole-of-society approach' to tackling hybrid security threats, and it's a one-of-a-kind agency, as all NATO and EU Member States are allowed to participate in its activities without any discrimination. The most important added value of the Hybrid CoE is to provide both participating states and organizations a high level of expertise and training in combating asymmetric threats. Additionally, the Centre also creates an appropriate venue for the EU and NATO to jointly conduct operations and exercises (Hybrid CoE; NATO Watch).

Besides creating Hybrid CoE, the first cyber exercise at EU level was organised in 2017, called EU Cybrid 2017. This strategic cyber defence exercise was jointly organised by the country then holding the rotating presidency of the Council of Ministers, Estonia, the Estonian Ministry of Defence and the European Defence Agency. Raising awareness of incidents related to cyberspace, their coordination, the elaboration of crisis response mechanisms and of a prominent strategic communication constituted the main reasons for the organisation of such a groundbreaking exercise (European Defence Agency, 2017). Moreover, acknowledging the impending risk that chemical, biological, radioactive and nuclear agents might represent, the European Commission together with DG Sante launched a new exercise at the beginning of 2018 – Chimera - aimed at strengthening health preparedness and response to biological and chemical terror attacks in the EU. According to official documents, Chimera was launched in order to test the level of preparedness and response planning to serious cross-border threats (mainly CBRN related) of the health, civil protection and security sectors from the EU and selected third countries. The exercise included the simulation of possible attacks involving CBRN agents, such as the deliberate spread of a communicable disease, simultaneously carrying out a cyberattack in critical infrastructure. This fictitious scenario enabled the organisers to test not just the reaction time, the level of preparedness of the competent authorities, but also the existing infrastructure, the required instruments and the communication tools at EU level linked to the countering of hybrid threats. Overall, the exercise was successful, as it has improved the capacity building, interoperability and coordination of the targeted sectors at EU, MS and also at the level of partners from third countries (Joint Framework 2017 to June 2018, 2018, pp. 7-8; Joint Action to Strengthen Health Preparedness, 2019).

Besides the Hybrid Toolbox, in the Strategic Compass reference is made to the setting up of EU Hybrid Response Teams, which are foreseen as flexible tools assisting not only national governments but also the Common Security and Defence Policy missions and operations as well as partner countries in countering such threats (Strategic Compass, 2022).

2.3. Inter-institutional cooperation measures boosting resilience building against hybrid threats

NATO had played a major role in the term 'hybridity' gaining popularity in the European Union. Moreover, it is being argued that resilience building to hybrid threats occupies a central position within the core documents elaborated at the level of both organizations. In NATO's White Paper from 2015 reference was made to strengthening ties with the EU, as regards the efficiency of countering hybrid threats, also targeting the achievement of a 'shared resilience' to such challenges. Concerning the consolidation of cooperation with the European Union with respect to the management of hybrid and cyber threats, NATO's Warsaw Summit from 2016 is of outmost importance, as it had extended the areas of cooperation between the two organizations (NATO Warsaw Summit, 2017, p. 2). Among the proposals jointly endorsed in this field, the most important are the "Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization" elaborated in 2016 and the "Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization" issued in 2018 (Lonardo, 2021, pp. 1076-1077).

The Joint Declaration, elaborated in 2016, acknowledges the unprecedented challenges that the Euro-Atlantic security community has to face, highlighting that only by working together and by making a more efficient use of resources (pooling and sharing) it is possible to win the fight against unconventional threats. The statement starts from the premise that resilience to hybrid threats can only be achieved by mutually reinforcing each other, as the stronger the strategic partner, the more capable to fence off any type of conventional/unconventional hazards. Among the concrete measures listed in the joint statement that address hybrid risks, we find (European Council, 2016, pp. 1-2):

- Extending and adapting operational cooperation at sea and on migration;
- Boosting coordination on cyber security and defence with respect to joint missions, operations, exercises, education and training;
- Foreseeing the organization of parallel and coordinated exercises including those related to the prevention of hybrid risks;
- Strengthening resilience to counter hybrid threats by enhancing joint efforts related to analysis, prevention, early detection, efficient and timely information sharing and cooperation on strategic communication and response;
- Developing coordinated procedures through respective playbooks.

The joint declaration elaborated two years later, consolidates even more the existing strategic partnership related to fighting off hybrid threats and provides a genuine assessment of the efficiency of the measures foreseen in 2016. Positive development could be noticed with respect to resilience building, the ability to respond to hybrid threats and to disinformation, prompt exchange of information and

the organization of simultaneous and coordinated exercises. Furthermore, there has been a considerable improvement in fighting migrant smuggling and trafficking networks and in crisis preparedness (European Council, 2018, pp. 1-2).

The Clingendael Report also argues that countering hybrid threats constitutes a priority area for both organizations, more than a quarter of the existing 74 proposals between the EU and NATO referring to the deterrence of hybrid challenges. Moreover, the report also confirms that improvement has been made in the field of information sharing between the staff of the EU Hybrid Fusion Cell and the NATO Hybrid Analysis Branch. The enhanced information sharing has led to the creation of a shared situational picture; additionally, some moderate progress has been registered as regards the exploring of possibilities how to make the best use of the facilities and exchange of publicly available information under the guidance of the Hybrid CoE (Zandee et al, 2021, pp. 6-16).

2.4. The regulatory and societal resilience building measures addressing hybrid threats

Even if they represent two distinct categories, within this research the regulatory and societal resilience building measures will be addressed together. These categories on many occasions intertwine and even complement each other.

More and more scholars and drafters of strategic policy papers at both EU and international level have claimed that since the assessment of elements of hybridity in threats is an arduous task and its management is an ongoing process, just creating the legal-political, institutional, inter-institutional and regulatory background of resilience building for the countering of asymmetric threats is simply not enough. Resilience building shouldn't take place only at the top, but also at the bottom, namely, since on many occasion citizens, the representatives of the civil society are the direct targets of actors carrying out hybrid types of activities, they should be also included in the process of countering them, thus favouring a 'whole of society' approach to resilience building. For the fight against hybrid threat generators to be successful, the existence of a societal resilience is imperative. As highlighted before, resilience building in the Southern and Eastern neighbourhoods constitutes one of the five pillars of the EU's Global Strategy from 2016, the document also emphasising the importance of investing in the promotion of societal resilience. The strategy paper argues that a resilient society that cherishes democracy, good governance and has trust in institutions represents the nucleus of a resilient state. Societal resilience is defined as "the ability of states and societies to reform, thus withstanding and recovering from internal and external crises" (European Union External Action Service, 2016, p. 23).

First of all, in order to attain the highest level of societal resilience, the representatives of the civil society must be well informed about the existence of such threats and of the methods of hostile state and non-state entities propagating them.

This is possible only by supporting the existence of transparent democratic institutions, the rule of law and of an independent media providing trustworthy information. Freedom of expression, information pluralism as well as boosting and later harnessing civic awareness through education and information are also essential. Thus, improving media literacy and the capacity to distinguish between quality information and disinformation constitute the backbone of societal resilience. Precisely, in order to be able to distinguish between genuine and fake information, in 2019, the EU has set up of the mechanism of the Rapid Alert System against Disinformation. According to former Commissioner Věra Jourová, the Rapid Alert System has proved it value for the first time in 2020, by efficiently tackling disinformation related to COVID-19 (European Parliament, 2020).

The specialists of the European Parliament also argue that members of the civil society shouldn't be only informed about hybrid challenges, but instead, they should be perceived as an essential resource, ought to be involved in both the planning and the execution of counter-hybrid strategies. In their view, well informed and conscientious civil society actors are able to perform 'watchdog functions', i.e. monitoring and revealing hybrid interference. In this regard, investigative journalism is given as a useful example (Wigell et al., 2021, p. 24) Bellingcat represents such an independent investigative journalism group, based in the Netherlands, gathering "researchers, investigators and citizen journalists using open source and social media investigation to probe a variety of subjects" (Bellingcat Official Site). The investigations of the group had led to gathering useful information concerning the downing of MH17 and to unfolding the Skripal poisoning case etc. Another prominent investigative journalism group is *The Baltic Center for Investigative Journalism Re: Baltica*, an NGO established in 2011, specialized in carrying out thorough investigations on pressing social problems, such as corruption, crime, human rights and disinformation, mainly related to the Baltic region. The mapping and containing of disinformation operations originating from the East (Russia), constitutes one of the most important reasons behind the setting up of the investigative group (The Baltic Center for Investigative Journalism; Kalniete & Pildegovičs, 2021, p. 30).

Besides deepening the relations with the civil society, the Global Strategy stresses the importance of identifying and involving other stakeholders as well, such as cultural organisations, religious communities, social partners and human rights defenders, enhancing societal resilience through the advancement of education, culture, and youth initiatives to promote pluralism, coexistence, and respect (Benke et al., 2018, p.71; European Union External Action Service, 2016, p. 26).

It has been argued that societal resilience can be attained only by supporting the existence of transparent democratic institutions, the rule of law and of an independent media providing reliable, verified and objective information to the public. Since information manipulation and disinformation are widespread in both written and online media, the use of various *regulatory instruments* is needed for

their limitation. As companies, such as Twitter, Google and Facebook have had transparency issues and have also provided a venue for state and non-state actors spreading disinformation, in recent years, both their activity and algorithms have come under scrutiny. Nowadays, big tech companies, like META (Facebook), have found themselves under a huge pressure, regulators, lawmakers and employees worldwide demanding from them to efficiently address the improper use of their services. In this regard, the EU's initiative, the Code of Practice on Disinformation elaborated in 2018 is revolutionary, as it has put the basis of the very first framework for self-regulation with the objective of combating disinformation in the world. The document was signed by the representatives of the social media networks and of the advertising industry (Kalniete & Pildegovičs, 2021, pp. 28-29). The Code was updated in June 2022 and signed by 34 actors, including "online platforms, players from the advertising ecosystem, fact-checkers, civil society, research, and other organizations […]" committed to tackle even more efficiently all aspects related to the practice of disinformation (European Commission, 2022 Code of Practice on Disinformation). Regrettably, at the beginning of 2025 Facebook' and Instagram's parent company, Meta has announced the elimination of independent fact checkers on Facebook and Instagram, favouring instead "community notes" in the X style, that enables users to comment on the veracity of posts, thus making it harder to detect fake news and disinformation on these social media platforms. (McMahon et al., 2025).

Conclusions

The article has aimed to develop a comprehensive framework for assessing the EU's resilience to hybrid threats by situating the CORE model within a multilayered analysis of Community-level initiatives. Instead of directly measuring resilience outcomes, the paper used qualitative content analysis to categorize EU responses into five groups- political/legal, institutional, inter-institutional, regulatory and societal, providing a structured framework for understanding resilience-building. The findings indicate that the Union's ability to support Member States in addressing hybrid challenges relies not only on political/legal instruments and institutional innovations but also on the coherence of inter-institutional collaboration, regulatory mechanisms and the proactive engagement of the civil society. By incorporating hybrid threat considerations throughout various policy sectors and prioritising anticipation, awareness and adaptability, the EU exemplifies and advance the capacity to conceptualize resilience as a comprehensive, whole-of-society ecosystem. Although the proposed framework does not encompass all thirteen domains of the CORE model, it offers the reader a substantial foundation for future empirical research, emphasizing the EU's capacity to serve as both a facilitator and enhancer of resilience in response to the prevailing unconventional security challenges.

References

Bellingcat. (n.d.). *Official Site*. https://www.bellingcat.com/about/

Benke, M., Czimre, K. R., Forray, K., Kozma, T., Márton, S., & Teperics, K. (2018). Learning regions for resilience in Hungary: challenges and opportunities. In T. Baycan & H. Pinto (Eds.) *Resilience, Crisis and Innovation Dynamics* (pp. 68-89). Cheltenham, United Kingdom: Edward Elgar Publishing. https://doi.org/10.4337/9781786432193.00011

Bērziņš, J. (2020). The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria. *The Journal of Slavic Military Studies*, *33*(3), 355-380. https://doi.org/10.1080/13518046.2020.1824109

The Baltic Center for Investigative Journalism. (n.d.). *About us.* https://en.rebaltica.lv/about-us/

Costa, R. (2021). *Hybrid Threats in the Context of European Security*, Report of the international conference organized at the National Defence Institute (IDN) on 18 May 2021 under the Framework of the Portuguese Presidency of the Council of the European Union. Instituto da Defenca Nacional. https://www.idn.gov.pt/pt/publicacoes/ebriefing/Documents/E-Briefing%20Papers/E-Briefing%20Papers%203.pdf

Council of the European Union. (2019). *Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions* (10 December 2019). Brussels, 10 December 2019 (OR. en) 14972/19. https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf

Cusumano, E. & Corbe, M. (2018). Introduction. In E. Cusumano & M. Corbe (Eds.), *A Civil-Military Response to Hybrid Threats* (pp. 1-14). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-60798-6_1

DeBenedictis, K. (2022). *Russian 'Hybrid Warfare' and the Annexation of Crimea. The Modern Application of Soviet Political Warfare*. London: I.B. Tauris

EEAS. (n.d.). *East StratCom Force*. https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11232

ENISA. (n.d.). *ENISA Mandate and Regulatory Framework*. https://www.enisa.europa.eu/about-enisa/regulatory-framework/legislation

EUR-Lex. (n.d.). *Solidarity Clause*. https://eur-lex.europa.eu/EN/legal-content/glossary/solidarity-clause.html

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. (2013). *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN/2013/01 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001global

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. (2016). *Joint Framework on Countering Hybrid Threats a*

European Union Response (JOIN/2016/18 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018

European Commission. (2018). *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Action Plan against Disinformation* (JOIN/2018/36 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0012

European Commission. (2018). *Joint Report to the European Parliament, the European Council and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats from July 2017 to June 2018* (JOIN/2018/14 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0014R(01)

European Commission. (2019). *Joint Action to Strengthen Health Preparedness and Response to Biological and Chemical Terror Attacks DG SANTE Unit C3 – Crisis Management and Preparedness in Health*. https://ec.europa.eu/chafea/health/funding/joint-actions/documents/ja-2019-presentation-03_en.pdf

European Commission. (2020). *EU Security Union Strategy: Connecting the Dots in a New Security Ecosystem***.** https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

European Commission. (2022). *The 2022 Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

European Council. (2016). *Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization*. https://www.consilium.europa.eu/media/24293/signed-copy-nato-eu-declaration-8-july-en.pdf

European Council. (2018). *Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty organization.* https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf

European Council. (2019). *A New Strategic Agenda for the EU 2019-2024*. https://www.consilium.europa.eu/media/39914/a-new-strategic-agenda-2019-2024.pdf

European Defence Agency. (2017). *First Cyber Exercise at EU Ministerial Level Focuses on Strategic Decision-Making*. https://eda.europa.eu/news-and-events/news/2017/09/07/first-cyber-exercise-at-eu-ministerial-level-focuses-on-strategic-decision-making#:~:text=The%20objective%20of%20EU%20CYBRID,response%20mechanisms%20and%20strategic%20communication

European Parliament. (2016). *Resilience in the EU's Foreign and Security Policy*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/583828/EPRS_BRI%282016%29583828_EN.pdf

European Parliament. (2020). *The EU's Rapid Alert System against Disinformation and how it Functions*. https://www.europarl.europa.eu/doceo/document/E-9-2020-006819_EN.html

European Union External Action Service. (2016). A *Global Strategy for the European Union's Foreign and Security Policy*. https://www.eeas.europa.eu/eeas/global-strategy-european-unions-foreign-and-security-policy_en

European Union External Action Service. (2022). A *Strategic Compass for Security and Defence. For a European Union that Protects its Citizens, Values and Interests and Contributes to International Peace and Security*. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

Europol. *European Cybercrime Centre - EC3*. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Fiott, D., & Parkes, R. (2019). The EU's Response to Hybrid Threats. *Chaillot Papers*, *151*,1-53. https://doi.org/10.2815/679971

Fridman, O. (2018). *Russian 'Hybrid Warfare'. Resurgence and Politicisation*. Oxford: Oxford University Press.

Fox, C. L. (2023). *Hybrid Warfare. The Russian Approach to Strategic Competition & Conventional Military Conflict*. 30-Press Publishing.

Galeotti, M. (2019). *Russian Political War. Moving Beyond the Hybrid*. Routledge: Taylor and Francis.

Giannopoulos, G., Smith H., & Theocharidou. (2021). *The Landscape of Hybrid Threats: A Conceptual Model.* Joint Research Centre. Publications Office of the European Union, Luxembourg. https://doi.org/10.2760/44985

Hedling, E. (2021). Transforming Practices of Diplomacy: The European External Action Service and Digital Disinformation. *International Affairs*, *97*(3), 841–859. https://doi.org/10.1093/ia/iiab035.

Hindren, R. (2021). *Calibrating the Compass: Hybrid Threats and the EU's Strategic Compass* (Hybrid CoE Working Paper 12*)*. The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2021/10/Hybrid_CoE_Working_Paper_12_Calibrating_the_compass_WEB.pdf

Hoffman, F. G. (2007). *Conflict in the 21st Century. The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.

Hoffman, F. G. (2009a). Hybrid vs. Compound War. The Janus Choice: Defining Today's Multifaceted Conflict. *Armed Forces Journal*. http://armedforcesjournal.com/hybrid-vs-compound-war/

Hoffman, F. G. (2009b). Hybrid Warfare and Challenges. *Joint Forces Quarterly*, *52*, 34-39. https://apps.dtic.mil/sti/tr/pdf/ADA516871.pdf

Hybrid CoE. (n.d.). *What is Hybrid CoE?* https://www.hybridcoe.fi/who-what-and-how/.

Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., & Giannopoulos G. (2023). *Hybrid Threats: A Comprehensive Resilience*

Ecosystem. Publications Office of the European Union, Luxembourg. https://doi.org/10.2760/37899

Kalniete, S., & Pildegovičs, T. (2021). Strengthening the EU's Resilience to Hybrid Threats. *European View*, *20*(1), 23–33. https://doi.org/10.1177/17816858211004644

Lonardo, L. (2021). EU Law Against Hybrid Threats: A First Assessment. *European Papers*, *6*(2), 1075-1096, https://doi.org/10.15166/2499-8249/514

McMahon, L., Kleinman, Z., & Subramanian, C. (2025). *Facebook and Instagram Get Rid of Fact Checkers.* BBC News. https://www.bbc.com/news/articles/cly74mpy8klo

Mészáros, E. L., & Țoca, C. V. (2023). The EU's Resilience and the Management of Hybrid Threats Coming from the Eastern neighbourhood: Belarus and the Deliberate Facilitation of Irregular Immigration. *Eastern Journal of European Studies*, *14*(1), 5-30. https://doi.org/10.47743/ejes-2023-0101

Najzer, B. (2020). *Hybrid Age. International Security in the Era of Hybrid Warfare*. London: I. B Tauris.

NATO. (2017). *NATO Summit Key Decisions.* https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf

NATO Watch. *Hybrid CoE*. https://natowatch.org/newsbriefs/2017/european-centre-excellence-countering-hybrid-threats-opens-helsinki

Ostárková. J., & Staníčková, M. (2021). How Well Do We Know the Issue of Resilience? Literary Research of Current Levels of Knowledge. *Eastern Journal of European Studies*, *12*(SI), 12-41. https://doi.org/10.47743/ejes-2021-si02

Pulido Gragera, J. (2019). The Concept of Criminal Insurgency as New Challenge of the International Security. In D. Garcia Cantalapiedra (Ed.) *The Greater Maghreb. Hybrid Threats, Challenges and Strategy for Europe* (pp. 97-111). New York: Lexington Books. http://hdl.handle.net/11268/8306

Rácz A. (2015). *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*. The Finnish Institute of International Affairs. https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf

Renz, B. (2016). Russia and 'Hybrid Warfare'. *Contemporary Politics*, *22*(3), 283-300. https://doi.org/10.1080/13569775.2016.1201316

Rinelli, S., & Duyvesteyn I. (2018). The Missing Link: Civil-Military Cooperation and Hybrid Wars. In E. Cusumano & M. Corbe (Eds.), *A Civil-Military Response to Hybrid Threats* (pp. 17-39). Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-60798-6_2

Wilkie, R. (2009). Hybrid Warfare: Something Old, Not Something New. *Air and Space Power Journal*, *23*(4), 13-18.

Von Clausewitz, C. (2007). *On War* (M. Howard & P. Paret, Trans.; Abridged ed.; B. Heuser, Intro. & notes). Oxford University Press.

Wigell, M., Harri, M., & Juntunen, T. (2021). *Best Practice in the Whole-of-Society Approach in Countering Hybrid Threats.* DG for External Policies.

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf

Zandee, D, Van der Meer, S., & Stoetman, A. (2021). *Countering Hybrid Threats Steps for Improving EU-NATO Cooperation*. Netherlands Institute of International Relations. https://www.clingendael.org/sites/default/files/2021-10/countering-hybrid-threats.pdf

HOW TO CITE:
Mészáros, E. L., & Țoca, C. V. (2025). Toward a systemic framework for evaluating the European Union's resilience to hybrid threats. *Eastern Journal of European Studies, 16*(02), 58-78. https://doi.org/10.47743/ejes-2025-0203