ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2024 (36)

COUNTERING HYBRID THREATS: PROBLEMATIC ASPECTS IN THE EUROPEAN REGION

Eglė ŠTAREIKĖ
Mykolas Romeris University
Maironio str. 27, LT-44211 Kaunas, Lithuania
E-mail: egle.stareike@mruni.eu
ORCID ID:0000-0001-7992-991X

DOI: 10.13165/PSPO-24-36-17

Abstract. *Countering hybrid threats is a complex and multifaceted challenge that requires a comprehensive and coordinated approach. Europe, like other regions, has been actively working to develop strategies and take steps to counter hybrid threats. General measures and priorities framework for countering hybrid threats may vary from one country to another based on their unique circumstances and vulnerabilities. Moreover, the evolving nature of hybrid threats requires a continuous reassessment of strategies and the ability to adapt to new challenges as they arise.*

This scientific article aim is to to analyze the hybrid threats influence to European Union's security environment and identify problematical aspects of countering hybrid threats. In order to achieve these goals, there will be analyzed international documents and scientific articles defining the concept of hybrid threat and general steps and measures that European countries and institutions have been considering and implementing to counter hybrid threats, the scale of the problem and possible solutions are reviewed in this research paper.

Keywords: *hybrid threats, the influence of hybrid threats, European Union's security environment, countering hybrid threats.*

Introduction

Europe faces growing and increasingly complex security challenges. Hybrid threats have become an integral part of our security challenges: war has returned to Europe, instability is growing in Europe's neighbouring regions, attempts to manipulate election results are emerging and democracies are increasingly portrayed as weak governance systems. The ability to spread disinformation quickly and widely through social media further increases the potential impact of hybrid threats. Furthermore, our increasing reliance on information technology tools for everyday work, banking, healthcare management, as well as elections and governance means that every European, Member State and business is at risk of being exposed to hybrid threats *(Jungwirth et.al, 2023).*

Hybrid threat actors are typically characterized by their desire to 1) undermine the integrity and functioning of democracies and undermine citizens' trust in democratic institutions; 2) manipulate established decision-making processes by blurring situational awareness, exploiting gaps in information flows, intimidating individuals and creating fear in target communities; 3) maximize impact by creating a cascading effect, in particular by tailoring attacks, combining elements from specific domains to overload even the best-prepared systems with unpredictable, negative consequences *(Jungwirth et.al, 2023).*

In the light of the above, this article analyzes the definitions of the hybrid threat and hybrid warfare, the importance of the influence of hybrid threats and European Union's security environment, as well as the problematic aspects of this regulation. The third part of the article analyzes general steps and measures that European countries and institutions have been considering and implementing to counter hybrid threats.

The relevance of this scientific article is associated with ensuring the implementation of the requirements for European Union's security environment and identifying the nature of the problematical aspects of general steps that European countries and institutions have been considering and implementing to counter hybrid threats.

The purpose of this scientific article is to analyze the hybrid threats influence to European Union's security environment and identify problematical aspects of countering hybrid threats. In order to achieve these goals, there will be analyzed international documents and scientific articles defining the concepts of hybrid threat and general steps and measures that European countries and institutions have been considering and implementing to counter hybrid threats, the scale of the problem and possible solutions are reviewed in this research paper.

The subject of the scientific article is problematical aspects of countering hybrid threats.

The following theoretical and empirical methods are used in the scientific article: the method of comparative analysis, logical - analytical and systematic analysis. The comparative analysis method was used to compare the concepts of hybrid threat and hybrid warfare. The logical-analytical method analyzes the importance of countering hybrid threats to European Union's security environment. Logical-analytical and systematic analysis methods are used to reveal the problematical aspects of international agreements and scientific doctrine, summarize the scientific article, reveal the main problem, and formulate conclusions.

The importance of the influence of hybrid threats

Hybrid threats refer to a complex blend of conventional and non-conventional tactics employed by state and non-state actors to undermine the security, stability, and interests of targeted entities. Hybrid action is characterized by ambiguity as hybrid actors blur the usual borders of international politics and operate in the interfaces between external and internal, legal and illegal, peace and war. The ambiguity is created by combining conventional and unconventional means – disinformation and interference in political debate or elections, critical infrastructure disturbances or attacks, cyber operations, different forms of criminal activities and, finally, an asymmetric use of military means and warfare (NATO. Countering hybrid threats, 2024).

„Hybrid Threats is a broad overarching concept that includes many types of activity: interference, influence, operations, campaigns and warfare/war. All of these activities can be seen as unwelcome interventions of one sort or another to a country's internal space. We need to keep in mind that the term Hybrid Threats is a Western concept used to discuss a security dilemma that states face that either has a democratic state system or are in the democratization phase“ (Giannopoulos et.al, 2020). Hybrid threats revolve around ideas like asymmetry, polymorphism, inequality, unaccountability, escalation, adaptability, multidimensionality, insidiousness, undetectability, gradualism, offensiveness, concealment, secrecy, ambiguity, opportunism, indeterminacy, disruption, manipulation, distortion, denial, ungovernability, misinformation, unlawfulness, usurpation, and amorality, etc. (Council of Europe, 2018). The concepts of hybrid threats and hybrid warfare are not synonymous but related.

Hybrid warfare is a broader concept that encompasses the strategic use of hybrid threats as part of a comprehensive military strategy. It typically involves the integration of multiple dimensions of conflict (e.g., political, military, informational) to destabilize an opponent and achieve specific aims, often without triggering a full-scale war (Caliskan, 2019).

It is important that the elements of hybrid warfare are implemented through hybrid threats. Their manifestations are shown in Table1. Hybrid threats.

Table 1. Hybrid threats

Hybrid warfare elements are implemented through these hybrid threats:	**Absence of a clear hierarchy and structure of the enemy**
	Propaganda and disinformation, manipulation of mass media
	Cyber attacks
	Espionage
	Psychological attacks
	Subversive activities
	Employment of culture, languages and religion by emphasizing differences
	Energy policy
	Influencing elections and political process
	Employment of criminal groups and organized crime
	Military pressure
	Coordinated activity of special forces, proxy groups, mercenaries, guerillas; combined and coordinated employment of overt and covert military paramilitary and civilian means
	Employment of means of economic, financial, social pressure and asymmetric tactics
	Actions to exploit the vulnerability of a country or region in order to influence or destabilize the enemy, hinder decision making and thus achieve the set tasks
	All forms of fighting are integrated into one battlefield and take place simultaneously
	Creation of equivocation, ambiguity
	Avoidance of an open conflict when the aggressor is clearly identifiable
	Achievement of objectives by avoiding the declaration of war, attracting the least attention of the international community, reducing conflict costs to the maximum
	Nuclear blackmail that might be used having started a hybrid assault and achieved certain results in deterring the enemy from attempted active actions
	Propaganda and disinformation, manipulation of mass media

Source: Bajarūnas, Keršanskas, 2018

The intensifying conflict of values between the West and authoritarian states undermines international norms and institutions and turns open Western societies into targets of comprehensive hybrid action. A conflict of values that extends to the domestic sphere of Western societies increases polarization and disunity within and among Western actors, making them more vulnerable to external interference. Recent developments in modern technology and an increasingly complex information environment provide powerful instruments for hybrid actors if not adequately countered by the Western community *(Aukia, Kubica, 2023)*.

The focus is on the behaviours, activities and tools how hostile state actors use influence tools in ways attempting to subvert democracy, sow instability, or curtail the sovereignty of other nations and the independence of institutions. These threats often combine elements such as cyberattacks, disinformation campaigns, economic coercion, proxy warfare, and more. The influence of hybrid threats can be profound and far-reaching, affecting internal security, the economy, and international relations in various ways *(Giannopoulos et.al, 2020).*

Evidence of constant cyber-attacks, disinformation campaigns, interference in democratic processes and the mobilization of migrants at the external borders of the European Union have seriously damaged EU-Russia relations. Hybrid attacks blur the lines between war and peace. They exploit the opportunities of an interconnected and globalised world to weaken the enemy without wasting resources on the conventional battlefield *(Bargués, P., Bourekba M., Colomina, 2022).*

The importance of countering hybrid threats: European Union's security environment

Countering hybrid threats is a complex and multifaceted challenge that requires a comprehensive and coordinated approach. Europe, like other regions, has been actively working to develop strategies and take steps to counter hybrid threats. General measures and priorities framework for countering hybrid threats may vary from one country to another based on their unique circumstances and vulnerabilities. Moreover, the evolving nature of hybrid threats requires a continuous reassessment of strategies and the ability to adapt to new challenges as they arise. Governments and international organizations are increasingly recognizing the importance of countering hybrid threats through a combination of diplomatic, economic, informational, and military measures. This requires cooperation between nations, the development of resilient societal structures, investment in cybersecurity and intelligence capabilities, and a comprehensive approach to managing both conventional and unconventional threats *(Jungwirth et al, 2023).*

It's worth noting that the impact of hybrid threats can vary depending on the specific circumstances, the actors involved, and the targeted country's vulnerabilities and resilience. As tactics evolve and new technologies emerge, understanding and addressing these threats will remain an ongoing challenge for policymakers and security experts. When it comes to understanding the different dimensions, activities, domains, tools, goals and nature of actors, the role of intelligence is essential to achieve a proper understanding of the situation, which in turn enables an ecosystem-based approach. All critical areas are addressed synergistically to build sufficient resilience. Countering hybrid threats relies on four distinct elements – understanding (situational awareness), resilience, deterrence and cooperation- which relate to the stages of hybrid actor activity *(EU, Countering hybrid threats, 2024):*

1. *Understanding hybrid threats* means recognizing their nature, objectives, and methods. Hybrid threats are often ambiguous, involving both state and non-state actors, with tactics that blend conventional warfare, cyberattacks, disinformation, economic pressure, and social manipulation.
2. *Building resilience* requires a whole-of-government and whole-of-society approach that focuses on addressing identified vulnerabilities. Resilience refers to a society's or system's ability to absorb, adapt to, and recover from hybrid threats. Strengthening resilience means minimizing vulnerabilities in critical sectors such as energy, communications, finance, and public institutions *(Jungwirth, 2023).*
3. *Deterrence* aims to prevent hybrid threats from being executed by increasing the costs for potential aggressors and reducing their incentives to engage in hybrid warfare. The EU Cyber Diplomacy Toolbox is an example of deterrence in practice. It allows the EU to impose diplomatic measures, including sanctions, on entities responsible for cyberattacks, thus increasing the potential costs for attackers and deterring future attacks *(The Cyber Diplomacy Toolbox, 2024).*

4. *Cooperation* involves working together at the national, regional, and international levels to counter hybrid threats. No single country can effectively combat hybrid threats alone, as they often cross borders and involve multiple actors *(EU, Countering hybrid threats, 2024).*

It is also important to understand that all EU countries must be prepared to deal with these threats, as one unprepared country remains vulnerable the whole block. In this regard, continuous lessons learned and established processes, technical solutions and innovations are vital to strengthen all three aspects.

An analysis of the complex challenges facing the EU and NATO encouraged both organizations to create a comprehensive approach that combines all the important things actors and means available: military forces, diplomacy, humanitarian aid, political processes, economic development and technology. Countering hybrid threats aims to acquire a new ones understanding of such threats and innovative leveraging existing opportunities, many of which are how economic development, anti-corruption or poverty eradication - live in non-military governmental and intergovernmental institutions agencies, the private sector and international non-governmental organizations *(EU, Countering hybrid threats, 2024).*

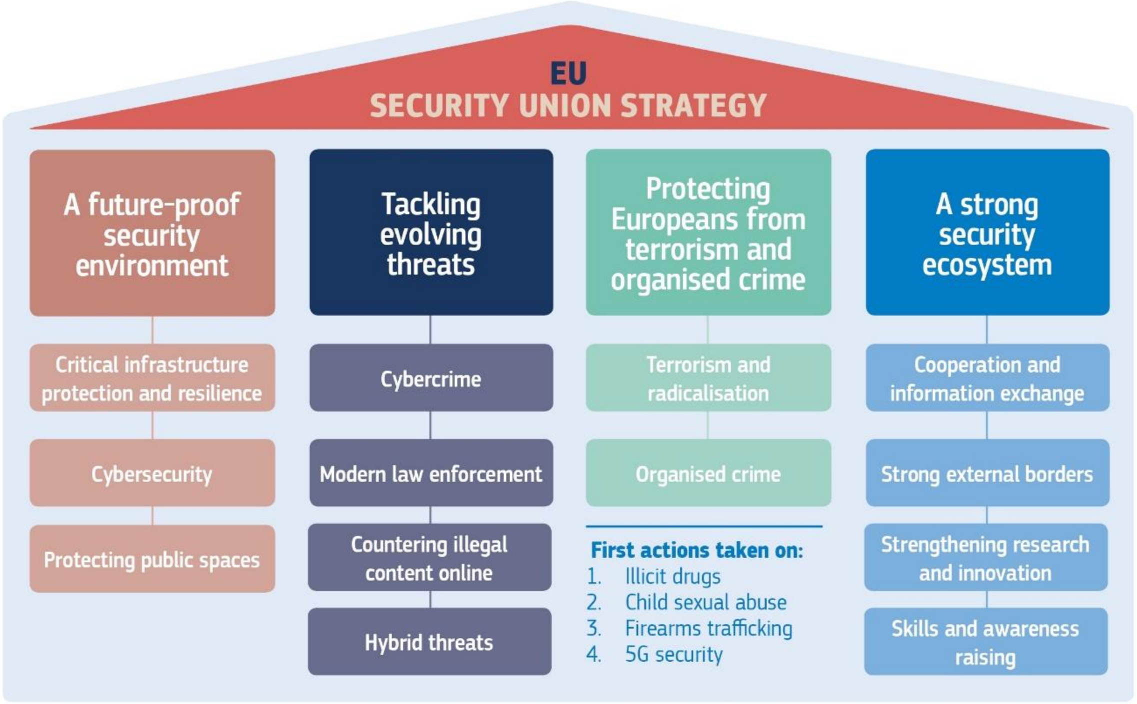
The EU approach to hybrid threats is set out in the 2016 Joint Framework (European Commission, 2016) and the 2018 Joint Communication on bolstering hybrid resilience (European Commission, 2018). The responsibility for combating hybrid threats rests primarily with Member States – due to the fundamental links with national security and defence policy, some vulnerabilities are common to all Member States, and some threats spread cross-border, for example, targeting cross-border networks or infrastructure. The Commission develop an EU approach to hybrid threats that seamlessly integrates external and internal dimensions and combines national and EU-wide dimensions. This covers the full range of activities, from early detection, analysis, awareness, resilience building and prevention to crisis response and consequence management *(European Commission, 2020).*

However, many Member States face common threats that can be more effectively addressed at the EU level. The EU can be used as a platform to strengthen national efforts and, through its regulatory capacity, to establish common guidelines that can help increase the level of protection and resilience worldwide EU. This is why the EU can play an important role in improving our collective situational awareness strengthening Member States' resilience to hybrid threats and prevention, response and recovery from the crisis. In addition to enhanced implementation, in the face of ever-evolving hybrid threats, special attention will be paid to incorporating hybrid considerations into policy-making, keeping up with dynamic changes and ensuring that no potentially important initiative is overlooked *(European Commission, 2016).*

Hybrid threats have manifested in EU politics in the last decade and has led to dramatic changes in the security environment of the European Union and the need for the Union to adapt accordingly. „The 2015 Council Conclusions on CommonSecurity and Defence Policy called for a 'joint framework with actionable proposals to help counter hybrid threats and foster the resilience of the EU and Member States, as well as partners' *(Council of the European Union, 2015).* The 'Joint Framework on countering hybrid *threats' (European Commission, 2016)* was published a year later, bringing hybrid threats to the focus of policymaking, and proposing 22 actions to counter hybrid threats, most of which recognised resilience as a key element. This framework was followed by the communication on 'Increasing resilience and bolstering capabilities to address hybrid threats' in which the importance of building resilience to counter hybrid threats was reiterated and expanded to sectors such as CBRN (chemical, biological, radiological and nuclear agents) and cyber threats *(European Commission, 2016; Hybrid threats: a comprehensive resilience ecosystem, 2023).*

In accordance with the 2019 Council conclusion (*Council of the European Union, 2019)*, about 200 measures were noted in the Joint Staff Working Document Mapping of measures related to enhancing resilience and countering hybrid threats was published in 2020 *(European Commission, 2020e).* The main focus is on the relevance and interconnection between the two fields – resilience and hybrid threats – and the efforts made by EU institutions to reinforce them during the last years.

Countering hybrid threats that aim to weaken social cohesion and undermine trust in institutions, as well as enhancing EU resilience are an important element of the Security Union Strategy (Picture Nr. 1). Key measures include an EU approach on countering hybrid threats, from early detection, analysis, awareness, building resilience and prevention to crisis response and consequence management – mainstreaming hybrid considerations into broader policy-making. The Commission and the High Representative will continue to jointly take forward this work, in close cooperation with strategic partners, notably NATO and G7. (*EU Security Union Strategy, connecting the dots in a new security ecosystem, 2020*).


EU
SECURITY UNION STRATEGY
A future-proof security environment
Critical infrastructure protection and resilience
Cybersecurity
Protecting public spaces
Tackling evolving threats
Cybercrime
Modern law enforcement
Countering illegal content online
Hybrid threats
Protecting Europeans from terrorism and organised crime
Terrorism and radicalisation
Organised crime
First actions taken on:
1. Illicit drugs
2. Child sexual abuse
3. Firearms trafficking
4. 5G security
A strong security ecosystem
Cooperation and information exchange
Strong external borders
Strengthening research and innovation
Skills and awareness raising

Picture 1. EU Security Union Strategy

Source: EU Security Union Strategy: connecting the dots in a new security ecosystem, 2020.

The EU Security Union Strategy (2020–2025) replaced the 2016–2020 strategy. This updated document builds on the previous strategy but adapts to new and evolving challenges, particularly focusing on digital transformation, resilience against cyber threats, and addressing hybrid threats. Key focus areas of the 2020–2025 strategy include:

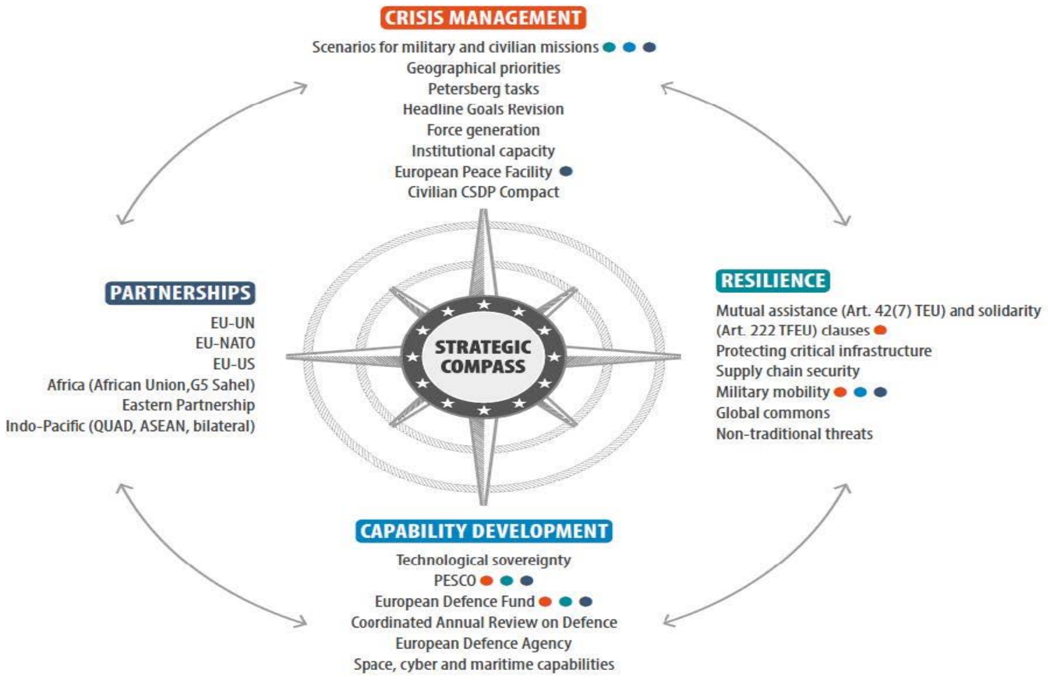
- *Cybersecurity*: stronger measures to protect against cyberattacks and safeguard digital infrastructures.
- *Countering hybrid threats*: continuing efforts to combat disinformation, foreign interference, and cyberattacks, with particular emphasis on strategic communication and public resilience.

- *Combating terrorism*: enhanced collaboration among EU member states to combat terrorism, especially through better intelligence sharing.
- *Resilience in critical cectors*: expanding protections for key sectors like health (in response to COVID-19), energy, and transportation, ensuring they can withstand both physical and cyber threats (Picture Nr. 1).

The process of developing the Strategic Compass was an important step towards strengthening the EU's crisis response capabilities. The aim was to create a modular tool for Member States that would allow them to respond collectively and individually to security threats. The introduction of the Strategic Compass was a watershed moment for the EU, allowing the bloc to defend its interests and protect its citizens in an era of increasing uncertainty *(A Strategic Compass for Security and Defence, 2024).*

The European Council adopted Strategic Compass in March 2022. The Compass set out an assessment of the threats and challenges the EU faces and will propose operational guidelines to enable the EU to become a security provider for its citizens. Having been conceived by the European Council, the Strategic Compass is an attempt to set the strategic vision of the Union from the top-down, while simultaneously building consensus among Member States from the bottom-up, by drawing upon their diverse perspectives to provide an instrument for coordinating their foreign policies *(Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence, 2024).*

In a multidimensional risk landscape that is increasingly characterised by both conventional and novel threats, no individual EU Member State has the strength nor the resources to address these threats alone. In this regard, the Strategic Compass will inform future EU policies and strategies across four work strands: act; secure; invest and partner (Picture Nr. 2).



Picture 2. Strategic Compass process and its baskets
Source: A Strategic Compass for Security and Defence, 2024.

The EU Strategic Compass and the EU Security Union Strategy (2020–2025) both focus on enhancing Europe's security, but they address different areas of concern and have distinct approaches and objectives. EU Strategic Compass focuses on defense and military capabilities. It serves as a military and defense roadmap to strengthen the EU's ability to respond to security threats both within Europe and globally. Also it emphasizes crisis management, enhancing military readiness and strengthening global partnerships with NATO, the UN, and others partners. The EU Strategic Compass focuses on external threats improving the EU's ability to respond to global crises and prioritizes military preparedness, rapid deployment, and coordinated defense efforts. Meanwhile, EU Security Union Strategy (2020–2025) focuses on internal security and emphasizes cybersecurity, counterterrorism, combating organized crime, and resilience against hybrid threats. EU Security Union Strategy‘s scope is more about protecting the EU's society, institutions, and critical infrastructure from threats like cyberattacks, disinformation, and terrorism. Focuses on internal threats such as cyberattacks, disinformation, and organized crime. It emphasizes preventive measures, building resilience, and securing critical sectors.

In essence, the Strategic Compass takes a more defense-oriented and military capabilities, external focus, while the Security Union Strategy deals with internal security and resilience against threats to EU society and infrastructure. focusing on protecting the EU's society and institutions from threats like terrorism, organized crime and cyberattacks.

General steps and measures that European countries and institutions have been considering and implementing to counter hybrid threats

The European security order has changed substantially as the current fundamentals were agreed in the Helsinki Final Act 1975. Although that treaty established the mutual Recognition of Cold War blocs, the application of its principles became a more complicated matter when the balance of power between East and West dramatically question after a more than a decade. From the end of Cold War and the collapse of Warsaw Pact, NATO became the undisputed leader security organization in Europe. Russia's invasion of Ukraine has deepened Europe's already significant dependence on the United States. From today's vantage point, this can be framed as Western unity having been strengthened and NATO having rediscovered its purpose *(Moeini, Paikin, 2023).*

"Russia's brutal invasion of Ukraine is interpreted differently across the alliance. The war is regarded as an existential threat by countries in the Intermarium, which hold historical grievances (and with reason) against Russian imperialism. In Western Europe, it is viewed as an attack on the European continent and community of nations, but not as an existential threat to the same degree. Rather, it is seen more as a significant geopolitical event on Europe's frontier with undesirable cascading effects, such as the flow of refugees, food and energy insecurity, or worst of all, the risk of nuclear escalation. Across the Atlantic, the invasion provides opportunities: the opportunity to weaken a historic, regional adversary, re-galvanize the "liberal international order", renew America's "indispensable" role in the world, and ultimately to reinforce the long-held strategic ontologies of the U.S. establishment." *(Moeini, Paikin, 2023).*

In recent years, more and more US leaders, under some public pressure, have demanded that European countries increase their military spending and pay for the security guarantees that Washington provides through NATO. But there is a certain cognitive dissonance surrounding America's call for greater burden sharing and the fact that a more independent Europe with an autonomous collective security architecture, a robust defence industry, and financial independence from Washington would indeed have responsibility for its security interests. A larger Europe with an independent strategic perspective will be a better asset and a far more effective partner for America in addressing major security challenges in a multipolar world than a Europe which has assumed its junior partner status.

The specific measures and priorities may vary from one country to another based on their unique circumstances and weak points. Moreover, the evolving nature of hybrid threats requires a continuous reassessment of strategies and the ability to adapt to new challenges as they arise. These steps represent considerations that might influence discussions on European security architecture and a general framework for countering hybrid threats in Europe:

1. *Strengthening intelligence sharing* both among European countries and with international partners is crucial. This allows for early detection and a better understanding of hybrid threats.

2. *Establishing early warning systems* to detect and respond to hybrid threats quickly is essential. This includes monitoring information operations, cyber threats, and other unconventional tactics.

3. *Resilience Building.* Investing in societal resilience is vital. This involves educating the public to recognize disinformation, reinforcing critical infrastructure against cyber-attacks, and fostering social cohesion to resist divisive tactics. „The concept of resilience has just as many meanings as hybrid threats. Resilience is about states and societies resisting collapse under the impact of disastrous events. They have to cope and deal with such events, adapt to them, and recover from their effects in a short period of time. It is obvious that post-facto resilience is only possible if state and society are able to anticipate the potential consequences of a series of events, be it man-made, a natural disaster, or an external challenge, like a crisis or war. Consequently, resilience is contextual; it has many forms dependent upon the context. Resilience has much to do with state capacity, governance, and the cohesion and thus the support of society for its state institutions and leaders.“ *(Dunay, Roloff, 2017).*

4. *Strengthening national and regional cyber security* capabilities is paramount. This includes the development of robust cyber defense mechanisms and cyber hygiene practices. On the production side of disinformation, the European Union approved in April 2022 a new legislative package to strengthen EU’s response to disinformation: the Digital Markets Act (DMA) and the Digital Services Act (DSA), that includes an updated Code of Practice on Disinformation which aims to tackle the spread of disinformation across technology platforms by making the platform owner (such as Meta, Twitter, etc.) liable for not curbing the spread of disinformation at its root (Bargués, Bourekba,Colomina, 2022).

5. *Effective strategic communication* is key to countering disinformation and propaganda. European countries have been working on communication strategies to counter false narratives and promote accurate information.

6. *Developing and updating legislation and regulations* to address hybrid threats, including laws related to cyber security, foreign interference, and election integrity. Given the presence of hybrid threats, a traditional rule-based approach may not be sufficient. Hybrid threats exploit the vacuum of law, but law is needed to address these same threats. This is because applicable international law is contested by both non-state and state actors using hybrid threats to achieve their goals, with one of the most recent examples of this being the actions of Russia in Ukraine. By annexing Crimea in 2014 and Donetsk, Kharkiv, Kherson, Luhansk, Mykolaiv, and Zaporizhzhia in 2022 and 2023, Russia has violated the principles of international law. Later, by artificially issuing Russian passports to residents of annexed territories of Ukraine, to a large extent, Russia created a basis to invoke its right to defend its citizens living abroad and to support these regions by declaring independence from Ukraine. Russia is the leader in using legal arguments in support of hybrid tactics. One of his favourite hybrid tactics is raising doubts about whether a certain action is legal under international law.

(*Janičatova, Mlejnkova, 2021; Sanz-Caballero, 2023.).* Using democratic norms and standards against democracy itself is a weaponization of the law. The right presupposes abuse of legal proceedings as a weapon of mass disinformation. This manipulation of norms has a pernicious, despicable effect on democratic societies. A deliberate misinterpretation of law is often intended to change customary law through state practice. What makes it a hybrid threat is any malicious intent to weaken states, subvert democratic governments, annexe territories, breach previous international agreements, or maliciously access other markets, etc. *(Sanz-Caballero, 2023).*

7. *Collaborating with international partners*, including NATO and the EU, to share best practices and coordinate responses to cross borders hybrid threats. A hybrid response requires that, in the absence of a clearly identified enemy, Western governments allocate public resources to target them. It is much easier for the other side, such as Russia, to do so simply because of its authoritarian nature. The classic strengths of Western governments are openness, an institutionalized decision-making process, attention to legal constraints, and accountability through legitimately elected legislative bodies. However, it does not always help to effectively respond to hybrid threats. As we can see, the Western response, although appropriate, is for these reasons slower than the security situation requires *(Bajarūnas, Keršanskas, 2018).*
8. *Strengthening economic resilience* against economic coercion and sanctions by diversifying trade partners and investing in industries critical to national security.
9. *Public and Private Sector Engagement.* Engaging the private sector, particularly technology companies, in efforts to combat disinformation, strengthen cyber security and protect critical infrastructure. Public engagement is an important aspect: the defending country must create a more resilient society. The only way to develop societal resilience is to maintain at least some of the home-field advantage, as the aggressor will try to build up and use the surprise effect. Therefore, a long-term plan and dedication to its implementation are required. The opponent must have a strong political mandate and a long-term security concept. Achieving this requires planning, awareness raising and education. Key societal stakeholders have a common understanding of the situation, a common threat and risk assessment, planning and training processes *(Bajarūnas, Keršanskas, 2018,).*
10. *Engaging in diplomatic efforts* to address hybrid threats at the international level, including advocating for norms of behavior in cyberspace.
11. *Protection of Elections and the Political System.* More and more countries are realizing that they are losing the battle for protection of democracy without ensuring a democratic order, free choice thus it will be more difficult to protect against hybrid threats in the future.

Conclusions

Summarizing the international agreements and commitments of the member states, the concept of hybrid threats aims to encompass conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner by state or non-state actors to achieve specific objectives, but below the threshold of formally declaring war. Hybrid methods are used to blur the lines between war and peace and to destabilize and undermine societies.

Countering hybrid threats is a complex and multifaceted challenge that requires a comprehensive and coordinated approach. Europe, like other regions, has been actively working to develop strategies and take steps to counter hybrid threats. Countering hybrid threats relies on four distinct elements – understanding (situational awareness), resilience, deterrence and cooperation- which relate to the stages of hybrid actor activity. It is important to understand that all EU countries must be prepared to deal with these threats, as one unprepared country remains vulnerable the whole block. In this regard, continuous lessons learned and established processes, technical solutions and innovations are vital to strengthen all three aspects.

Specific measures and priorities may vary from country to country, taking into account their unique circumstances and vulnerabilities. Furthermore, the evolving nature of hybrid threats requires a constant reassessment of strategies and the ability to adapt to new challenges as they arise. The following steps can be identified as potentially influencing the debate on the European security architecture and a common framework for countering hybrid threats in Europe: strengthening intelligence sharing, establishing early warning systems, resilience building, strengthening cyber security improvements, effective strategic communication and international cooperation, economic resilience building, public and private sector engagement, diplomatic efforts engagement, protection of elections and the political system.

Acknowledgements. This article was funded by Erasmus + project HYBRIDC (Cooperation for Developing Joint Curriculum on Tackling Hybrid Threats), implemented by Mykolas Romeris University (partner) in cooperation with Police Academy of the Ministry of the Interior of Croatia, coordinator Estonian Academy of Security Sciences (EASS).

References

1. Aukia, J., Kubica, L. 2023. Russia and China as hybrid threat actors: The shared self-other dynamics. *The European Centre of Excellence for Countering Hybrid Threats*. Available at: https://www.hybridcoe.fi/wp-content/uploads/2023/04/NEW_Hybrid_CoE_Research_Report_8_web.pdf (Accessed: 16 September 2024).
2. Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence. 2024. Report of the High Representative of the Union for Foreign Affairs and Security Policy to the Council. Available at: https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2ndYear_Report_0.pdf (Accessed: 22 September 2024).
3. A Strategic Compass for Security and Defence. 2024. The Diplomatic Service of the European Union. Available at: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en (Accessed: 22 September 2024).
4. Bajarūnas, E., Keršanskas, B. 2018. *Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome.* Lithuanian Annual Strategic Review, Volume 16, Issue 1 (pp. 123–170). https://doi.org/10.2478/lasr-2018-0006 Available at: https://journals.lka.lt/journal/lasr/article/152/info (Accessed: 1 August 2024).
5. Bargués, P., Bourekba M., Colomina, C.(eds.) 2022. *Hybrid threats, vulnerable order* CIDOB *report # 08* CIDOB. Available at: ttps://www.cidob.org/en/publications/publication_series/cidob_report/cidob_report/hybrid_threats_vulnerable_order (Accessed: 22 September 2024).
6. Caliskan, M. 2019. Hybrid warfare through the lens of strategic theory. Defense & Security Analysis, 35(1), 40–58. Available at: https://doi.org/10.1080/14751798.2019.1565364 (Accessed: 2 September 2024).
7. Council of the European Union. 2015. ‘Council Conclusions on CSDP’, Foreign Affairs Council, 8971/15, pp. 1-16. Available at: https://data.consilium.europa.eu/doc/document/ST-8971-2015-INIT/en/pdf (Accessed: 30 August 2024).

8. Countering hybrid threats. 2023. NATO. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm (Accessed: 30 August 2024).
9. Dunay, P., Roloff, R. 2017. *Hybrid Threats and Strengthening Resilience on Europe's Eastern Flank*. Available at: *https://www.marshallcenter.org/en/publications/security-insights/hybrid-threats-and-strengthening-resilience-europes-eastern-flank-0* (Accessed: 1 February 2024).
10. *EU. Countering hybrid threats, 2024.* Available at: https://www.eeas. europa.eu/sites/default/files/documents/2024/2024-countering-Hybrid-Threats.pdf(Accessed: 15 Octo ber 2024).
11. European Commission, 2016. Fact Sheet: Joint Framework on countering hybrid threats, Brussels, 6 April. Available at http://europa.eu/rapid/press-release_MEMO-16-1250_en.htm (Accessed: 30 August 2024).
12. European Commission. 2016. *FAQ: Joint Framework on countering hybrid threats*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250 (Accessed: 1 February 2024).
13. European Commission. 2020. *Communication from the Commission to the European Parliament, the European Council, the council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy.* COM(2020) 605 final,27. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from =EN. (Accessed: 14 July 2024).
14. European Commission (2020e), Joint Staff Working Document on Mapping of Measures Related to Enhancing Resilience and Countering Hybrid Threats, SWD (2020) 152 final. Available at: https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/swd/2020/0152/COM_SWD (2020) 0152_EN.pdf (Accessed: 15 February 2024).
15. *EU Security Union Strategy: connecting the dots in a new security ecosystem.* 2020. European Commission. Available at: https://ec.europa.eu/commission/presscorner /detail/en/ip_20_1379 (Accessed: 3o August 2024).
16. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G. *Hybrid threats: a comprehensive resilience ecosystem*, 2023. Publications Office of the European Union, Luxembourg, doi:10.2760/37899. Available at: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf (Accessed: 13 September 2024).
17. Janičatová S, Mlejnková P. 2021. *The ambiguity of hybrid warfare: a qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities*. In: Contemporary Security Policy, vol. 42, no. 3, pp. 312–344.
18. Moeini, A., Paikin, Z. 2023. In search of a European security order after the Ukraine war. The Institute for Peace & Diplomacy. Available at: https://peacediplomacy.org/wp-content/uploads/2023/04/In-Search-of-a-European-Security-Order-After-the-Ukraine-War.pdf (Accessed: 1 February 2024).
19. NATO. 2010. "BI-SC Input to a New Capstone Concept for the Military Contribution to Countering Hybrid Threats". Available at: https://www.act.nato.int/images/stories /events/2010/20100826_bi-sc_cht.pdf . (Accessed: 1 October 2024).
20. NATO. 2014. Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. Available

at: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm, (Accessed: 1 October 2024).

21. Sanz-Caballero, S. 2023. *The concepts and laws applicable to hybrid threats, with a special focus on Europe*. Humanities and Social Sciences Communications, Vol. 10, 360 (2023). Available at: https://www.nature.com/articles/s41599-023-01864-y (Accessed: 1 February 2024).

22. The Cyber Diplomacy Toolbox, 2024. Available at: https://www.cyber-diplomacy-toolbox.com/(Accessed: 1 October 2024).