ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2024 (36)

RESPONSE TO HYBRID THREATS: POLICIES, CONCEPTS AND STRATEGIC APPROACHES

Danguolė SENIUTIENĖ
Mykolas Romeris University
Maironio str. 27, LT-44211 Kaunas, Lithuania
E-mail: dseniutiene@mruni.eu
ORCID ID: 0000-0002-7572-5239

Laima PAULAUSKYTĖ
Mykolas Romeris University
Maironio str. 27, LT-44211 Kaunas, Lithuania
E-mail: laima_paula@mruni.eu
ORCID ID: 0009-0007-1477-8963

DOI: 10.13165/PSPO-24-36-14

Abstract*. In a changing security environment in Europe, hybrid threats have become a major challenge that requires a comprehensive and adaptive response. Hybrid threats include conventional and unconventional approaches, such as cyberattacks, disinformation campaigns, conspiracy theories, economic coercion, and external warfare, to undermine security, stability and democratic institutions in the region.*
Disinformation campaigns or conspiracy theories can be constructed for strategic purposes (for example: to inform or warn others) in order to manipulate, provoke and target specific people or groups for financial or political reasons. Especially in less democratic countries, the purpose of conspiracy theory is to create a feeling that there is a gap between those citizens who feel excluded from decision making or feel powerless of their choices, while decreasing their intention to be included into the political process of voting. However, on the other hand, conspiracy theory can be used as a tactic for politicians, too. A great example is a example of Hungary, where politicians were using the Great Replacement conspiracy theory against refugees and EU policies mobilizing Hungarians to achieve his political goals.
The changing nature of hybrid threats poses complex challenges to European security, as they blur the boundaries between military and non-military action, state and non-state actors, and the physical and virtual spheres.
This article analyses the possible response to hybrid threats, introducing the main actors, under discussions true the policies, concepts and strategic approaches, main focusing on the case of Europe. The article reviews different theories, discussing key concepts and possible cooperation frameworks and the analysis of the legal regulation.

Keywords: *security, hybrid threats, conspiracy theories.*

Introduction

The global security environment is becoming more contested, complex and interconnected. As armed conflicts and civil wars re-emerge even on the EU's neighbourhood, new and unconventional security threats have emerged or grown stronger, including cyber-attacks, hybrid threats, terrorism, disinformation, conspiracy theories, climate change or artificial intelligence. In an increasingly interconnected world, Europe's security starts abroad. (EEAS, 2023).

There is a strong link between what happens outside of the EU's borders and security within Europe. In a rapidly changing world, security challenges have become more complex, multidimensional. When it comes to security, the interests of all Member States are inseparably linked. The EU made security a priority in its Global Strategy and has been working over the past years to create the conditions for Member States to collaborate more closely with each other on security and defence. (EEAS, 2023).

In other words, hybrid threats, disinformation, conspiracy theories and attacks are coordinated actions that exploit the thresholds of detection and attribution designed to further

strategic goals by deliberately targeting vulnerabilities. They cover a broad spectrum of techniques used by malign actors to compromise security, undermine decision-making processes and destabilise democratic institutions. (Lisboa, 2023).

As highlighted by recent example, such as the weaponisation of migration at the Belarusian border, hybrid threats are often hard to pin down and deliberately target states' vulnerabilities. Thus, EU Policy creating common recommendations to improve the attribution of hybrid attacks and to develop a coordinated strategy for addressing critical vulnerabilities across the European Union. This key to making states more capable to withstand and recover from shocks.

The COVID-19 crisis has also reshaped our notion of safety and security threats and corresponding policies. It has highlighted the need to guarantee security both in the physical and digital environments. It has underlined the importance of open strategic autonomy for our supply chains in terms of critical products, services, infrastructures and technologies. It has reinforced the need to engage every sector and every individual in a common effort to ensure that the EU is more prepared and resilient in the first place and has better tools to respond when needed.

Citizens cannot be protected only through Member States acting on their own. Building on our strengths to work together has never been more essential.
The work must also go beyond the EU's boundaries. Protecting the Union and its citizens is no longer only about ensuring security within the EU borders, but also about addressing the external dimension of security. (European Commission 2020, p. 2-3).

Our daily lives depend on a wide variety of services – such as energy, transport, and finance, as well as health. These rely on both physical and digital infrastructure, adding to the vulnerability and the potential for disruption. During the COVID-19 pandemic, new technologies have kept many businesses and public services running, whether keeping us connected through remote working or maintaining the logistics of supply chains. But this has also opened the door to an extraordinary increase in malicious attacks, attempting to capitalise on the disruption of the pandemic and the shift to digital home working for criminal purposes. (European Commission 2020, p. 3-4).

The COVID-19 crisis has also underlined how social divisions and uncertainties create a security vulnerability. This increases the potential for more sophisticated and hybrid attacks by state and non-state actors, with vulnerabilities exploited through a mix of cyber-attacks, damage to critical infrastructure, conspiracy theories, disinformation campaigns, and radicalisation of the political narrative.

The aim of the present article will analyse the policy, concept and strategies of possible response to hybrid threats. The scientific literature and legal acts analytical methods were used to develop the topic and provide conclusions.

Hybrid threats concepts in EU policy

While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, conspiracy theories, using

social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats.

This a particular problem with the EU's use of hybrid threat terminology is the way it fails to distinguish between different forms of hybrid threats, thereby making it difficult for policymakers to delineate institutional responsibilities and formulate more targeted countermeasures. Hence, the EU now needs to address some of these conceptual challenges involved with the mapping of hybrid threats. One specific question concerns the need to systematise terminology. EU hybrid threat analysis needs to solve the problem of creating analytic differentiation in order to facilitate the identification of empirical variation between different hybrid threat types. (Wigell, Mikkola, Juntunen, 2021).

There is no legally bounding definition on hybrid threats in the EU, but good common understanding: „Hybrid threats refer to a wide range of methods or activities used by hostile state or non-state actors in a coordinated manner in order to target the vulnerabilities of democratic states and institutions, while remaining below the threshold of formally declared warfare. Some examples include cyber-attacks, election interference and disinformation campaigns, including on social media." (Council Press Release 2019).

Insofar as countering hybrid threats relates to national security and defence and the maintenance of law and order, the primary responsibility lies with Member States, as most national vulnerabilities are country-specific. However, many EU Member States face common threats, which can also target cross-border networks or infrastructures. Such threats can be addressed more effectively with a coordinated response at EU level by using EU policies and instruments, to build on European solidarity, mutual assistance and the full potential of the Lisbon Treaty.

Joint Communication (European Commission 2016) aims to facilitate a holistic approach that will enable the EU, in coordination with Member States, to specifically counter threats of a hybrid nature by creating synergies between all relevant instruments and fostering close cooperation between all relevant actors[1]. The proposed response focuses on the following elements:

- ✓ improving awareness ("It is essential that the EU, in coordination with its Member States, has a sufficient level of situational awareness to identify any change in the security environment related to hybrid activity caused by State and/or non-state actors. To effectively counter hybrid threats, it is important to improve information exchange and promote relevant intelligence-sharing across sectors and between the European Union, its Member States and partners".),
- ✓ building resilience (Resilience is the capacity to withstand stress and recover, strengthened from challenges. To effectively counter hybrid threats, the potential vulnerabilities of key infrastructures, supply chains and society must be addressed. By drawing on the EU instruments and policies, infrastructure at the EU level can become more resilient.),
- ✓ preventing (Analyse relevant indicators to prevent and respond to hybrid threats and inform EU decision-makers.),
- ✓ responding to crisis and recovering (A rapid response to events triggered by hybrid threats is essential. When preparing their forces, Member States are encouraged to take potential hybrid threats into account. To be prepared to take decisions swiftly and

[1] Possible legislative proposals will be subject to Commission better regulation requirements, in line with Commission's Better Regulation Guidelines, SWD(2015) 111

effectively in case of a hybrid attack, Member States need to hold regular exercises, at working and political level, to test national and multinational decision-making ability).

Member States are predominantly responsible to respond to hybrid threats by enhancing their resilience, and detecting, preventing and responding to hybrid threats. The Commission plays an important role in providing coordinated responses at EU level in cases where many EU Member States face common threats, which can also target cross-border networks or infrastructures. The EU complements national efforts with policy initiatives, best practices, and facilitating coordination among Member States.

The main pillars of the EU response are: enhancing situational awareness, boosting resilience in all critical sectors, providing for an adequate response and recovery in case of crisis and cooperation with like-minded countries and organisations, incl. the North Atlantic Treaty Organisation.

The European Commission coordinates and develops policy initiatives on several key issues within its competences e.g. protection of critical infrastructure, cybersecurity measures, tackling (online) disinformation, securing free and fair elections, etc.

Since 2016, the Commission together with the High Representative of the Union for Foreign Affairs and Security Policy has set up a broad array of measures to counter hybrid threats in a substantial number of policy areas through the 2016 *Joint Framework on countering hybrid threats – a European Union response* and the 2018 *Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats.* In addition, the 2020 *EU Security Union Strategy* announced a new approach based on mainstreaming hybrid threats considerations into all policy initiatives.

The aim of hybrid threat activity is to constrain the freedom of manoeuvre of democracies in order to discredit its model compared to authoritarian regimes. Therefore, the aim and intent of the hostile actor is to:

- undermine and harm the integrity and functioning of democracies, by targeting vulnerabilities of different domains, creating new vulnerabilities through interference activity, exploiting any seams, creating maximum ambiguity and undermining trust of citizens in democratic institutions;
- change the decision-making processes, by blurring situational awareness, exploiting gaps in information flows, intimidating individuals and creating fear factors in target societies;
- create cascading effects by using a tailor-made combination from the 13 domains of the conceptual model to challenge and overload even the best-prepared systems. This can result in unpredicted consequences (European Commission and, 2023).

Insofar as countering hybrid threats relates to national security and defence, the primary responsibility lies with Member States, as most national vulnerabilities are country-specific. 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 boost national efforts and, through its regulatory capacity, establish common benchmarks that can help raise the level of protection and resilience across the EU. That's why the EU can play an important role in improving our collective situational awareness, in building Member States' resilience to hybrid threats, and in preventing, responding to and recovering from crisis.

One key aspect of the EU's response to hybrid threats is the establishment of the EU Hybrid Fusion Cell, a platform for information sharing and coordination among member states

to identify and respond to hybrid threats effectively. This framework enables swift and coordinated action in the face of multifaceted challenges. (European Commission, 2019).

The EU has also prioritized strategic communication and public diplomacy as essential tools in countering disinformation and propaganda campaigns that often accompany hybrid threats. By enhancing its communication strategies and promoting transparency, the EU aims to build societal resilience against manipulation and misinformation. (European Commission, 2019).

In response to major geopolitical shifts at work and an increasingly degraded security environment, the EU adopted an ambitious action plan to strengthen its security and defence policy by 2030. The Strategic Compass is the result of work started in 2020 among the institutions and Member States, and is based on a common analysis of the threats and vulnerabilities that Europeans are faced with collectively. This unprecedented exercise in the history of the EU contributed to the emergence of a common strategic culture and the strengthening of cohesion among Europeans in the field of defence and security, as war returns to the European continent. Based on this common interpretation of security environment, the Compass establishes the major strategic guidelines and new European initiatives to be implemented in order to enable Europeans to defend their interests and their freedom of action wherever necessary: in seas and oceans, airspace, outer space, cyber space, and the information space. (EEAS, 2024).

The Compass covers all aspects of the Common Security and Defence Policy (CDSP), and is based on four pillars:

- ✓ *Act* (Strengthening the EU's capacity for action in an increasingly brutal and unpredictable world.)
- ✓ *Secure* (Strengthening the ability to protect common strategic spaces and defend the values, rules and principles that the EU upholds.)
- ✓ *Invest* (Involves enhancing technological sovereignty by improving defence capabilities.)
- ✓ *Partner* (Strengthen the EU's position as an international partner.) (EEAS, 2024).

Main elements of the Joint Framework

The Joint Framework offers a comprehensive approach to improve the common response to the challenges posed by hybrid threats to Member States, citizens and the collective security of Europe. It brings together all relevant actors, policies and instruments to both counter and mitigate the impact of hybrid threats in a more coordinated manner. In particular, it builds on the European Agenda on Security adopted by the Commission in April 2015, as well as on sectorial strategies such as EU Cyber Security Strategy, the Energy Security Strategy and the European Union Maritime Security Strategy. Together with the upcoming European Union Global Strategy for foreign and security policy and the Defence Action Plan, and ongoing work on capacity building in support of security and development (CBSD) in third countries, the Joint Framework is part of the strategy of the Commission and the High Representative to increase the EU's capacity as a security provider.

The EU counter-hybrid threats policy is based on four lines of action: situational awareness; resilience, response and cooperation (Figure 1).

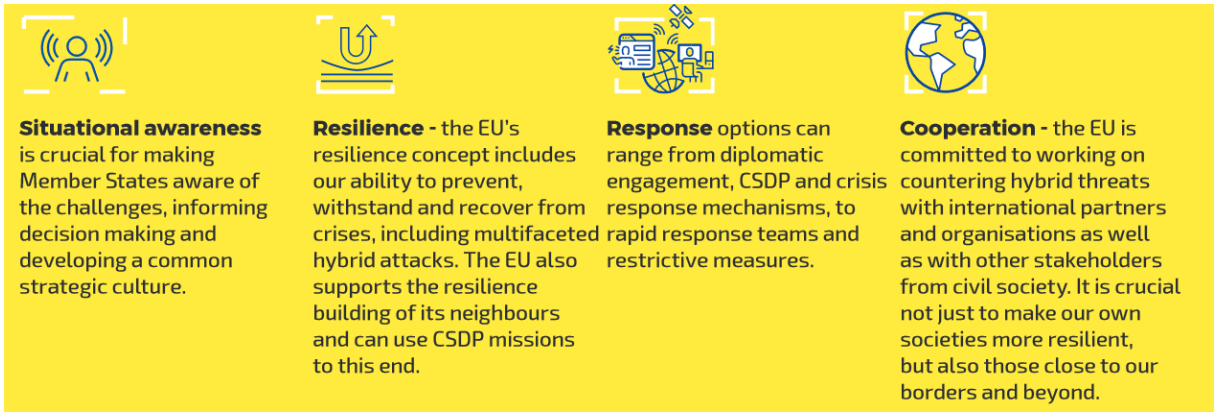

Figure 1. EU counter-hybrid threats policy – actions
Source: Countering Hybrid Threats (2022), (https://www.eeas.europa.eu/sites/default/files/documents/2022-03-28-countering-Hybrid-Threats_NewLayout.pdf)

Conclusions

Hybrid threats is a complex phenomenon and therefore the action to combat is difficult. Without a holistic approach that must cover all essential aspects of hybrid threats, it is difficult for actionable structures and dedicated capabilities to ensure a tailored response.

Therefore, in order to counter hybrid threats in a changing security environment in Europe, it is essential that policymakers, security experts and stakeholders strengthen cooperation, information sharing and coordination at national, regional and international level. The European Union plays a key role in developing policies, concepts and capabilities to counter hybrid threats, with a focus on resilience, deterrence and response mechanisms.

In addition, building the resilience of critical infrastructures, strengthening cybersecurity tools, strengthening strategic communication and public diplomacy, and investing in defence capabilities are key components of the EU's approach to countering hybrid threats. By adapting to a dynamic security environment and leveraging innovative technologies and strategies, Europe can effectively mitigate the impact of hybrid threats and ensure its security and stability in the face of changing challenges.

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. Countering hybrid threats: Council calls for enhanced common action, 2019. European Council. [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/ (2024).
2. European Commission 2016, *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response.* JOIN/2016/018 final. Document 52016JC0018, p. 2. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (2023).

3. European Commission 2016, *Defence Action Plan.* [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4088 (2023).
4. European Commission 2019, *A Europe that protects: good progress on tackling hybrid threats.* [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2788 (2023).
5. European Commission 2020, *European Agenda on Security*. [Online]. Available at: https://home-affairs.ec.europa.eu/european-agenda-security-legislative-documents_en (2023).
6. European Commission 2020, *EU Cyber Security Strategy*. [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (2023).
7. European Commission 2022, *Energy Security Strategy.* [Online]. Available at: https://energy.ec.europa.eu/topics/energy-strategy_en (2023).
8. European Commission 2023, *European Union Maritime Security Strategy*. [Online]. Available at: https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/maritime-security-strategy_en (2023).
9. 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, pp. 1, 6, 15-16, 27. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from =EN. (2023).
10. European Commission 2018, *Joint Communication to the European Parliament, the European Council and the Council Increasing resilience and bolstering capabilities to address hybrid threats.* JOIN/2018/016 final. Document 52018JC0016. [Online]. Available at: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016 . (2023).
11. European External Action Service 2019, *European Union Global Strategy for foreign and security policy*. [Online]. Available at: https://www.eeas.europa.eu/eeas/global-strategy-european-unions-foreign-and-security-policy_en (2023).
12. European External Action Service 2022, *EU counter-hybrid threats policy – actions.* [Online]. Available at: *https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en (*2023).
13. European External Action Service 2023, *EU Peace, Security and Defence. Working for a safe Europe and a stable world.* [Online]. Available at: https://www.eeas.europa.eu/eeas/eu-peace-security-and-defence_en (2023).
14. European External Action Service 2022, *A Strategic Compass for Security and Defence.* [Online]. Available at: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en (2023).
15. European Parliament 2021, *Best Practices in the whole-of-society approach in countering hybrid threats.* [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf (2023).
16. European Centre of Excellence for Countering Hybrid Threats, 2023. Hybrid threats as a Concept. [Online]. Available at: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (2023).
17. European Council, 2023. EU's Strategic Compass for Security and Defence: Articles and reports. [Online]. Available at: https://consilium-europa.libguides.com/strategic-compass/articles (2023).

18. *FAQ: Joint Framework on countering hybrid threats*, 2016. Available from: https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250 [31 August 2023].
19. Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue *Addressing Hybrid Threats*, 2018. [Online]. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf (2023).
20. Joint Staff Working Document, *Sixth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats 16.9.2022 SWD(2022) 308 final.* [Online]. Available at: https://defence-industry-space.ec.europa.eu/system/files/2023-07/SWD_2022_308_6_EN_document_travail_service_conjoint_part1_v5.pdf *(2023).*
21. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019. [Online]. Available at: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf (2023).
22. Lisboa Laura, *How to protect the EU against hybrid threats (2023).* [Online]. Available at: *https://youngthinkers.ceps.eu/how-to-protect-the-eu-against-hybrid-threats/* (2023).
23. Luigi Lonardo (2021), *EU Law Against Hybrid Threats: A First Assessment.* [Online]. Available at: *https://www.europeanpapers.eu/en/system/files/pdf_version/EP_eJ_2021_2_19_Articles_SS2_6_Luigi_Lonardo_00514.pdf* (2023).
24. Paulauskytė, Laima. *Macro-level Factors Influencing Conspiracy Theory Acceptance in the Baltic and Central European States during 2020–2022.* Master's Final Degree Project. [Online]. Available at: Macro-level factors influencing conspiracy theory acceptance in the Baltic and Central European states during 2020–2022 / (2023).
25. Sanz-Caballero Susana, *The concepts and laws applicable to hybrid threats, with a special focus on Europe. Humanities and Social Sciences Communications volume 10, Article number: 360* (2023). [Online]. Available at: https://www.nature.com/articles/s41599-023-01864-y (2023).
26. Seniutienė, Danguolė. Migration as a Challenge for Contemporary Public Security: Lithuanian case. Research Journal Public Security and Public Order. No. 35,2024. [Online]. Available at: https://ojs.mruni.eu/ojs/vsvt/article/view/8145 (2024).
27. Wigell, Mikael, Mikkola, Harri, Juntunen, Tapio. *Best Practices in the whole-of-society approach in countering hybrid threats* (2021). Online]. Available at: https://www.researchgate.net/profile/Mikael-Wigell/publication/351836523_Best_Practices_in_the_whole-of-society_approach_in_countering_hybrid_threats/links/6357970f6e0d367d91c4d9b8/Best-Practices-in-the-whole-of-society-approach-in-countering-hybrid-threats.pdf (2021).