UDC: 338.2:327
DOI: https://www.doi.org/10.33111/iep.eng.2024.41.12

# European Experience in Countering Hybrid Threats for Ukraine's Economic Recovery

OKSANA KARPENKO[1]

ANNOTATION. The article summarizes the experience of the EU countries in countering hybrid threats, outlines the directions of its possible and appropriate use in the process of Ukraine's economic revival, characterizes the categorical apparatus of the study: the concepts of hybrid threats, actors, actions are defined. The author identifies effective mechanisms for countering hybrid threats in the EU, which include institutional initiatives, sanctions policy, as well as specific ad hoc measures on information, energy and cybersecurity, in particular the activities of the European Center of Excellence for Countering Hybrid Threats, reducing the resource dependence of countries through diversification of supplies, the establishment of the European Cyber Security Agency, and campaigns to counter disinformation. Particular attention is paid to the methods and tools for implementing the EU Conceptual Model of Hybrid Threats (2021), which has a wide range of domains: infrastructure; cyberspace; space, economic, military and defense, culture, social, public administration and legal; intelligence, diplomacy, political and information spheres, and thus aims to raise awareness, establish mutual understanding between the parties, and identify the main aspects that enable an adequate understanding of the hybrid threat landscape. It is shown that hybrid threats involve the use of different approaches to avoiding them and developing resilience to them, which led to the emergence of the Model of an Integrated Resilience Ecosystem (2023). The article reveals its essence, specifies the areas of application, structure by domains (areas of activity), spaces (public, governance and services), and levels (local, national, international) that form the ecosystem. Current vulnerabilities, hostile actors and risks to national security are identified and the possibilities of eliminating their negative impact on a wide range of activities in the context of hybrid threats are substantiated based on the study of European experience. The results of the implementation of the project "Academic Counteraction to Hybrid Threats" (WARN) within the framework of the EU Erasmus+ Program in the field of "Capacity Building of Higher Education" (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP) to ensure the improvement of national security and overcome the lack of security services that has arisen due to the emergence of hybrid threats are investigated.

KEYWORDS: hybrid threats, European experience, higher education institutions, academic counteraction to hybrid threats, algorithm of managerial decision-making, security, counteraction, economic revival of Ukraine.

[1] **Oksana Karpenko** – Doctor of Economics, Professor, First Vice-Rector of International Scientific and Technical University named after Academician Yuriy Bugay (Kyiv, Ukraine). Scientific interests: trends in the development of modern management, public administration reform, organizational and economic mechanisms for improving the efficiency of enterprises, theory and practice of knowledge transfer at the national and international levels, academic counteraction to hybrid threats. E-mail: o.karpenko@istu.edu.ua ORCID: https://orcid.org/0000-0003-2943-1982

The article is based on the materials of the WARN project "Academic Countering Hybrid Threats" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP), co-funded by the Erasmus+ program of the European Union. The European Commission's support for the production of the materials contained in Section 4 does not constitute an endorsement of the content, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

IEP, No. 41 (2024) pp. 173–182

ISSN 1811-9832/2024/No. 2 (41)

## Introduction

Ensuring the resilience of the state and society to threats of various kinds and developing responses to numerous challenges caused by the impact of hybrid threats are at the heart of the global security environment.

Today's Ukraine faces numerous challenges, including hybrid threats that include military, economic, information and cyber elements. These threats are aimed at undermining economic stability, destroying trust in state institutions, and blocking the country's recovery.

In the context of European integration and close cooperation with the European Union, using their experience in countering hybrid threats is important to ensure Ukraine's economic revival.

The purpose of the article is to study the European experience of countering hybrid threats. In order to achieve this goal, the paper uses an integrated approach based on general scientific, general economic and applied aspects of the impact of hybrid threats on national security.

## Hybrid threats, actors, actions

In the modern world, hybrid threats have become a serious challenge for many countries, including Ukraine. The concept of "hybrid threats" refers to actions carried out by state or non-state actors that aim to undermine or harm a target group by influencing its decision-making at the local, regional, national or institutional level. Such actions are coordinated and synchronized and deliberately target the vulnerabilities of democratic states and institutions. Actions may take place, for example, in the political, economic, military, civilian or information spheres. They are carried out using a wide range of means and are designed to remain below the threshold of detection and attribution.[2]

Hybrid threats are aimed at destabilizing democratic states through **economic pressure** (sanctions, manipulation of energy resources, undermining supply chains), **cyber threats** (attacks on critical infrastructure, financial system, state registries), **information campaigns** (disinformation aimed at creating panic and distrust in the state), **political influence** (support for corrupt practices, interference in domestic politics).

Hybrid players try not to convince, not to fight, but to influence the algorithm of management decision-making.[3]

Hybrid actions are characterized by ambiguity created by combining traditional and non-traditional means – disinformation and interference in political debates or elections, disruption of critical infrastructure, cyber-

[2] Hybrid threats as a concept. Hybrid CoE. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

[3] Methodology of training in the context of hybrid threats: a manual / E. Balashov, M. Bilokon, T. Borozentseva, M. Holovyanko, S. Hryshko, T. Zhovtenko et al. Kharkiv: LLC "TECHNOLOGY CENTER GROUP", 2023. 84 p. https://sciencebookgroup.org/catalog/book/338 [In Ukrainian]

attacks, various forms of criminal activity, and, finally, asymmetric use of military means and warfare.

## Mechanisms for Countering Hybrid Threats in the EU

The above-mentioned actualizes the need to strengthen counteraction to hybrid threats, and in this regard, along with the adoption of important policy documents, the European Union has created and is currently operating a number of organizations whose purpose is to conduct research on the genesis and transformation of hybrid threats, develop methods, tools and mechanisms to counter these threats, organize joint training and consultations for member states, etc.

*Table 1*

**EFFECTIVE MECHANISMS FOR COUNTERING HYBRID THREATS IN THE EU COUNTRIES**

| Mechanisms | Characteristics |
|---|---|
| Institutional | The legal framework for the EU's protection against hybrid threats has been formed: "Joint Framework for Countering Hybrid Threats – European Union Response" (2016), "Building Resilience and Strengthening Capabilities to Counter Hybrid Threats" (2018), "Report on the Implementation of the 2016 Joint Program on Countering Hybrid Threats and the 2018 Joint Communication on Building Resilience and Strengthening Capabilities to Counter Hybrid Threats" (2020), "Mapping of Measures Related to Building Resilience and Countering Hybrid Threats" (2020), "EU Operational Protocol for Countering Hybrid Threats (EU Playbook)" (2016), EU Security Strategy 2020, on which the European Council adopted a non-legislative resolution. The EU has the European Center of Excellence for Countering Hybrid Threats (Hybrid CoE), which combines the efforts of member states to combat hybrid attacks. Its tasks include analytics, training and experience exchange. |
| Energy security | Reducing dependence on Russian energy resources by diversifying suppliers. For example, Poland and Lithuania have established LNG terminals, which has allowed them to reduce their dependence on Russian gas. Creation of the EU Energy Union, which ensures the integration of energy systems of member states. |
| Cybersecurity | The introduction of the NIS 2 Directive on the security of networks and information systems, which strengthens the requirements for the protection of critical infrastructure. Establishment of the European Cyber Security Agency (ENISA) to coordinate efforts to combat cyber threats. |
| Information security | Campaigns to counter disinformation, such as the East StratCom Task Force initiative aimed at exposing Russian propaganda. Strengthening independent media and media literacy among the population. |
| Sanctions | The EU is actively applying economic sanctions against the aggressors, including asset freezes and trade restrictions. |

*Source*: compiled with the use of data[4]

[4] Khmel A. 2022. Combating Hybrid Threats in the EU (based on the regulatory framework of the European Union). Acta de Historia & Politica: Saeculum XXI. 2021/2022. Vol. 3. P. 91–101.

The functioning of the above organizations and the implementation of the adopted documents will help prevent and detect hybrid threats, in particular, strengthen the fight against terrorism and organized crime, increase the resilience of critical infrastructure to cyberattacks, promote research and innovation, develop the education system, etc.

## Conceptual model of hybrid threats

One of the EU's responses to the numerous challenges posed by hybrid threats is the development of the Hybrid Threats conceptual model[5] by the Joint Research Center of the European Commission (JRC[6]) and the European Center of Excellence for Countering Hybrid Threats (Hybrid CoE).[7]

The European Commission's Joint Research Centre (JRC) provides independent, evidence-based knowledge to support EU policies in order to have a positive impact on society.

The activities of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) are aimed at: conducting research, analyzing hybrid threats and methods of combating them; organizing joint training for member states; conducting consultations at the strategic level between EU and NATO members, engaging governmental and non-governmental experts in dialogue.

The main objectives of the Conceptual Model of Hybrid Threats[8] are to raise awareness, build understanding with stakeholders, and identify key issues and gaps for future research.

The "Conceptual Model of Hybrid Threats"[9] identifies four main pillars that need to be studied in order to fully understand the hybrid threat landscape:

- hostile actors (and their strategic goals);
- tools used by the enemy actor;
- target domains (areas);
- phases (including the types of activities observed in each phase).

Thus, a hostile actor (state or non-state) with goals but limited capabilities to achieve them can apply a variety of tools to a number of

---

[5] Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Th eocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. https://publications.jrc.ec.europa.eu/repository/handle/JRC123305.

[6] Joint Research Center. https://commission.europa.eu/about-european-commission/departments-and-executive-agencies-old/joint-research-centre_en.

[7] The European Center of Excellence for Countering Hybrid Threats (Hybrid CoE). https://www.hybridcoe.fi/about-us/.

[8] Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. https://publications.jrc.ec.europa.eu/repository/handle/JRC123305.

[9] Ibid.

domains to perform a certain type of activity in different phases to achieve a number of objectives and undermine the decision-making capacity of the state that is the target of hybrid threats (the target state).

Hostile actors who engage in hybrid threat-related activities will try to influence the target's decision-making algorithm. Decision-making can be small (business transactions), local (people during elections), and decisions made by policy and legislative professionals. If the operation is successful, it will contain only some aspects that make the threat hybrid in nature. This means that the action can cause harm on its own and needs to be identified and countered at an early stage. For this reason, it is important to study the actors behind a hybrid threat.

The "Conceptual Model of Hybrid Threats"[10] identifies the following domains: infrastructure; cyber; space; economic; military and defense; culture; social/social; public administration; legal; intelligence; diplomacy; political; information. Domains should not be studied separately, as the impact on one domain can cause a cascading effect in others. This is especially important when considering the impact of a hybrid threat on a domain. In each domain, there may be a variety of tools that a hostile actor can use to target specific domains to achieve its goals.

Hybrid threats is an overarching concept that includes a wide range of activities in the hybrid threat landscape: interference, influence, campaigns, and war.

The different types of hybrid threat activities in the "Conceptual Model of Hybrid Threats"[11] are placed on a timeline, indicating that there is a potential for hybrid threat escalation that encompasses both short-term and long-term capabilities. The timeline has three distinct phases, namely preparation, destabilization, and coercion. All phases have a strong psychological component. The range of actions, including interventions, influence, campaigns, and war, coincide at different stages.

Hybrid warfare involves the synchronized use of many instruments of influence, selected with regard to specific vulnerabilities across the entire spectrum of social functions to achieve synergistic effects.

## A model of an integrated resilience ecosystem

Today, we are witnessing rapid developments and increasing sophistication of hybrid threats. Therefore, resilience to hybrid threats needs to be developed and implemented at all levels, and resilience indicators

[10] Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. https://publications.jrc.ec.europa.eu/repository/handle/JRC123305..

[11] Ibid.

should be considered not only in terms of different areas, but also as a comprehensive ecosystem approach. In other words, the development of resilience to hybrid threats requires going beyond resilience in individual areas, building it systematically, taking into account the dependencies and interdependencies between different parts of society – "The comprehensive resilience ecosystem (CORE) model"[12], which should facilitate the process of making informed management decisions at different levels of government.

"The Comprehensive Resilience Ecosystem Model is a systematic representation of a democratic society as a whole. It is used to analyze and ultimately counter hybrid threats that seek to undermine and damage the integrity and functioning of democracies, alter decision-making processes and create cascading effects.[13]

The novelty of this model is that it allows policymakers to assess how adversaries use hybrid threats to alter democratic decision-making. It shows how hybrid threats challenge democratic systems step by step, creating different types of stress. It also allows us to track dependencies and possible cascading effects. This is important for identifying hybrid threats. Foresight plays a crucial role in this process.

The ecosystem is based on the seven pillars of democratic systems: a sense of justice and equal treatment, civil rights and freedoms, political responsibility and accountability, rule of law, stability, reliability/accessibility, and foresight. These seven pillars are the foundation of a sustainable, democratic society and are essential for building resilience to hybrid threats. They are the ultimate targets of attacks by hostile actors to satisfy their own strategic interests.

The domains (spheres) from the Conceptual Model of Hybrid Threats[14] are also an integral part of the ecosystem: infrastructure, cyber, space, economic, military/defense, cultural, social/societal, public administration, legal, intelligence, diplomatic, political, and information spheres. If domains are well developed in terms of resilience, they can act as shields against malicious actions. On the other hand, a lack of resilience in domains can open entry points for hostile actors.

The ecosystem consists of three spaces – Civic Space, Governance Space, and Service Space – representing three sectors of society.

---

[12] Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023, doi: https://doi.org/10.2760/113791, JRC129019. https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf.

[13] Ibid.

[14] Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305.

The three levels of the ecosystem represent the different "layers" that exist in the organization of society – local, national, international.

Because the elements are interconnected, resilience-building measures for one element will affect the other elements, either positively or negatively. The hostile actors behind hybrid threats seek to exploit the different elements and their interconnections to maximize their impact. Therefore, policymakers need to understand the interdependence between the various elements in order to build resilience to hybrid threats and detect malicious activity at an early stage.

This ecosystem approach helps to identify early warning signs, support their analysis, and identify potential response trajectories. The "Integrated Resilience Ecosystem Model"[15] can be used as a "dart board" to map how actors use specific tools to attack different areas and create cascading effects in different spaces and at different levels. It helps to analyze and understand the impact, development/stages, as well as how intensively, which areas and levels are affected by hybrid threats and how much they depend on each other. In essence, it helps decision makers to choose which resources, tools and measures to mobilize at the EU, Member State and operational levels.

Resilience is the key to countering hybrid threats and should be developed systematically. Building resilience in separate areas is not optimal, as hybrid threats aim to create cascading effects and exploit interconnections. A systemic approach is needed, taking into account the existing dependencies and interdependencies in society.

## Project "Academic Counteraction to Hybrid Threats"

One of the responses to the challenges posed by the impact of hybrid threats was the implementation of the project "Academic Counteraction to Hybrid Threats" (WARN) within the framework of the EU Erasmus+ Program in the field of "Capacity Building in Higher Education" (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)[16], which is to be completed on November 14, 2024. The mission of the project is to improve national security and overcome the lack of security services that has arisen due to the emergence of hybrid threats. Target groups: students, universities, teachers, companies and organizations, society in general.

Seven Ukrainian universities worked on the project, namely: Kharkiv National University of Radio Electronics, Ukrainian Catholic University, State

[15] Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023, https://doi.org/10.2760/113791, JRC129019. URL: https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf.

[16] WARN Project Website. URL: http://warn-erasmus.eu.

University of Infrastructure and Technology, National University of Ostroh Academy, National Academy of Culture and Arts Management, V. N. Karazin Kharkiv National University, Horlivka Institute of Foreign Languages of Donbas State Pedagogical University. European partners in the consortium included: University of Jyvдskylд (Finland) – project coordinator, Йcole Supйrieure de l'Enseignement de France; University of Coimbra (Portugal); University of Tartu (Estonia).

Based on the results of the project implementation:[17]

— 7 centers of excellence (based on updated laboratories) were created and equipped.

— 11 existing master's programs of the project consortium were adapted and 1 new program was created and accredited.

— 24 syllabi of the newly developed disciplines were prepared.

— The curricula of 18 courses on countering hybrid threats for the lifelong learning cycle in 11 project domains were created and published.

— Seven training courses were developed to improve the skills of university teachers in all fields based on a new methodology for teaching countering hybrid threats.

— Educational and methodological materials for 12 new disciplines and 39 updated disciplines on countering hybrid threats were prepared and published on the websites of higher education institutions.

— 51 new sets of training materials for practical classes were developed and published on university websites.

— One electronic manual on the new methodology of hybrid training "New methodology of training to counter hybrid threats" was developed (common for all partners). [18]

— A "Glossary of Hybrid Threats" was created and published.[19]

— 2432 students were enrolled and trained in master's project programs on countering hybrid threats.

— 1504 teachers from universities outside the consortium were trained on the new teaching methodology for teaching countering hybrid threats and received certificates confirming their skills.

— 4,594 students from professional sectors took advanced training courses under project-based lifelong learning programs to acquire skills to counter hybrid threats in their own fields.

— 17 new partners joined the WARN community.

---

[17] Golovianko Mariia. Application of European Resilience Experience Against Hybrid Threats in the Erasmus+ Project WARN. URL: https://warn-erasmus.eu/wp-content/uploads/2024/11/warn_application_eu-resilience_experience_against_hybrid_threats.pdf.

[18] Methodology of training in the context of hybrid threats: a manual. E. Balashov, M. Bilokon, T. Borozentseva, M. Holovyanko, S. Hryshko, T. Zhovtenko et al. Kharkiv: LLC "TECHNOLOGY CENTER GROUP", 2023. 84 p. https://sciencebookgroup.org/catalog/book/338 (in Ukrainian)

[19] Glossary of hybrid threats. Erasmus+ project WARN "Academic Response to Hybrid Threats". 2024. 203 p. https://openarchive.nure.ua/handle/document/29379

— The project has established a separate conference dedicated to research on countering hybrid threats in various fields, "Management and Administration in the Context of Countering Hybrid Threats to National Security."

Higher education institutions of Ukraine, through the introduction of relevant academic disciplines and the organization of advanced training courses, can create effective means to explain the nature of, inform about, and prevent hybrid threats, as well as minimize the negative effects of hybrid threats.

## Conclusions

Countering hybrid threats is becoming a priority, as they blur the clear line between war and peace by combining military capabilities with political, diplomatic, economic, cybersecurity and disinformation measures.

To make informed management decisions at different levels in the face of hybrid threats, a resilience-based approach should be implemented. The peculiarity of making such decisions is that they need to be made in conditions of environmental turbulence: uncertainty, ambiguity, and time constraints.

Taking into account the European experience, Ukraine should integrate into European cyber and energy security initiatives, use EU technical and financial support to modernize its infrastructure, improve its strategy for countering hybrid threats based on European practices, and focus on combating disinformation by increasing the level of media literacy.

European experience in countering hybrid threats is an important resource for Ukraine's economic revival. A comprehensive approach, integration into relevant European initiatives, and adaptation of best practices will not only protect the Ukrainian economy, but also lay the foundation for its development in the face of current security challenges.

** This article was translated from its original in Ukrainian*

## References

1. Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rócz, A., Schmid, J. and Schroefl, J. 2021. "The landscape of Hybrid Threats: A Conceptual Model (Public Version)". Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305.

2. EU Commission. 2024. Joint Research Center. https://commission.europa.eu/about-european-commission/departments-and-executive-agencies-old/joint-research-centre_en.

3. Glossary of hybrid threats / Erasmus+ project WARN "Academic Response to Hybrid Threats". 2024. 203 c. https://openarchive.nure.ua/handle/document/29379

4. Golovianko, M. 2024. "Application of European Resilience Experience Against Hybrid Threats in the Erasmus+ Project WARN." https://warn-erasmus.eu/wp-content/uploads/2024/11/warn_application_eu-resilience_experience_against_hybrid_threats.pdf.

5. Hybrid CoE. 2024. "Hybrid threats as a concept." https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

6. Hybrid CoE. 2024. "The European Center of Excellence for Countering Hybrid Threats." URL: https://www.hybridcoe.fi/about-us/.

7. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G. 2023. "Hybrid threats: a comprehensive resilience ecosystem – Executive summary", Publications Office of the European Union, Luxembourg, 2023, JRC129019. DOI: https://doi.org/10.2760/113791. https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf.

8. Khmel A. 2022. "Combating Hybrid Threats in the EU (based on the regulatory framework of the European Union)." *Acta de Historia & Politica: Saeculum XXI*. 2021/2022. VOL. III. P. 91–101.

9. *Methodology of training in the context of hybrid threats: a manual*. E. Balashov, M. Bilokon, T. Borozentseva, M. Holovyanko, S. Hryshko, T. Zhovtenko et al. Kharkiv: LLC "TECHNOLOGY CENTER GROUP", 2023. 84 p. https://sciencebookgroup.org/catalog/book/338 (in Ukrainian)

10. WARN Project Website. http://warn-erasmus.eu.

Received: October 20, 2024
Accepted: November 18, 2024
Released: December 31, 2024