Terrorism – Studies, Analyses, Prevention, 2025, special edition: 133–158

https://doi.org/10.4467/27204383TER.25.017.21520

Article

Hybrid threats to critical infrastructure in the European Union. Selected Hybrid CoE analyses

ALEKSANDER OLECH https://orcid.org/0000-0002-3793-5913

Defence24

Abstract

The author of the article describes the progression of hybrid threats, particularly in Central and Eastern Europe, with a focus on Russian influence operations. By examining 6 key publications from the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), the author identifies hybrid tactics, from disinformation and cyberattacks to maritime and kinetic threats. The research explores strategic competition, resilience-building, and legal frameworks necessary to counter challenges of these tactics. The findings highlight the need for continuous adaptation to emerging challenges, increased international cooperation, and proactive measures to mitigate the impact of hybrid operations on Western states. Understanding the evolution of these threats is important for strengthening national security, improving resilience, and developing effective counterstrategies.

Keywords

Russia, critical infrastructure, hybrid threats, terrorism, Finland, Baltic Sea

Introduction

Hybrid threats and their evolution are becoming increasingly significant for global security. These are no longer just negative actions that can be easily categorised as competition in Europe between European Union and NATO Member States and the Russian Federation (RF). Today, hybrid threats are evident on a global scale, with the Kremlin's imperial policies amplifying their scope and refining the tools used to exert influence, alongside the malicious activities of other actors, such as North Korea and Iran.

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) defines hybrid threats as actions conducted by state or non-state actors that aim to undermine or harm a target by combining overt and covert military and non-military means. These activities use detection thresholds and attribution, as well as the boundary between war and peace, to influence decision-making processes at different levels – local, regional, state or institutional – in order to achieve the strategic objectives of the attacking entity and simultaneously harm the attacked entity.

The objective of hybrid action is to affect diverse decision-making processes at the regional, national, or institutional levels to promote and/or attain strategic goals while concurrently undermining the target, predominantly Western nations in contemporary contexts.

Apparently benign actions may be a part of a hybrid operation, thata ccording to the perpetrator's plan, should remain hidden or reduce the victim's ability to associate the act to its initiator. This complicates any response, as such operations – evident in the case of countries along NATO's and the EU's eastern border – occur below the threshold of war or involve actors that are challenging to verify. Despite certain attacks being ascribed to Russia, Iran, or China, the reactions from Western states remain constrained.

Some of state and non-state actors are keen to exploit gaps in international law to complicate the collective defence of Western nations against hybrid threats. This constitutes their paramount advantage. A significant obstacle for nations adhering to international law is the protracted process of consultation and decision-making on the appropriate response, which requires the involvement of actors such as the UN, EU, NATO. During this period, the antagonist can carry out hybrid activities. This is also apparent in the creation of tools to minimise threats, as for law-abiding nations, this process is significantly prolonged.

All Central and Eastern European countries are exposed to hybrid threats, which can take any form of attack as long as they remain below the threshold of war. However, the line defining when a conflict actually begins or when an attacked state (or entity) can respond remains blurry.

Since 2014, the frequency of hybrid attacks executed by the RF has been consistently progressing. These assaults are perpetrated by military personnel, intelligence agencies, journalists, and politicians, alongside individuals who are either oblivious to their support of Russian influence or are recruited agents who opt to act in Russia's interest for financial, professional, or political gain, or due to personal convictions. As a result, hybrid threats can be observed not only in the sphere of war, the perspective of compliance with international law, but also in cybersecurity, information (disinformation), politics, economics, culture, religion, and society. Additionally, such threats include kinetic actions, such as maritime and aerial incidents (e.g. airspace violations). Russia seeks every means to negatively impact its chosen adversaries.

This analysis is based on 6 scientific publications from the Hybrid CoE:

1. *The Landscape of Hybrid Threats: A Conceptual Model*[1] – presents the evolution of hybrid threats, the activities of Russia, China, and non-state actors, as well as the areas in which hybrid attacks are carried out.
2. *The concept of hybrid war in Russia: A national security threat and means of strategic coercion*[2] – primarily focuses on threats to Russia itself, which in turn serves as a justification for developing strategies to protect its own interests and to create strategic competition with Western states in specific areas.

[1] G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, Publications Office of the European Union, Luxembourg 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf [accessed: 2.01.2025].

[2] K. Pynnöniemi, *The concept of hybrid war in Russia: A national security threat and means of strategic coercion*, Hybrid CoE Strategic Analysis / 27, May 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/05/20210518_Hybrid_CoE_Strategic_Analysis_27_The_concept_of_hybrid_war_in_Russia_WEB.pdf [accessed: 10.01.2025].

3. *Handbook on maritime hybrid threats: 15 scenarios and legal scans*[3] – scrutinises a diverse array of hybrid threats, especially those pertinent to activities in the maritime sphere. This is particularly significant regarding current challenges in the Baltic Sea region.
4. *A comprehensive resilience ecosystem*[4] – it takes into account increasing complexity of attacks, including hybrid threats, the ability to recover and rebuild infrastructure; it is crucial for understanding resilience – a pillar of national and multinational security.
5. *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*[5] – provides a model example of how the RF instrumentalises hybrid attacks as a tool of destabilisation in its near abroad. This is a particularly valuable publication for countermeasures undertaken by governments and international organisations.
6. *Protecting maritime infrastructure from hybrid threats: legal options*[6] – examines hybrid threats to maritime infrastructure, highlighting legal gaps and security challenges. It calls for stronger international cooperation and legal reforms to protect critical undersea assets.

The discussed research is important for understanding the concept of hybrid operations carried out against the broadly defined Western states. The analysis demonstrates how the form and scope of hybrid threats have evolved over the years, as well as the main challenges NATO and EU countries face in responding to them. Particular attention has been given to actions conducted by the RF.

[3] *Hybrid CoE Paper 16: Handbook on maritime hybrid threats: 15 scenarios and legal scans,* March 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/03/NEW_web_Hybrid_CoE_Paper-16_rgb.pdf [accessed: 17.01.2025].

[4] R. Jungwirth et al., *Hybrid threats: a comprehensive resilience ecosystem*, Publications Office of the European Union, Luxembourg 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf [accessed: 22.01.2025].

[5] H. Praks, *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage,* May 2024, https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf [accessed: 30.01.2025].

[6] A. Sari, *Hybrid CoE Research Report 14: Protecting maritime infrastructure from hybrid threats: legal options,* March 2025, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf [accessed: 6.03.2025].

The author has extracted essential components from each reviewed publication to delineate a roadmap of the analysed hybrid threats, emphasising their evolution in recent years. Simultaneously, he indicated that some of them will emerge in various forms and locales in the future, while present actions by adversaries (e.g. damage to critical infrastructure, CI) lay the foundation for subsequent assaults.

An empirical analysis and review of the studies presented are crucial for advancing research on hybrid threats. However, further studies are being carried out analysing emerging security threats from different perspectives. Consequently, it is pertinent to persist in dialogues regarding hybrid threats to elucidate the phenomenon, enhance public awareness, foster resilience, and formulate best practices and responses for both effective reaction and prevention.

Comprehensive resilience ecosystem

Resilience is the capacity of a system – personal, community, or institutional – to withstand, bounce back, and change following disturbances. Academic study has changed over time from seeing resilience as something fixed to seeing it as a dynamic process, where adaptation and transformation are quite important[7]. Resilience is becoming a pillar of national security given the growing complexity of attacks, including hybrid threats, and the need of recovery and repair infrastructure.

Resilience is sometimes defined depending on cultural viewpoints, which influence the development and execution of policies. In Russia, for instance, resilience is usually connected with endurance and stability. While resilience in many Arab countries is shaped by geopolitical events, in China the focus is on adaptation[8].

The European Union's priorities in the first decade of 21st century were crisis management and safeguarding of CI. The concept of resilience was only formally integrated into the process of EU policy-making in 2017 with the document: *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*. The European Commission first presented the *Joint Communication to the European*

[7] R. Jungwirth et al., *Hybrid threats: a comprehensive resilience ecosystem…*, p. 17.

[8] Ibid., p. 19.

Parliament and the Council. Joint Framework on Countering Hybrid Threats a European Union response document in 2016. The paper listed 22 actions meant to counter hybrid threats. Adopted by the European Council on 25 May 2022, the *Strategic Compass for Security and Defence* is currently the guiding concept of the EU's resilience strategy[9].

The COVID-19 pandemic influenced NATO's strategy. The Allies worked on preparing the healthcare sector. In 2020, NATO undertook a revision of the Seven Baseline Requirements (7BLR) for civil preparedness to take into account the impact of the pandemic. During the Brussels Summit, the Alliance decided to strengthen its resilience through (...) *work across the whole of government, with the private and non-governmental sectors, with programmes and centres of expertise on resilience established by Allies, and with our societies and populations, to strengthen the resilience of our nations and societies*[10].

Democratic systems, in addition to relying on trust in society, government, and state institutions, are built on 7 main pillars:

1) feeling of justice and equal treatment, including a belief in a fair and impartial system, protection of property and identity;
2) civil rights and liberties such as freedom of speech, the right to vote;
3) political responsibility and accountability, expressed through free and fair elections and open public debate;
4) rule of law, i.e. equality of all before the law and independence of the judiciary;
5) political, social, and economic stability;
6) reliability and availability, understood as a guaranteed access to basic goods and services;
7) foresight capabilities, i.e. the ability to identify threats and develop intensive public-private cooperation, implementation of innovations).

It is these elements that constitute the foundation of the resilience and durability of modern democracies[11].

The foundations of the Comprehensive Resilience Ecosystem (CORE) are 3 main domains: civic (society and culture), governance (administration,

[9] Ibid., p. 26.

[10] Ibid., p. 29.

[11] Ibid., p. 33.

political processes, diplomacy), and services (infrastructure, economy). CORE can promote cross-sectoral efforts involving the entire society by summarising key interconnections. It provides a methodology that enables a better understanding of interactions between systems, institutions, and social factors. It allows for the presentation of incidents and their consequences, as it serves as a mechanism for enhancing resilience against hybrid threats and fortifying democratic societies. CORE concentrates on hybrid threats that aim to exploit systemic vulnerabilities at local, national, or international scales. It can serve as an important signal for the evolution and expansion of resilience capabilities. Support from policymakers is necessary to introduce appropriate legislation and raise public awareness of the potential consequences of hybrid attacks.

In addition, continued development of technologies to detect, warn of, counter and mitigate hybrid threats to enhance resilience is essential[12].

The landscape of hybrid threats

States and regions perceive not only security but also the constantly evolving hybrid threats in different ways[13]. These threats, along with hybrid actions, are understood as a combination of regular and irregular actions (i.e. of varying intensity and frequency), both undertaken by armed forces as well as criminals, terrorists, or even political organisations[14]. Such new form of threat, or rather its diverse nature, indicates the need to verify the ability of states to respond to perils of this kind. This is primarily related to actions of governments, efficiency of defence systems, and international security cooperation in terms of security. In this case, it is crucial to view the current situation in Ukraine, the Balkans, Syria, Libya, or Central Africa through the prism of both military and non-military challenges.

Hybrid actions are primarily carried out by actors with authoritarian or totalitarian views on power. Their objective is to direct all possible

[12] Ibid., p. 78.

[13] G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model...*, p. 9.

[14] A. Olech, *Cooperation between NATO and the European Union against hybrid threats with a particular emphasis on terrorism,* Institute of New Europe, 17.03.2021, https://ine.org.pl/en/cooperation-between-nato-and-the-european-union-against-hybrid-threats-with-a-particular-emphasis-on-terrorism/ [accessed: 10.02.2025].

(authoritarian) tools against democratic systems[15]. As a result, governments of this nature often last for decades and become more entrenched over time. Importantly, one authoritarian leader is replaced by another.

State actors engaging in hybrid activities are mainly authoritarian or totalitarian states. Their internal strategy for maintaining power is considered identical to the strategy of hybrid warfare, in the context of which democratic states are perceived as an existential threat to these regimes. Therefore, these regimes attempt to undermine and weaken the capabilities of democratic states. Here, information plays a very important role – it is a tool that enables the manipulation of social beliefs and discourages collective action against the regime[16].

The development of media, including social media, has created new opportunities for disinformation and propaganda activities. Now anyone can be a broadcaster and publish from anywhere; new platforms have emerged that are beyond state control; there are new opportunities to distort content; media globalisation has accelerated; new business models have developed, and the economic structure has become data-driven[17]. Disinformation from authoritarian countries is far more frequent and powerful in terms of the scope of the information being spread. This is due to the fact that democratic countries have regulatory and verification processes in place[18]. It should be noted that debunking fake news is several times more difficult than publishing false information.

In the past, the promotion of democracy was considered a hybrid threat – for example, the activities of NGOs in non-democratic countries and their efforts to promote democracy. These actions are solely intended to push authoritarian states towards democracy. However, as these states become aware of this, they respond by introducing laws on foreign actors or banning the activities of NGOs and think tanks. Currently, a hybrid threat should be defined as a form of covert, coercive, or corrupt use of force (e.g. blackmail). Referring, for instance, to the activities of NGOs aimed

[15] G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model…*, p. 15.

[16] Ibid., p. 16.

[17] Ibid., p. 17.

[18] Ibid., p. 18.

at promoting democracy[19], it has also been suggested in the past that soft power and public diplomacy could be considered hybrid threats.

It should be noted that the costs of conducting irregular attacks described as hybrid actions are much lower than those of traditional war. Moreover, the attacker is not, at least not entirely, exposed to a strong reaction of international community. The hybrid conflict in Ukraine is part of an evolution that is taking place in post-Soviet countries (as is currently happening in Belarus, for example). It is a multidimensional crisis, comprising the actions of national and supranational entities pursuing their political and economic interests with the available range of methods: from the conventional use of armed forces to fake news distribution. Allowing the development of separatist enclaves, such as those in Moldova, Georgia, and Azerbaijan, is a serious problem and requires these countries to cooperate with NATO and EU Member States and create a common sphere of security.

Russia

In Russia, a strategy of self-regulation is in place. This means that, through ingrained Russian values, citizens – including businesses and other non-state actors – act without prior coordination with the authorities, implementing solutions aligned with the political concepts proposed by Moscow. This approach facilitates the decentralised execution of strategic goals, allowing for flexibility in actions. Russianness serves as a unifying element, binding all Russians together to safeguard Russia’s national strategic interests and the objectives set by the highest leadership – critical for mobilising society[20].

Reflexive control is a fundamental concept in Russian strategic theory, highlighting the role of psychological manipulation of adversaries. The objective is to establish circumstances in which adversaries make choices that coincide with Russia’s strategic aims while perceiving themselves as acting contrary to Moscow’s interests[21].

[19] Ibid.

[20] Ibid., p. 19.

[21] Ibid., pp. 19–20.

China

China bases its attempts to achieve great power status on Halford Mackinder's Heartland theory[22]. China seeks to achieve this by becoming a maritime power[23]. It relies on Sun Tzu and his concept of the art of effectively deceiving the enemy and, ideally, winning a war without the need to resort to weapons[24]. Three factors determine the strategic behaviour of Chinese military forces: strategic thinking, strategic environment, and military potential. This triad shapes comprehensive planning and strategy execution in response to hybrid threats[25].

Traditional Chinese strategy operates within a dialectical framework that recognises dynamic properties such as "weakness" and "strength". The concepts are fluid and adaptable, functioning both as abstractions and as actions in strategic practice[26]. The Chinese concept of the 3 wars includes psychological warfare (achieving goals by influencing the psyche, e.g. deterrence, coercion, deception), public opinion warfare (influencing domestic and international support by using selective information provided through various media, shaping a specific system of values in society), and legal warfare (actions taken in order to gain legal advantage by utilising or modifying national and international law to achieve political or military superiority)[27].

Non-state actors

A state operating through non-state entity is, for example, Iran, which uses Hezbollah. Another example is Russia and the Wagner Group. One can point to entities such as Islamic militias in Africa and the Middle East, as well as terrorist groups like the IRA (Irish Republican Army), ETA (Basque: Euskadi Ta Askatasuna), or the Tamil Tigers. Another group of non-state actors is beginning to develop, namely private military groups (private military companies, PMC), sometimes referred to as security companies.

[22] Heartland (or "pivot area"), according to Mackinder, it is the area of Eurasia – roughly today's Russia and Central Asia – a region less vulnerable to attacks from the sea, difficult to conquer, but crucial for dominance over the continent.

[23] G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model…*, p. 20.

[24] Ibid., p. 21.

[25] Ibid.

[26] Ibid.

[27] Ibid.

The Wagner Group is also among them. The role of PMCs in creating hybrid threats is growing[28].

Covert state actions by the aggressor have the advantage that they make it more difficult for target states to not only detect and prevent the possibility of harmful operations, but also to attribute responsibility for these operations to the foreign state, e.g. in the case of the annexation of Crimea, to Russia and the Night Wolves MC (Russian: Ночные Волки). The aggressor states can deny and reject accusations, achieve their goals secretly, e.g. gain access to critical sectors (e.g. Russian interference in the 2016 US presidential election)[29].

Criminal organisations operating in target countries are increasingly being used by aggressor countries. For example, they provide these countries with existing smuggling networks, supply forged documents, commit financial crimes, or simply threaten strategic countries, groups, or individuals[30].

Understanding hybrid threats as the existence of criminal or terrorist organisations is crucial. However, a small number of these entities have conducted operations against Western states to achieve their goals. So far, they have used violence or threatened to use it, but not on a scale that would clearly classify them as hybrid states[31].

Hybrid threat domains

There are 13 domains in which hybrid threats may occur: infrastructure, economy, intelligence, information, cyberspace, diplomacy, politics, culture, society, legal, military/defence, outer space and administration[32]. In the context of hybrid threats the most important are:

1. Cyberspace – as a new field for delivering threats in the form of cybercrime, propaganda, espionage, terrorism, and even war. Smaller actors have greater opportunities to operate in cyberspace than in the real world[33].

[28] Ibid., p. 23.

[29] Ibid., pp. 23–24.

[30] Ibid., p. 24.

[31] Ibid.

[32] Ibid., p. 26.

[33] Ibid., p. 28.

2. Outer space – hybrid actions in this space are increasingly concerning due to the fact that several countries are developing counter-space capabilities. As a result, this may affect other domains, e.g. the military, because the space sphere is its integral part[34].
3. Society – the social domain is usually used to generate, deepen, or exploit socio-cultural divisions that will cause social upheavals necessary to continue or succeed in hybrid threat activities[35].
4. Legal domain – refers to a set of legal regulations, actions, processes, and institutions. Authoritarian states may use counter-laws, create them to achieve their goal, or exploit gaps in existing law in democratic countries. For example, reliance on the right to freedom of speech creates space for disinformation campaigns[36].
5. Intelligence – a state usually uses its intelligence capabilities to support planned or ongoing hybrid threat activities or may attempt to influence the intelligence operations of the target state[37].
6. Diplomacy – hybrid actions, especially in this sphere, aim to create divisions at the national or international level, support information campaigns, and interfere in the decision-making process (diplomatic sanctions, using embassies)[38]. Diplomacy intersects with domestic politics, so state decision-makers must create two-level strategies. Diplomacy is also closely related to the economy, social sphere, and legal sphere. Actions in the sphere of diplomacy may negatively impact the economy of a state[39].
7. Information – if it is controlled, falsely disseminated or inspires certain actions, it can become an element of hybrid warfare and influence the adversary.

Since the annexation of the Crimea by Russia in 2014, many initiatives have been undertaken to strengthen the resistance of the EU and NATO to hybrid threats. These efforts must be recognised by the Member States, and the pace of activities and their intensity must be maintained. Due to

[34] Ibid.

[35] Ibid., p. 30.

[36] Ibid.

[37] Ibid., p. 31.

[38] Ibid.

[39] Ibid., p. 32.

the ever-changing nature of hybrid threats, continued vigilance is required. Strategic approach towards combating hybrid threats, which would involve not only international but also national structures, including entire societies, as they are the main victims of terrorism, is essential.

Due to the relatively broad scope of NATO and EU activities, a comprehensive and multi-level structure is currently being created that will enable a multi-phase response to security threats. The improvement of the previously existing response schemes, whether military, political, economic or social, allows for effective intervention and creates a geopolitical apparatus which today is of high necessity. The response is essential to adequately address the emerging challenges posed by hybrid threats.

Russian concept of hybrid war

In the ongoing debate in Russia a hybrid warfare is characterised as a blend of military and non-military actions aimed at achieving political goals[40]. It should be noted that the early implementation of information warfare allows political objectives to be met without the use of armed forces[41]. Later, it is only necessary to maintain authoritarian power. This is why, in 2014, military and non-military actions were linked and framed as hybrid warfare with Russia[42].

Ukraine no longer has any chances of reclaiming the territories taken by Russia in 2014. In other words, hybrid operations, including those conducted as part of the subsequent invasion and the full-scale in 2022, have led to the complete takeover of these territories. Moreover, they have significantly strengthened the RF's capabilities to conduct further hybrid operations in Ukraine and across the EU and NATO eastern flank.

In Russia, hybrid warfare is seen as an endeavour to undermine its sovereignty, civilisational distinctiveness and status of one of the world's major powers. This strategy is described as a combination of destructive and constructive actions, with the ultimate goal of causing the self-disorganization and self-disorientation of the target state. Destructive

[40] K. Pynnöniemi, *The concept of hybrid war in Russia: A national security...*, p. 3.

[41] Ibid., p. 4.

[42] Ibid.

actions are those taken by the West to divide Russian society, destroy Russian culture, and erase its traditions. Constructive actions, on the other hand, are simply Russia's defence against these activities. In Russian academic debate, the United States is identified as the main actor behind these efforts. In turn, not only the US but also the EU are mentioned in state documents as those who provoke tensions in Eurasia, especially in Ukraine[43].

In 2003, General Makhmut Gareev distinguished 3 categories of threats to Russia:

1) threats to Russia's political sovereignty and, as a result, its status as a great power,
2) possibility of using nuclear weapons against Russia,
3) the third group of threats is multi-dimensional – it includes rapid development of military technology, as well as disruption of the equilibrium of power near Russia's borders[44].

This division is still relevant. It currently coincides with Russia's persistent antagonism towards NATO and EU nations, especially regarding the situation in Ukraine. In 2013, General Gareev claimed that a significant geopolitical transformation has occurred globally, fundamentally changing the balance of power and the nature of threats, thereby requiring novel strategies and methods of response. The updated threat typology encompasses the creation of controlled chaos to incite diverse forms of unrest in adversarial nations, the subversion of undesirable power structures from within, and the destabilisation of a state's internal cohesion, exemplified by the situations in Libya and Syria[45].

Following the Crimea attack, Gareev said Russia should be proud of its actions and improve the use of soft power along with political, diplomatic, and informational tools – these components are essential for a strategic deterrent system[46]. Concurrently, hybrid warfare is defined as a strategic coercion tool[47].

In Russian military terminology, strategic deterrence encompasses a collection of offensive and defensive instruments – nuclear, non-nuclear,

[43] Ibid.

[44] Ibid., p. 5.

[45] Ibid.

[46] Ibid.

[47] Ibid.

and non-military – that collectively constitute a "combined strategy of containment, deterrence, and coercion"[48]. Russia views deterrence as measures intended to avert conflict. Moscow employs intimidation as a deterrent, motivated by the fear of potential repercussions (e.g. threatens nuclear weapon deployment to dissuade others from utilising them against itself). The amalgamation of military and non-military coercive strategies is regarded as a strategic threat to Russia[49].

Hybrid warfare is defined as a type of non-military strategic coercion that includes economic sanctions, cyberattacks, and information operations. These actions seek to subvert Russia's political framework, provoke discord in its adjacent territories, and contest its position as a dominant force in a multipolar world[50]. The RF therefore not only identifies hybrid threats for itself, but also makes full use of its capabilities to attack other nations in this way in all domains where it identifies threats. The RF performs these actions before it becomes a target itself.

Russia's hybrid threat tactics against the Baltic Sea region

A model example of the RF's actions in the near abroad is the instrumentalisation of hybrid attacks as a tool of destabilisation. The variety of tools at Russia's disposal – from kinetic threats (such as sabotage) to non-kinetic threats (such as disinformation)[51] – is expanding every year, and Russian intelligence services are consistently intensifying their operations, seemingly without fear of repercussions or countermeasures.

The rise in aggressive activities has been particularly noticeable in the countries of NATO's eastern flank since February 2022 – namely, Estonia, Latvia, Lithuania, Finland, Poland, and Sweden. The objective is to weaken support for Ukraine, create internal instability in these nations, and destabilise the unity of EU and NATO structures[52]. Given the new

[48] Ibid., p. 6.

[49] Ibid.

[50] Ibid.

[51] H. Praks, *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region…*, p. 5.

[52] Ibid., pp. 6–7.

US administration and the uncertain situation in Ukraine, the eastern flank countries are likely the next targets for destabilisation.

Russia is determined to operate below the threshold of open war, as it understands that a prolonged conflict with NATO could end in Moscow's defeat and the complete restructuring of Russia's political system. The Kremlin's long-term goal is to reorganise Europe's security architecture and expand Russian influence – both by exerting control over Central and Eastern Europe and by securing favourable interlocutors in Western European countries[53].

Russian disinformation is built on crafting a false narrative of Ukraine's inevitable defeat, portraying EU and NATO governments as neglecting their own citizens in favour of supporting Ukraine, and exploiting social media to manipulate public opinion and shape societal moods[54]. The volume of fake news aimed at discouraging support for Ukraine and fostering hostility toward its citizens is increasing daily. Some segments of European societies believe these narratives, which in turn fuels reluctance to aid Kyiv. This also serves as a means for the Kremlin to identify which groups are most susceptible to manipulation.

One of Russia's greatest assets is its diaspora in the Baltic states and Central Asia. Moscow actively supports pro-Russian organisations, funds initiatives promoting the Russian language, and strongly opposes the removal of Soviet monuments. It also uses various institutions, including the Orthodox Church, as political tools[55]. On top of that, Russian intelligence agencies work to recruit new operatives.

Russia has established a comprehensive espionage network along NATO's eastern flank, particularly visible during operations in the Baltic states commencing in late 2023. In January 2024, Estonia's Internal Security Service (Estonian: Kaitsepolitseiamet, KAPO) apprehended a Russian political science professor from the University of Tartu, who was purportedly engaged in espionage for over a decade[56]. Around the same time, KAPO uncovered a group suspected of working with Russian intelligence to carry out vandalism and physical attacks in Estonia. By April 2024, authorities had arrested 13 people, some of whom had previous

[53] Ibid., pp. 7–8.

[54] Ibid., pp. 9–10.

[55] Ibid., pp. 12–13.

[56] Ibid., p. 14.

criminal records. The group successfully carried out several attacks, including damaging the personal car of Estonia's Minister of Internal Affairs and defacing monuments linked to the country's resistance against the Soviet Union. Estonian officials described these incidents as part of a hybrid warfare strategy[57].

Russian intelligence also relies heavily on hacker groups to attack CI and government institutions. A December 2023 report from the European Union Agency for Cybersecurity (ENISA) revealed that half of all DDoS attacks that year were connected to Russia's war on Ukraine[58]. This came just as the US announced it was halting its own cyber operations against Russia[59].

For years, Russia, in cooperation with Belarus, has been using migration as a tool to exert pressure and influence on neighbouring countries. Moscow and Minsk manipulate migration flows through disinformation, using people from the Middle East, Africa, and Central Asia to create controlled migration pressure. This forces NATO countries to strengthen their security infrastructure and intensify discussions on updating legal regulations. Migration pressure was used before the invasion of Ukraine to test NATO's response and stir public opinion, as well as before Finland's accession to the Alliance[60]. Similar tactics are applied against Ukraine and Georgia to prevent their closer integration with NATO or Western structures in general.

Frontline states are the most vulnerable to hybrid threats, such as sabotage of CI. One reason for this is that Europe's underwater network of cables and pipelines was not designed with hybrid warfare threats in mind[61]. The same goes for acts of sabotage and efforts to polarise societies, inciting protests and creating tensions. All of this is aimed at destabilising countries that oppose Russia.

[57] Ibid., p. 15.

[58] Ibid., p. 18.

[59] M. Untersinger, *Les Etats-Unis ordonnent une pause des cyberopérations contre la Russie, selon plusieurs médias,* Le Monde, 4.03.2025, https://www.lemonde.fr/pixels/article/2025/03/03/les-etats-unis-ordonnent-une-pause-des-operations-cyber-contre-la-russie_6575971_4408996.html [accessed: 4.03.2025].

[60] H. Praks, *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region...,* pp. 19–20.

[61] Ibid., p. 21.

Maritime hybrid threats and legal aspects of maritime infrastructure protection

The definition of hybrid threats by the Hybrid CoE specifies that these are coordinated and synchronised actions deliberately targeting systemic and institutional weaknesses using a wide range of means. This also applies to actions carried out in the maritime domain[62].

Hybrid actions, such as partial maritime transit blockade or restriction of access to state infrastructure, can pose significant risks for geographically small nations that typically rely on 1 or 2 critical maritime facilities[63]. This is now more evident in the context of cable disruptions (e.g. fiber optic, energy) in the Baltic Sea, as well as Russia's use of the so-called shadow fleet. Such actions force EU countries to respond and continuously monitor all ship movements in the Baltic Sea.

It should be emphasised that a flagship model of hybrid attack is an attack on underwater CI (e.g. pipelines)[64]. This is an example of an action that will undoubtedly continue to recur in the contemporary competition for resources.

An increasingly common threat, associated with the development of AI and other new technologies, are cyberattacks, categorised as hybrid threats. Such attacks may result in the loss of control over vessels, damage to port infrastructure, and interruptions in supply chains[65]. Cyberspace has similarities to the maritime operating environment, particularly in terms of its dispersion, maneuverability, and difficulty in control.

The maritime domain presents various opportunities for covertly undermining the security of particular CI, with the intent to harm or incapacitate it. An adversarial state may utilise underwater weaponry, deploying it by itself or through someone else and trigger explosions near the CI. A potential scenario entails the establishment of control zones surrounding islands. Although this contradicts the United Nations Convention on the Law of the Sea[66] (UNCLOS), an adversary may adopt a strategy of *faits accomplis* or assert claims to such regions – typically

[62] *Hybrid CoE Paper 16: Handbook on maritime hybrid threats...*

[63] Ibid., pp. 19–20.

[64] Ibid., pp. 12–13.

[65] Ibid., pp. 14–16.

[66] *United Nations Convention on the Law of the Sea, drawn up at Montego Bay on 10 December 1982.*

to establish a checkpoint, a military installation, or to ensure access to resource deposits, fishing stocks, or a transportation route within an exclusive economic zone[67].

China has been developing artificial islands and military facilities in regions also claimed by the Philippines, Vietnam, and Malaysia. They implement a policy of faits accomplished facts, constructing infrastructure and asserting control over navigation in areas where they lack full rights under UNCLOS. Subsequent to the annexation of Crimea, Russia instituted control zones in the Sea of Azov and surrounding the Kerch Strait, thereby impeding Ukraine's access to its ports. Japan and China are embroiled in conflicts regarding the Senkaku Islands, as China consistently dispatches coast guard vessels, establishing a de facto presence that may result in a change of control over the region.

An antagonist is also capable of deliberately carrying out illegal detentions and inspections of maritime vessels, justifying these actions under the pretext of counterterrorism efforts. Boarding a vessel may result in sabotage of its infrastructure or the installation of harmful and espionage software[68]. This is another method of negatively impacting operations in the maritime domain, where vessels remain constant targets of hostile actions.

Hostile states may use fleets of fishing boats (of non-state origin) or instrumentalise non-state groups to exert pressure on CI and maritime units[69]. This tactic involves leveraging ship owners, their fleets, or flags to create the illusion that the perpetrator is from another country and not, for example, Russia.

Unfriendly states may use weather modification technologies, e.g. by spraying chemicals into the atmosphere to induce rain, storms or fog, or even artificially initiate phenomena similar to natural disasters aimed at paralysing the CI of their target. A hostile nation may use these actions as a smokescreen to carry out a hybrid attack, involving for example damaging underwater telecommunications and energy infrastructure[70].

A hybrid attack may also entail the intentional obstruction of a maritime strait. Firstly, it makes it more difficult for states to guarantee

[67] *Hybrid CoE Paper 16: Handbook on maritime hybrid threats...*, p. 17, 21.

[68] Ibid., p. 27.

[69] Ibid., p. 36.

[70] Ibid., p. 46.

the unimpeded transit of maritime vessels, and secondly, it can trigger an international political crisis, by paralysing both the domestic and foreign relations of the targeted state[71]. Such actions, especially regarding the Suez Canal or the Bab-El-Mandab Strait, should be anticipated in the future due to the establishment of new naval bases in the Horn of Africa. This also illustrates a potential threat that may arise in the Baltic Sea.

Further threats result from violations of international law, mainly violations of the UNCLOS. The recommendations presented in *the Handbook on Maritime Hybrid Threats: 15 Scenarios and Legal Scans* emphasise potential responses that comply with international legal standards. Over-reliance on this legal framework carries significant risks. This is because an asymmetry arises: some entities operate within the limits of the law, while others take advantage of its limitations, which gives them a strategic advantage. In such instances, the benefits gained from a successfully conducted hybrid attack can significantly outweigh the negative consequences resulting from international legal sanctions, which prompts some states to deliberately violate the law. This indicates that in a period of escalating geopolitical competition, addressing the actions of aggressors may prove exceedingly difficult, leaving mitigation and damage repair as the sole alternatives.

A potential protection strategy involves the maximum marginalisation of the hostile state or non-state actor, accompanied by continuous monitoring. This would aid in reducing the implementation of its detrimental actions, particularly in the area of maritime security.

The protection of maritime CI has become a pressing issue in light of recent hybrid threats targeting undersea cables and pipelines. The report highlights the growing vulnerabilities in this domain, particularly as state and non-state actors exploit regulatory gaps and technological weaknesses to conduct disruptive operations[72]. These hazards, which can have significant geopolitical, security, and financial ramifications, include sabotage, cyberattacks, and interference with marine traffic[73]. Securing maritime assets has become a top concern for EU members and NATO

[71] Ibid., p. 31.

[72] A. Sari, *Hybrid CoE Research Report 14: Protecting maritime infrastructure from hybrid threats…*, p. 5.

[73] Ibid., p. 6.

allies given the vital part marine infrastructure plays in global trade, energy distribution, and communication networks[74].

Legal systems have great power to solve these problems, but they also impose major constraints. The UNCLOS convention, by establishing jurisdictional zones allowing coastal states different degrees of control over maritime activities, make it difficult for states to act decisively against hybrid threats arising outside their territorial boundaries given the scattered character of legal regulations. Although current legal tools give general authority for preserving situational awareness, they lack clear procedures for reactions, especially in cases of threats developing in international waters[75].

The vulnerability of submarine communication cables, essential for global internet connectivity and financial transactions, is a significant concern. Hybrid threat actors have exhibited their capacity to target these cables, as evidenced by the recent incidents in the Baltic Sea[76]. The RF, as previously stated, has no qualms about intensifying the nefarious activities it has conducted in Central and Eastern Europe in recent years.

The challenge of assigning accountability for these hybrid attacks complicates adequate response, as offenders may exploit jurisdictional ambiguities to avoid legal liability. The need is for close international collaboration and intelligence-sharing systems to prevent potential threats, considering both the economic and security risks linked to such disruptions[77].

It is necessary to develop and publish a comprehensive strategy to mitigate these vulnerabilities. Initially, states must guarantee the comprehensive application of their domestic legal frameworks to effectively implement legislative and executive jurisdiction, in accordance with the provisions of UNCLOS. This involves recognising that there are legal deficiencies, which hybrid threat actors can exploit and adapting national legislation to enhance cross-border cooperation in the field of law enforcement. Secondly, legal interpretations must be modified to address emerging threats, including the intentional targeting of undersea infrastructure via cyber and kinetic methods[78].

[74] Ibid., p. 8.

[75] Ibid., pp. 16–17.

[76] Ibid., p. 27.

[77] Ibid., pp. 32–36.

[78] Ibid., p. 32.

Another key recommendation is the reinforcement of diplomatic efforts to establish new international rules for the protection of critical maritime assets. The report suggests that EU and NATO members work collectively to strengthen regulatory measures, including the adoption of binding agreements that enhance the security of submarine cables and pipelines. Additionally, joint exercises and real-time information-sharing initiatives should be expanded to improve threat detection and response capabilities[79].

The evolving nature of hybrid threats requires a proactive and adaptive legal strategy. States must be prepared to update and expand their policies in response to emerging challenges. Safeguarding maritime infrastructure is not just a national security concern but a global imperative[80]. This issue is particularly relevant in the Baltic Sea region.

Summary

The research analysed, based on Hybrid CoE studies, provides a comprehensive understanding of hybrid threats, particularly their implications for CI in the European Union, with a strong impact on Central-Eastern Europe. The main malicious actor in recent years has been, and still is, the RF. However, more adversaries are using hybrid tools to increase their presence and influence. At the same time, the nature of hybrid threats is rapidly evolving.

The study *The Landscape of Hybrid Threats: A Conceptual Model* provides a broad view of the evolution and mechanisms of hybrid threats posed by both state and non-state actors. In turn, *The Concept of Hybrid War in Russia: A national security threat and means of strategic coercion* provides an understanding of Russia's strategic goals by portraying its hybrid activities in the context of geopolitical competition. *Handbook on maritime hybrid threats: 15 scenarios and legal scans* emphasises the need to focus more on maritime area (mainly in the Baltic Sea), which is vital for the EU and NATO in terms of infrastructure, economic and transport stability, as well as regional security. Equally crucial is *A comprehensive resilience ecosystem*, which underlines the need of resilience against changing hybrid threats and

[79] Ibid., p. 36.

[80] Ibid.

supports national and international security structures. This is especially important now since Europe has to concentrate on its own security and cannot rely just on US backing. *Russia's Hybrid Threat Tactics Against the Baltic Sea Region* is an indispensable tool for comprehending attacks and acts of sabotage. It should be taken into account in the development of new policies, as it offers a concrete case study of Russian hybrid tactics together with their impact and required countermeasures. *Protecting maritime infrastructure from hybrid threats: legal options* points up important legal weaknesses in maritime security, supporting global cooperation and legal changes.

Emphasising the need for proactive security policies, resilience-building actions, and legal changes to effectively address emerging challenges, these studies provide essential insights for understanding and minimising hybrid threats to the CI of EU countries. It must also be added that the states on the eastern flank are struggling with the challenge of responding to the RF and non-state actors and have to take care of their own security.

Current research on hybrid threats reveals multiple dysfunctions within the EU's system for countering these threats, which hinder effective action. They must be eliminated immediately by:

a) developing a transcontinental agreement to counter hybrid threats,
b) delineation of particular states, organisations, and factions that may be a source of hybrid threats,
c) revision of existing definitions of hybrid threats, given the phenomenon's continual evolution,
d) validation of terminology and shared characteristics of hybrid threats, warfare, and terrorism,
e) standardisation of legal systems of international community in the field of crimes and activities related to hybrid threat, as well as other criminal acts,
f) preservation of a cohesive counter-hybrid threats policy within international alliances,
g) reassessment of plans and strategies in state counter-hybrid threats programmes, which would enhance target orientation and funding for pertinent organisations engaged in combating hybrid threats,

h) implementation of a long-term counter-hybrid threats policy with continuous funding and training for essential counter-hybrid threats units,

i) thorough education of the public, particularly children and adolescents, regarding the hybrid threats that exist, as well as the perception and comprehension of diverse religions and cultures[81].

Finding an appropriate way to combat hybrid threats is a fundamental objective at both national and international level. An objective assessment of the evolution of this phenomenon is closely linked to the development and coordination of a counter-hybrid threats policy and the raising of public awareness of it. The nature of these threats determines the actions and the emergence of laws that are the government's response to the dangers. Stereotypes should be replaced by in-depth analyses aimed at recognising hybrid threats as an overriding threat to state security, given its diversity depending on the territory in which they occur. Hybrid threats can take different forms in the Baltic States, France, Poland and Ukraine. It is relevant to be aware of its existence, its evolution and its increasing incidence. Counter-hybrid threats activities must be given greater prominence in political debates and scientific research. This is the only way to reach valid conclusions and conceptualise practical actions, also at the international level.

The European Union and NATO have demonstrated that there is a strong mutual will to strengthen security in the Euro-Atlantic area and to combat hybrid threats jointly. Time is needed to develop specific solutions. In a dynamic geopolitical environment, only a multi-level security policy will enable objectives to be achieved. Both the EU and NATO have instruments of military and political cooperation for an effective response. It is crucial not only to eliminate emerging threats, but also undertake global initiatives to prevent them[82]. In this respect, the main focus should be placed on the challenges in Central and Eastern Europe. However, for these to be carried out effectively, the commitment of each Member State is essential. With no permanent and unwavering cooperation, the current efforts of international structures may turn out to be futile.

Hybrid CoE should initiate research on hybrid threats emanating from external actors in Africa and the Middle East, particularly in the context of Europe. It is imperative to provide an annual hybrid threat assessment

[81] A. Olech, *French and Polish fight against terrorism*, Poznań 2022, p. 198.

[82] A. Olech, *Cooperation between NATO and the European...*

for EU Member States, utilising reports from national security agencies. It would be also beneficial to convene roundtable discussions, both in-person and online, for EU experts specialising in hybrid threats. Their discussion of the most pressing challenges and concepts could result in a report containing multiple perspectives of hybrid threats, taking into account each country's circumstances. From the author's viewpoint, the Hybrid CoE is prepared to establish a transnational strategy for addressing hybrid threats.

In 2025, more than a decade after the Russian assault on Ukraine and 3 years after the full scale invasion and various hybrid attacks on EU Member States, it is imperative to enhance not only policies and resilience but also to respond more effectively. The characteristics of these threats clearly indicate that hybrid warfare is already underway, as confirmed by analyses conducted by the Hybrid CoE. In the current situation, implementing proactive countermeasures and building systemic resilience is just as important as diagnosing and describing the nature of these actions.

Bibliography

Olech A., *French and Polish fight against terrorism*, Poznań 2022.

Internet sources

Giannopoulos G., Smith H., Theocharidou M., *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, Publications Office of the European Union, Luxembourg 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf [accessed: 2.01.2025].

Hybrid CoE Paper 16: Handbook on maritime hybrid threats: 15 scenarios and legal scans, March 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/03/NEW_web_Hybrid_CoE_Paper-16_rgb.pdf [accessed: 17.01.2025].

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, https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf [accessed: 22.01.2025].

Olech A., *Cooperation between NATO and the European Union against hybrid threats with a particular emphasis on terrorism*, Institute of New Europe, 17.03.2021, https://ine.org.pl/en/cooperation-between-nato-and-the-european-union-against-hybrid--threats-with-a-particular-emphasis-on-terrorism/ [accessed: 10.02.2025].

Praks H., *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*, May 2024, https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf [accessed: 30.01.2025].

Pynnöniemi K., *The concept of hybrid war in Russia: A national security threat and means of strategic coercion*, Hybrid CoE Strategic Analysis / 27, May 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/05/20210518_Hybrid_CoE_Strategic_Analysis_27_The_concept_of_hybrid_war_in_Russia_WEB.pdf [accessed: 10.01.2025].

Sari A., *Hybrid CoE Research Report 14: Protecting maritime infrastructure from hybrid threats: legal options*, March 2025, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf [accessed: 6.03.2025].

Untersinger M., *Les Etats-Unis ordonnent une pause des cyberopérations contre la Russie, selon plusieurs médias*, Le Monde, 4.03.2025, https://www.lemonde.fr/pixels/article/2025/03/03/les-etats-unis-ordonnent-une-pause-des-operations-cyber-contre-la-russie_6575971_4408996.html [accessed: 4.03.2025].

Legal acts

United Nations Convention on the Law of the Sea drawn up at Montego Bay on 10 December 1982 (Journal of Laws of 2002 item 543).

Aleksander Olech, PhD

Head of International Cooperation at Defence24. Lecturer at both national and international universities, NATO associate, analyst, and publicist. Former Deputy Director of the Department of Africa and the Middle East at the Ministry of Foreign Affairs. Graduate of the European Academy of Diplomacy and War Studies University. Main research interests: French-Russian relations, challenges in Africa and NATO security policy.

Contact: a.olech@defence24.pl