Journal on Baltic Security, 2023; 9(1): 32-68

Research Article

Open Access
https://doi.org/10.57767/jobs_2023_001

Teresa Usewicz and Jarosław Keplin*

Hybrid Actions and Their Effect on EU Maritime Security

Received 21 July 2022
Accepted 20 January 2023

Abstract: This article addresses the hybrid challenges to the maritime security of the European Union. While hybrid threat issues are generally extensively reported in scientific literature, the authors point out that their integration with EU maritime safety issues represents a novel study strategy. The article contends that the maritime space is crucial for the prosperity and safety of EU Member States. The authors suggest potential applications for using the maritime environment as a site for hybrid impacts. The results of the conducted research are essential in determining the directions in which EU security and safety policy and those of the various Member States will develop. Attention to the possibility of using maritime spaces for hybrid warfare is a necessary condition for an effective response. Proper threat identification requires monitoring and cooperation of many actors.

Keywords: European Union, maritime security, hybrid threats

* **Corresponding author:** Teresa Usewicz, PhD. Polish Naval Academy Filipkowskiego street 20/2 81-578 Gdynia Poland t.usewicz@gmail.com
and Jarosław Keplin, PhD. Pomeranian Univeristy in Słupsk, Krzysztofa Arciszewskiego street 22A 76-200 Słupsk Poland, jaroslaw.keplin@apsl.edu.pl

Introduction

The contemporary environment is susceptible to dynamic processes that, both in the eyes of states and international organizations alike, make ensuring a state free from threats an increasingly demanding task. The concept of state security has evolved as a result of changes in the security environment. In recent years, the 2014 Russian annexation of Crimea acted as a turning point in thinking about security issues in Europe. This was also the moment when the terms 'hybrid war', 'hybrid conflict', 'hybrid threats', 'grey zone operations', or 'fourth-generation conflict' began to proliferate in public discourse. These terms quickly gained popularity, and the debates in academia and the military at the time resulted in many interpretations of these phenomena being presented in the literature. However, rather than clarifying their nature and separating them from other threats, these attempts to define hybrid threats have only popularized the term.

The European Union, like other actors, was forced to adapt to the changing international security environment. Several documents on the fight against hybrid activities have been adopted to that end. However, because the European Union is not a state, but rather an international organization, the situation is particular. Therefore, its powers are limited, especially in the area of security in its broadest sense. Through its institutions and specialized agencies, the European Union seeks to coordinate actions to raise the level of security both within the EU and its immediate neighbourhood. However, it cannot interfere with the security policies of the Member States. Such actions are usually aimed at initiating new cooperation mechanisms among the Member States or coordinating and monitoring existing ones. One of the areas where cooperation is particularly desirable and its effects are evident is maritime security. Its significance has grown in recent years in the EU, individual Member States, and globally. Maritime transport, marine resources, and energy resources accumulated in the seabed are only some of the aspects vitally affecting the economies of many countries.

Moreover, these issues affect coastal and inland states that rely on the seas and oceans. The European Union recognizes the importance of maritime spaces for the security and economic development of the Member States. In doing so, it is

taking some steps towards sustainable use of marine resources, the protection of vulnerable marine ecosystems, and strengthening the capacity of states to protect and defend their maritime areas and other areas of EU interest. An awareness of hybrid operations are one of the elements that must be included in the process of building the maritime capabilities of states. However, neither scientific literature nor EU documents support this.

The authors note that the possibility of hybrid action at sea is rarely presented in the public debate and in academic studies, which, in their view, leads to a gap in the research approach to European Union security.

The Approach to Methodology in Addressing the Adopted Research Problems

A complete analysis of hybrid action is challenging. This is primarily due to the broad and multifaceted nature of the research field. As a result, hybrid actions in the context of their impact on EU maritime security were chosen as the subject of study, with time, space, the sources of these actions, characteristics, and dependencies among the studied areas as the research categories.

This approach determined the main objective of the article as an attempt to consider hybrid actions in the process of ensuring EU maritime security. The main research problem was formulated based on the research objective, as expressed by the question: *How could hybrid operations impact EU maritime security?*

Conducting theoretical-empirical scientific research on the presented research problem necessitated its division into the following specific problem areas.

- The following specific research problems were identified at the preliminary research stage: How are hybrid threats defined?
- How are hybrid threats addressed in concept papers, as well as the performance of selected institutions and other actors in the fields of internal security and EU CSDP?
- How vital is maritime security for the security of the EU as a whole?

- How can the marine environment be used in hybrid operations?
- In light of the need for the Member States and the EU to ensure maritime security, how should the European Union prepare for hybrid threats?

Adopting such specific problems is critical for clarifying and understanding the hybrid characteristics of threats as part of the scientific search for the subject of research concerning previous achievements in this area.

The analysis of the issues under consideration enabled us to present the following research hypothesis:

> The EU maritime space is critical for the security and prosperity of Member States and as such, it is potential source of hybrid impacts. Hybridity is a dysfunctional feature that makes it challenging to recognise and identify threats and potential aggressors, significantly reducing the European Union's maritime security. A potential adversary can exploit several different elements in this aspect, one of which is the particular vulnerability of democratic states to hybrid impact.

To solve the research problems, various, mainly theoretical, research methods and techniques were used. Learning about little-known features of hybrid threats and examining their negative impact on EU maritime security made it possible to verify the working hypothesis. From the point of view of research design this necessitated the application of a multi-stage research process and many theoretical and empirical research methods used adequately to the type of problem being solved. Therefore, from a methodological perspective, the study needed to be essentially based on an inductive approach, which is an attempt to understand hybrid threats and find solutions to the problems they pose.

The research work primarily involved desk-based research of scientific articles, monographs, websites, and normative and conceptual documents adopted by various institutions and entities, especially at the EU level. An essential component of the research was observation and expert consultation conducted during participation in the *Multinational Capability Development Campaign* (MCDC) in the *Countering Hybrid Warfare* (CHW) project of the 2015-2016 and 2017-2018 editions and the Hybrid Warfare Table Top Exercise organized in 2018 by the European Center of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki.

Another method used by the authors was comparative analysis, which was used to compare the definitions of hybrid threats and, as a result, to identify some recurring elements, which are universal features in the approach to defining this type of threats.

A consideration of the theoretical aspects of the hybridity on the contemporary security environment was one of the two main stages of the research. The second concerned the maritime dimension of EU safety in the context of hybrid actions. According to the authors, the synthesis of the hybridity of modern threats to the EU, with the issue of EU maritime security as its locus, has achieved a new quality and filled a niche in scientific literature. Although hybrid threats are relatively well-described in the extant literature, as is maritime security, the combination of these two elements in terms of EU security provides a new picture of reality.

The literature reviewed in this article is divided into two categories. The first category relates to understanding and explaining hybrid threats based on the approach of international organizations and institutions. The discussion deliberately omits the approaches of various researchers in this regard. The second category includes literature that determines the approaches of international organisations and institutions in countering hybrid threats as a practical component to dealing with such challenges.

Analysis of Terms and Concepts Used in the Subject Literature

As mentioned above, the hybrid nature of the contemporary security environment began to be strongly emphasised after 2014. Nevertheless, this does not mean that similar activities did not take place earlier. Over the centuries, they have been used mainly by non-state actors, separatist or terrorist groups. These were primarily overt or covert activities conducted below the threshold of war, aimed at achieving specific objectives, using a wide range of tools, both military and non-military. Even a cursory analysis of the evolution of the security environment reveals that as early as in ancient China, one can find inclinations towards hybrid actions.

One of the most significant ancient thinkers and philosophers of this period, the author of the oldest and at the same time one of the most famous manuals on warfare, Sun-Tzu, called the 'fox of war', was a promoter of non-violent settlements. As A. Waldron notes, 'Sun-Tzu, concerned not with war so much as with the methods best employed by soldiers, seeks to minimize the use of force, rather as did the mercenary leaders, the condottieri of the European renaissance' (Sun-Tzu, 2007, p. 14).

His maxims provide a crucial intellectual basis for understanding hybrid action. In this ancient thinker's approach, the propagation of deception and manipulation influence the mood in the enemy's ranks. According to him, the ideal solution is to achieve the set goals without bloodshed. 'Being victorious a hundred times in a hundred battles is not the most excellent approach. Causing the enemy forces to submit without a battle is the most excellent approach' (Sun-Tzu, 2007, p. 85).

Today, hybrid activities take on different forms. Non-state actors, as well as states use them. Effectiveness in action is what counts.

It is worth noting that the first definitions of hybrid threats appeared in US studies (e.g., Training Circular TC 7-100 Hybrid Threat, November 2010) even before 2014. However, only the international shock caused by Russia's illegal annexation of Crimea and Sevastopol prompted analysts and experts to seek new terms for the situation we were in. As A. Rácz notes,

> The term hybrid war did not emerge immediately after the start of the Russian operation in Crimea. While the elusive, indirect, and highly effective warfare conducted by the Russian forces took not only Ukraine but the whole world by surprise, experts and journalists were casting around for expressions to describe this suddenly emerging, unprecedented phenomenon. When the Russian operation unfolded in late March, even the leading military and defense affairs journal Jane's had not yet come up with a concrete name but spoke only about a 'novel approach to warfare' (Rácz, 2016, p. 40).

This thesis is supported by the words of US General Philip Breedlove, Commander of NATO forces in Europe, who stated in one of his interviews for the German newspaper '*Die Welt*', commenting on the events in Ukraine, '(...) the big problem for NATO is how to react to the new way of waging war. We are working on it' (Bolzen, 2014).

Since 2014, many definitions of conflict and hybrid threats have emerged. This article primarily focuses on those proposed within NATO and the EU.

The NATO Glossary of Terms and Definitions presents a Hybrid Threat as a 'type of threat that combines conventional, irregular and asymmetric activities in time and space' (AAP-6 Edition, 2020, p. 64).

This is a very synthetic account of the problem under study in general. It does not explain the actual problem or specify the operating environment and the conflicting parties. In turn, the European Centre of Excellence for Countering Hybrid Threats proposed the following definition:

> The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil, or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution (Hybrid CoE).

This approach clarifies that these are actions below the threshold of open conflict in which possible means and methods of violence are vaguely formulated. Such a broad spectrum of impact on areas of state function allows these measures to be freely interpreted and, in practice, classified as mere threats. It is worth mentioning that the possible means of influence are also used in classical wars and by states and non-state actors in times of peace.

In 2016, the European Union adopted the Joint Framework on countering hybrid threats a European Union response JOIN(2016) 18 final. They include the following definition of hybrid threats: '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' (European Commission, 2016). This is a broad definition, but unlike the others, it attempts to identify the entity that may

carry out these activities, the purpose for which they are carried out, the means and ways of exerting pressure, the environment/area in which the activities may be carried out. This means that, in this approach, the effects that may result from a hybrid action are considered necessary. In contrast to the definitions presented earlier, it means that the aggressor, while undertaking hybrid actions, may preserve existing economic and/or diplomatic relations. This also implies that these activities can be carried out within the framework of the state's normal operations, without the use of military instruments.

A similar approach to hybrid threats is outlined in the aforementioned Bi-SC Input to a New NATO Capstone Concept for the Military Contribution on Countering Hybrid Threats. It states that 'hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives' (NATO Supreme Allied Commander, 2010, p. 2).

The NATO definition refers to the situation that an aggressor may use in the event of regional instability, a tense political situation in a country as a target of a potential attack, but also in case of uncontrolled migration and natural disasters, which could significantly contribute to the achievement of its objective.

According to the Allied Joint Doctrine, the concept of Hybrid Threats 'occurs where conventional, irregular and asymmetric threats are combined in the same time and space. Conflict could involve a range of transnational, state, group, and individual participants operating globally and locally. Some conflicts may involve concurrent inter-communal violence, terrorism, cyberspace attacks, insurgency, pervasive criminality, and widespread disorder. Adversaries may also choose a long-term strategy to avoid defeat rather than seeking victory, to try and outlast NATO's will and determination' (NATO Standard AJP-01, pp. 2-11).

In the presented approach, one can see a significant definitional extension of the studied problem. The analysis of the definition constructed in this manner allows us to conclude that the definitional scope has widened in comparison to the previous ones. Space and time were highlighted as two factors. Hybrid threats can have a global scope or develop only in national or minority groups, and the aggressor's action can be implemented over time.

A similar definition can be found on the NATO website:

> Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace and attempt to sow doubt in the minds of target populations. They aim to destabilize and undermine societies (NATO, 2021).

It is worthwhile to consider the definition proposed by the Council of Europe, or more precisely its Parliamentary Assembly, which has not been oblivious to the growing number of hybrid threats. Resolution 2217(2018) refers to 'hybrid war, which poses a new type of threat consisting of a combination of military and non-military techniques such as cyber-attacks; mass disinformation campaigns, including fake news, in particular via social media; interference in election processes; disruption of communications and other networks; and many others' (Parliamentary Assembly, 2018).

Despite many attempts to define hybrid warfare and hybrid threats, some military researchers and theorists believe that using these terms is counterproductive and, in some cases, even dangerous.

N. Freier believes that hybrid threats can be everything to everyone. He argues that the enemy must be aware of and prepared for all challenges in any war, not just selectively for a particular type of threat. He adds, 'Most thoughtful analysts agree that warfare has always had high-low, hybrid components' (Freier, 2009, p. 8).

E. Richborn-Kjennerud and P. Cullen also recognised the problem of imprecise definitions of hybrid warfare and hybrid threats. They point out that definitions in the area of hybridity, especially those published after 2014, refer directly to Russia's actions rather than to the phenomenon understood holistically. The definitions presented are broad enough to encompass a wide range of phenomena, and their interpretability is broad enough to distort the picture of the traditionally

understood term in times of peace and war (Richborn-Kjennerud and Cullen, 2016, pp. 1-2).

The presentation of hybrid warfare from the perspective of the Russian Federation is critical for the theoretical consideration of the phenomenon of hybridity. For Russia, the term hybrid war has more of a propaganda dimension than a classification one. According to Russian researchers and information presented in the media, it is argued that the term hybrid war does not originate from Russian military strategic thinking. To the contrary, hybrid actions are attributed to the West. From the perspective of Russia, the current threats to the West are better described as a political war (Galeotti, 2018).

R. Pukhov, director of the Center for Strategic Analysis and Technology in Moscow, also criticises the Western view of hybrid war theory. Analysing the events in Ukraine, it can be described as a low-intensity conflict that is similar to other historical events. He adds that no new tactics have been used in Ukraine (Wójtowicz, 2016, p. 111).

Pukhov did, however, note that hybrid warfare had become a significant challenge for NATO due to the Alliance's commitments, as these activities do not meet the standard definition of warfare and have fallen into the so-called 'grey zone' (Dura, 2021).

It is worth mentioning that cyber threats are often cited as an example of hybrid threats in the pertinent literature. It is important to emphasise that the increase in cyber threats has not fundamentally changed the dimensions of war and peace but only expanded their spatial dimension. Similarly, actions in the economic sphere that may be deliberate hybrid actions resulting in, for example, the creation of a state of economic dependence, manipulation of the currency exchange rate, and many others, remain threats from the economic area, not hybrid threats. Diplomatic actions between states are not considered hybrid threats because they aim to reach economic agreements or obtain military support for the represented country, thereby avoiding open conflict. Hybrid activities, on the other hand, can exist between these two dimensions. They are used as a less expensive alternative to classical armed conflict. In hybrid actions, the effects of a hostile action are recognised sooner than the aggressor being the perpetrator of these threats.

Depending on the goal and how the proxy is used, the aggressor makes its actions difficult to detect. Therefore, priority should be given to the specifics of these risks and their interconnections. Moreover, globalisation, modern technologies, and digitalisation have significantly increased their effectiveness and the possibilities to influence selected goals. It is also to be expected that in the future, NGOs and private military companies will be used as proxy, and that the area of future conflicts will be cyberspace as a platform from which 'low-intensity warfare' will be waged indirectly (Mumford, 2013, pp. 40-46).

Hence, it is essential to continuously monitor the security environment through the lens of informational, political, and economic activities to detect the characteristics of hybrid activities at an early stage. The appearance of these elements, at least in part, may be indicative of the hybrid activities undertaken (Niedzielski, 2016, p. 40).

In summary, attempts to define hybrid warfare and hybrid threats were intended to help understand contemporary threats that challenge state security in the 21st century. Indeed, this approach was intended to facilitate capacity development to counter and respond to these threats. The concept of hybrid warfare and threats is widely used without a recognised definition and explained in many ways. This is due to the variety of research concepts, the way it is understood, and the authors' views of the proposed definitions.

The article's authors assume that despite the multiplicity of definitions of hybrid threats, some essential elements constitute a common element to define this type of threat.

Based on the definitions presented, it is possible to advance a thesis that the actions described through the tools used, under conditions of peaceful functioning of the state, can be viewed as *hybrid actions*. The term action in this article refers to the *intentional behavior of a state or non-state actor that will result in the expected response of the area of influence (e.g., state policy, public behavior, receipt of information consistent with the will of the aggressor)*. In contrast, the term hybrid threat is understood as the effect of a hybrid action.

A key element that appears in almost all definitions of hybrid threats is the combination of conventional and unconventional actions and the use of information as a weapon of warfare. For the last few years, actions in the cognitive sphere have become increasingly important; they allow not only manipulating large social groups, influencing their moods and diluting responsibility for these actions. One of the fundamental difficulties in combating hybrid threats in the information space is assigning specific actions to specific actors. As stated by US Army Lieutenant General Karen H. Gibson, Deputy Director of National Intelligence for National Security Partnership, 'The challenge for US intelligence is identifying, and providing 'public attribution of what our adversaries are doing' (Garamone, 2019).

The ambiguity and blurring of responsibility are primarily the result of a combination of conventional and unconventional actions, as well as the use of information to divert societal attention or shape a widespread conviction of a given actor's innocence while attributing responsibility to another designated entity.

As a result, threats with hybrid characteristics and features are from the result of an adversary's deliberate action, where the aggressor's intentions are determined by the target of the action, the vulnerability of the attacked, and the aggressor's capability.

The characteristics for hybrid impact are primarily:

- Achievement of the aggressor's long-term goal;
- Conducting activities indirectly through a proxy;
- Avoiding the crossing of 'thresholds' that could be considered as violations of, e.g., international law, UN mandates, international treaties, or conventions;
- Conducting intensive information/disinformation activities by controlling the media and using world events to divert attention from the actual aggressor;
- The use of high-tech tools in a manner inconsistent with their original purpose;
- The use of terrorist and cyber-terrorist attacks as an element of intimidation of state governments and the public.

Furthermore, hybrid actions need not always be destructive in their effects on areas of state function; sometimes, their purpose may be to generate situational discomfort and concern.
In conclusion, therefore, it can be assumed that hybrid actions are complex and multi-faceted. Depending on the objective pursued, the party undertaking such activities may carry them out in various areas, differing in time, space (geographical area), and intensity.

Moreover, an analysis of available literature on hybrid threats leads to the following observation: this issue is well described and identified among the Euro-Atlantic states. NATO and EU Member States are increasingly aware of the complexity and multidimensionality of the activities to which they may fall victim. Simultaneously, social and cultural conditions render them particularly susceptible to this kind of impacts. Liberal democracy and de facto constituent elements such as freedom of thought, professed values, political pluralism, individualism, equality of rights, respect for minority rights, and freedom of action in the public sphere are conducive to the use of hybrid tools. A liberal society is open and tolerant, but it is also much more susceptible to new ideas that enter it with ease, primarily through social media. Potential adversaries are well aware of this. They are aware that liberal democracy is also a power struggle that is decided at the ballot box, which means that one has to meet the expectations of the voters from time to time. These expectations can be shaped, thereby influencing the decision-making in a country.

In this context, an interesting case study might be the 2016 Brexit referendum. According to a report published by the Intelligence and Safety Committee of Parliament, Russia interfered in British politics, particularly in the independence referendum in Scotland and the campaign leading up to Brexit. The report states that 'Russia considers the UK one of its top Western intelligence targets' (Intelligence and Security Committee of Parliament, 2020, p. 2); it also says that Russia conducts activities in cyberspace with the help of criminal groups aimed, among other things, at interfering in elections in other countries. The article

provides the following examples of Russia promoting disinformation and attempting to gain political influence:

> • 'Use of state-owned traditional media: open-source studies have shown serious distortions in the coverage provided by Russian state-owned international broadcasters such as RT and Sputnik;
> • 'Bots' and 'trolls', as open-source studies have identified significant activity on social media;
> • 'Hack and leak': the US has publicly avowed that Russia conducted 'hack and leak' operations concerning the 2016 Presidential Election, and it has been widely alleged that Russia was responsible for a similar attack on the 2017 French Presidential Election; and:
> • 'Real life' political interference: it has been reported that Kremlin-linked entities have made 'soft loans' to the (then) National Front in France, seemingly at least in part as a reward for the party's support that of Russia's annexation of Crimea and the GRU-sponsored failed coup in Montenegro in October 2016 – an astonishingly bold move in a country just a few months away from its accession to NATO' (Intelligence and Security Committee of Parliament 2020, p. 9).

This example demonstrates that geographical distances and borders are irrelevant for hybrid activities. These actions are 'tailor-made' based on the situation in a given country and the adversary's desired outcome. The range of possibilities here is endless. For this reason, hybrid threat definitions are generally quite broad, if not 'flexible'. This is primarily because they must address dynamic changes in the safety environment and encompass multiple activities that are often difficult to capture and identify. Actors who use such tools have almost unlimited possibilities, and their 'creativity' and potential for harm can astound even the most well-prepared actors.

Hybrid Threats and EU Security

In the case of internal security, the situation is specific as a shared competence (according to Article 4 of the Treaty on the Functioning of the EU). This means that both the EU and the Member States carry out tasks in this area. Nevertheless, the Member States bear the primary responsibility. Under the non-violation clause (Article 72 of the Treaty on the Functioning of the EU), the EU must not undermine the exercise of the responsibilities of its Member States for maintaining law and order and safeguarding internal security. Therefore, it is the responsibility of the states to ensure resilience in the context of hybrid and all other threats.

The key document regarding internal security is currently the EU Security Union Strategy for 2020 to 2025. The lack of a clear indication that the document only deals with aspects of internal security indicates a shift in approach to safety and a more holistic view of it. As Margaritis Schinas, Vice-President for Promoting our European Way of Life, notes,

> Security is a cross-cutting issue which goes into almost every sphere of life and affects a multitude of policy areas. With the new EU Security Union Strategy, we are connecting all the dots to build an entire security ecosystem. It is time to overcome the false dichotomy between online and offline, between digital and physical and between internal and external security concerns and threats (European Commission, 2020).

The term 'hybrid' appears as many as 25 times, which for a 28-page document shows the priority given to this type of threat. It is worth noting that the previous strategy on internal security adopted in 2010 did not mention this type of threat.

The Strategy identifies four priority areas for EU action, namely:

- A future-proof security environment;
- Tackling evolving threats;
- Protecting Europeans from terrorism and organized crime;
- A strong European security ecosystem.

In the part devoted to 'Tackling evolving threats', next to cybercrime, modern law enforcement, and countering illegal content online, provisions concerning hybrid threats have been included. They mention, among other things, the necessity of

treating the issue of hybrid threats in a comprehensive manner, i.e., combining the external and internal dimensions of security. Such an approach must 'cover the full spectrum of action - from early detection, analysis, awareness, building resilience and prevention through to crisis response and consequence management' (European Commission, 2020a). Building resilience is key in this context, and the first step should be to define benchmarks for the different sectors in which Member States and EU actors operate.

The strategy underlines that while the primary responsibility for countering hybrid threats lies with the Member States, 'some vulnerabilities are common to all the Member States and some threats extend across borders, such as targeting cross-border networks or infrastructure (EU Security Union Strategy, 2020, p. 14). Interestingly, the authors of the document note that due to the COVID-19 pandemic, 'the potential for more sophisticated and hybrid attacks by state and non-state actors has increased, with vulnerabilities exploited through a mix of cyberattacks, damage to critical infrastructure, disinformation campaigns, and radicalization of the political narrative' (EU Security Union Strategy, 2020, p. 4).

It is worth mentioning that the strategy also announces the creation of a restricted online platform for Member States' reference on counter-hybrid tools and measures at the EU level.

In the case of the CSDP, the EU's role is even more limited. This is the exclusive competence of the Member States, and cooperation in this area is intergovernmental.

According to Article 42 of the Treaty on European Union, the CSDP provides the EU with an operational capacity that draws on civilian and military assets, which can be used for peace-keeping missions, conflict prevention, and strengthening international safety. These tasks shall be executed based on capabilities provided by the Member States. The CSDP is an integral part of the Common Foreign and Security Policy, implemented within the EU by setting general guidelines and adopting decisions defining actions, positions, principles, and enhancing systematic cooperation among states. The European Council is responsible for defining the strategic directions for developing this policy. However, its implementation is the responsibility of the High Representative for Foreign

Affairs and Security Policy and, above all, of the Member States. Decisions are taken in the Council of the European Union (CEU), specifically the Foreign Affairs Council (FAC), bringing together defence, trade, or development ministers, depending on the subject under discussion. Guaranteeing rapid access to the Union's budgetary resources for the immediate financing of Common Foreign and Security Policy initiatives, particularly mission preparation activities, remains an essential competence of the EU Council (the EU Treaty).

In the areas of safety, defence, and foreign policy, the European Parliament also has specific powers, derived from its legislative and control functions. Under Article 36 of the TEU, the High Representative of the Union for Foreign Affairs and Security Policy shall regularly consult the European Parliament on the Common Foreign and Security Policy and the Common Security and Defense Policy and shall be periodically informed on developments in these policies. Furthermore, he or she shall have the right to address inquiries in this field to the Council and the High Representative and make recommendations. Twice a year, a debate is also organized in the European Parliament on implementing these policies. The Parliament also adopts two reports, one on CFSP by the European Parliament's Committee on Foreign Affairs (AFET) and one on the CSDP by the Committee on Foreign Affairs Subcommittee on Security and Defense (SEDE).

The mission of the mentioned SEDE subcommittee is 'to enable in-depth public debate and close parliamentary scrutiny of all EU actions in the field of CSDP, particularly in terms of institutions, capabilities, and operations. The SEDE subcommittee intends to actively contribute to the formulation of the EU's security and defense policy', said its current chair, N. Loiseau (Loiseau, 2019).

It is worth mentioning that, as announced in 2015, a special cell for assessing hybrid threats has been created, i.e., The Hybrid Fusion Cell, part of the European External Action Service (EEAS). Its role is to generate strategic analyses to aid decision-makers.

The above-mentioned actors' actions must be correlated with the changing, highly dynamic international security environment. Recent years have seen an

intensification of efforts to ensure broadly understood security. On the one hand, this is a result of the emergence of new challenges and threats; on the other hand, an increasing number of elements are subject to securitisation. The growing number of actors within the EU and the subsequent documents that deal with safety issues show that the existing arrangements and mechanisms are insufficient and that further steps need to be taken. Hybrid threats have been one of the factors forcing a change in approach in recent years, both in the Member States and EU actors.

The intensification of activities in the area of security is evidenced, among other things, by the data contained in the SEDE Activity Report 2014-2019. According to this document, '77 committee meetings, 22 missions, 27 reports and opinions, 28 hearings, 10 workshops and some 60 studies, reflected an increasingly challenging, changing and volatile international environment' had been organised (SEDE 2019, p. 4).

In this document, hybrid threats are identified as anti-EU propaganda campaigns to distort the truth, provoke doubt, undermine societal trust, and divide the Member States. According to the authors, as a consequence, this may lead to a paralysis of the EU's decision-making processes and weakening its relations with strategic partners worldwide. The report also concludes that concerted efforts to strengthen the EU's capacity to counter disinformation and propaganda campaigns from third parties are needed to counter these phenomena effectively.

In the body of the document, the term *hybrid* appears 11 times in the following contexts:

- The specification of the EU's defense policy activities after 2016;
- Elements that have become an integral part of the SEDE agenda and have had a significant impact on its activities;
- EU and NATO cooperation;
- Critical threats to EU security;
- An integrated approach to crisis and conflict resolution, i.e., the adoption of the CSDP Civilian Agreement (2018);
- The subject of debate between SEDE members and NATO representatives.

Thus, one can see that hybrid threats have become a permanent element in the EU discursive space. The intensification of activities on this topic is noticeable in the activities of all entities involved in security and defense and security documents drafted after 2014.

In 'A Global Strategy for the European Union's Foreign and Security Policy', adopted in 2016, the term hybrid, on the other hand, appears five times, mainly in the context of the challenges and threats the EU must face, in connection with terrorism, climate change, and economic instability.

2016 also saw the release of the aforementioned Joint Framework on Countering Hybrid Threats, which was the EU's answer to changes in the security environment. The article comprehensively addresses the issue of hybrid threats. Another essential document in this area was the 2017 Joint Communication - A Strategic Approach to Resilience in the EU's External Action. The aim of the document was 'to identify how a strategic approach to resilience can increase the impact of EU external action and sustain progress towards EU development, humanitarian, foreign and security policy objectives, given the more fluid landscape of global challenges and risks that the EU global strategy describes' (European Commission, 2017). Meanwhile, several other documents have been adopted. The issue of hybrid threats figures prominently, including in an action plan against disinformation (European Commission, 2018a), 'Increasing resilience, and bolstering capabilities to address hybrid threats. Communication' (European Commission, 2018b) or the conclusions of the March 2018 European Council. (European Council, 2018). In addition, 2019 saw the adoption of the EU's new strategic agenda for 2019-24, with hybrid threats identified as one of the priority areas that affect the lives of EU citizens. In the same year, the Council of the European Union called for an enhanced joint action (Council of the European Union, 2019).

The document laid out the priorities and guidelines for countering and increasing resilience to hybrid threats. 'In its conclusions, the Council underlines the need to continue developing cooperation with international organizations and partner

countries on enhancing resilience and countering hybrid threats, in particular EU-NATO cooperation and cooperation with countries in the EU's neighbourhood' (Council of the European Union, 2019). It emphasises the importance of resilience of the EU states and actors in the context of disinformation, the development of state-of-the-art technologies, the protection of critical infrastructure, the interdependence of various critical functions and services, including financial services, and the critical role of the private sector. The key to success is close cooperation and action on many levels and a holistic approach to security. The European Union, like the Member States, must take care of security both externally and internally. The correlation between the two is particularly evident today, and ensuring internal security requires strong responses. Hence, missions and operations are an essential element of EU security and defence policy. It is worth looking at this issue in the context of hybrid operations.

There are currently six military operations and eleven civilian missions under EU auspices. Various activities are carried out within the framework of civilian missions and military operations, e.g., training, policing, and observation related to security sector reform. In these kind of operations, the perception of the participants in the mission by the country's citizens on whose territory they are deployed is crucial. Local social attitudes, mission participants, and the EU itself may be subject to hybrid interactions. An example is the EULEX mission in Kosovo, which is regarded somewhat sceptically by the Kosovars. Although 'the role of the EU and other donors is deeply rooted in the Kosovo system, much of the progress made comes from their contributions. However, from the citizens' point of view, they also share the blame for things that did not go well' (Rashiti 2019, p. 13). Public dissatisfaction with mission outcomes may provide fertile ground for hybrid actions, especially given that the Russian Federation has long convinced the people of the Western Balkans that their accession to the EU is highly improbable and that the EU itself is untrustworthy.

Considering the foregoing, it is reasonable to conclude that the issue of hybrid threats, unlike any other to date, combines the dimensions of the EU's internal and external security.

The blurred boundary between the internal and external security dimensions is the main reason that the possibility of hostile influence should be considered from the

internal perspective of the individual Member States and international actors such as the EU and NATO.

The Maritime Dimension of EU Safety and Hybrid Threats

The specific nature of the marine environment poses a challenge from the perspective of the services and others tasked with ensuring maritime security. The vastness of the seas and oceans, the difficulty in controlling and monitoring them, and natural hazards are just some of the difficulties faced by states and institutions in conducting maritime activities. In the case of the European Union, out of the 27 Member States, as many as 22 are maritime countries, i.e., have access to the sea. Having free access to the sea is a factor that gained in importance in recent years. This is due to many reasons, but the most important is the growing importance of maritime transport.

Nevertheless, maritime transport is only one of the factors to be taken into account when analysing the importance of the seas and oceans for the economies of EU countries. The multi-faceted impact of a coastal location on economic growth is quite widely described in scientific literature. However, it is undoubtedly worth to illustrate the importance of this factor to the EU itself. One of the most important determinants is seaports and their share in gross domestic product. They are an essential link in the transport chain, they logistical nodes, and places of employment for many people. They attract investors and technological innovation, which in turn increases the competitiveness of a country's economy.

There are over 1,200 seaports in the European Union, 329 of which are part of the Trans European Transport Network (ESPO, 2019). There are seaports on in the EU that are of crucial importance to the global economy. According to data published by the World Shipping Council, of the world's 50 largest ports, seven are located in the EU. In 2019, the total volume for these ports was 55.94 million TEU (World Shipping Council, 2019). The importance of maritime transport for Europe is also demonstrated by the number of connections between European

ports and different regions of the world. According to the European Port Performance Dashboard, these figures are as follows:

- With Africa - 348,
- With Central and south America - 629,
- With the Far East - 848,
- With the Middle East - 89,
- With North America - 340 (European port performance dashboard, 2012).

This means that Europe has the highest number of connections to ports in different regions of the world. This, in turn, is closely correlated with other elements that make Europe a maritime powerhouse. One of them is the shipbuilding industry, which is a strategic element of the economy of many countries. In 2019, the value of the shipbuilding industry globally reached $162.5 billion, with 285 active shipyards worldwide (as of April 2021). The European shipbuilding industry (according to the Shipyards' & Maritime Equipment Association of Europe, of which 16 European countries are members, representing almost 100 percent of the European shipbuilding industry) is made up of some 22,000 large, small or medium sized manufacturers and suppliers of seagoing vessels. They generate an annual production value of around €70 billion and directly employ over 320,000 people, accounting for 50 percent of the global market share European marine equipment (Shipyards' & Maritime Equipment Association of Europe, 2021).

The following data also demonstrates the strength of the maritime domain within EU countries:

- The EU coastline is 53,563.9 kilometres long and is almost four times as long as the land border, which is 13,770 kilometres long (CIA World Factbook, 2021);
- The traditional blue economy sectors provide 4.5 million direct jobs and generates over €650 billion in turnover (European Commision 2021, at VI);
- The marine living resources sector made profits of €7.3 billion in 2018 (up 49 percent from 2009) (European Commision 2021, p. 35);

- Use of marine renewable energy (such offshore wind) is growing, with a 15 percent increase employment in 2018 (compared to 2017) (European Commision 2021, at VI);
- Almost €500 billion worth of services are generated within a 10 kilometre coastal zone
- In 2018, the EU-27's Gross Domestic Product (GDP) was estimated to be €13,500 billion, with 193 million people employed. The contribution of the Blue Economy established sectors to the EU-27 economy in 2018 was 1.5 percent in terms of GVA and 2.3 percent in terms of employment (European Commision 2021, p. 6);
- 'The Blue Economy emerging, and innovative sectors include marine renewable energy (i.e., Ocean energy, floating solar energy and offshore hydrogen generation), Blue bio-economy and bio-technology, Marine minerals, Desalination, Maritime defense, security and surveillance, Research and Education and Infrastructure and maritime works (submarine cables, robotics). These sectors offer significant potential for economic growth, sustainability transition' (European Commision 2021, at VI);
- 'The majority of oil and gas production in Europe takes place offshore. Following the departure of the United Kingdom from the EU, which operates 363 offshore installations, there are currently around 193 installations in European waters. Given the EU's high energy demand, these operations help ensure a secure supply of energy' (Safety of Offshore Oil and Gas Operations Directive).

Given the above data, the seas and oceans generate a range of benefits for EU economies, and their importance will increase in the years to come. Therefore, the possibility of all kinds of disruptions and threats affecting the stability, security and safety of maritime economic sectors should be a matter of concern at both the national and supranational levels. The European Union, recognising the importance of maritime safety, adopted the Maritime Safety Strategy (2014). The document clearly states that 'the EU depends on open, protected and secure seas and oceans for economic development, free trade, transport, energy security, tourism and good status of the marine environment' (European Union Maritime

Security Strategy, p. 2). Moreover, the EU's maritime interests are not limited to adjacent basins but are defined globally, so that the EU's area of interest is de facto the entire global maritime domain. The number and multiplicity of linkages between states that use the seas and oceans compel us to think about security of *interconnected vessels*. Instability and disruptions in energy supply or other commodities in distant regions are often quickly reflected in small, local markets, affecting individual and industrial customers. In analysing the EU maritime domain in the context of hybrid threats, protecting the marine environment from such threats can be particularly challenging. First of all, there are various human activities, both civilian and military, that occur in the seas and oceans. In addition, the marine environment is an area of competition and clash between state and non-state actors. Rivalries range from territorial disputes to mineral and energy resources to the control over specific bodies of water and trade routes. As a result, in terms of hybrid operations, it is possible to express the belief that the maritime plane has a high potential for harm.

In the next part of the article, examples of hybrid impacts in the marine environment are shown.

Primarily, it is essential to note that businesses in maritime industries are digitising their operations, increasing the risk of cyber incidents.

> In a 2020 Safety at Sea and BIMCO Maritime Cyber Security survey, despite the majority of respondents (77%) viewing cyber-attacks as a high or medium risk to their organizations, few appear to be prepared for the aftermath of such an attack. 64% of respondents said their organization has a business continuity plan in place to follow in the event of a cyber-incident. However, only 24% claimed it was tested every three months, and only 15% said that it was tested every six to 12 months. Only 42% of respondents said that their organization protects vessels from operational technology (OT) cyber threats, and some respondents went so far as to describe their company policy to OT cyber risk as 'careless' (A Comprehensive Guide to Maritime Cybersecurity, p. 4).

According to the authors of the report cited above, the number of attempted cyber incidents targeting the maritime industry has increased by 400 percent since 2020. Maersk, among others, saw how severe the losses caused by such incidents could be, when in 2017 'the largest container ship and supply vessel operator with

offices across 130 countries and over 80,000 employees went dark after being hit with NotPetya' (A Comprehensive Guide to Maritime Cybersecurity, p. 8). As a result of the attack, Maersk lost most of its data, with over 49,000 laptops and 4,000 servers destroyed. Damages were estimated at over $300 million (A Comprehensive Guide to Maritime Cybersecurity, p. 9). There were, of course, more similar events (e.g., China Ocean Shipping Company in 2018 or Norsk Hydro in 2019). It should be emphasized that, in addition to reputational and financial losses, a cyber-attack targeting the maritime industry poses a real threat to the lives and health of people working on the seas and oceans and infrastructure, as well as marine ecosystems. Such actions can also have political ramifications and compel states or other actors to behave in certain ways. Another element to consider is the activities of environmental organisations, which can become a tool in the hands of actors conducting hybrid operations. Increased protection of the world's seas and oceans is becoming increasingly important, both for countries and industry. Grassroots pro-environmental initiatives, particularly popular in European Union societies, are increasingly being reflected in pre-election campaigns at various levels in the Member States. They are becoming the focus of public debate as well as the efforts of many NGOs and individual EU citizens. Without a doubt, the situation is difficult. According to data compiled by the World Health Organization, 'to date, marine ecosystems, particularly coastal ecosystems, have lost 19–35% of foundational habitats globally, such as seagrass meadows, coral reefs, and mangroves' (World Health Organization- (WHO), 2019).

Human activity is responsible for the majority of the pollution that enters the seas and oceans. Moreover, 'Eighty percent of pollution to the marine environment comes from the land. One of the biggest sources is called nonpoint source pollution, which occurs as a result of runoff. Nonpoint source pollution includes many small sources, like septic tanks, cars, trucks, and boats, plus larger sources, such as farms, ranches, and forest areas' (National Ocean Service). Thus, the most significant source of pollution in the oceans is human activity, particularly transport and the associated risks to the marine environment. This issue is

increasingly alarming and a clear threat to human life and health. Hence, the possible use of pro-environmental organisations that could lead, for example, to blocking maritime transport routes or entrances to commercial ports is one possible way to shake up a country's maritime economy and transport. Such actions may be judged as legitimate by the public, which, coupled with possible ineptitude on the part of the state and the services, may result in public dissatisfaction and several other negative consequences.

When looking at potential areas for hybrid action, another factor to be considered is maritime disputes between states, the most common cause of which is fishing and oil resources. An interesting point in this context is that 'Analyzing data from the issue Correlates of War project, which includes diplomatic conflicts over maritime areas (1900–2007) in the Americas, Europe, Middle East, and Asia. This study finds that pairs of democracies have the highest chance of experiencing diplomatic maritime disputes among all pairs of countries in the same region or dyads involving major powers' (Daniels & Mitchel, 2017, p. 293-310). A dispute between Denmark and Canada, for example, dates back to the 1970s when the border between Canada and Greenland was drawn. The dispute is over Hansa Island and its overlapping economic zones. A special task force was established in 2018 to develop recommendations to resolve the dispute. However, according to Professor M. Byers, the dispute is convenient for the governments of both countries and recurs most often before elections, 'So the politicians play this dispute, they can beat their chests over Arctic sovereignty knowing that there is absolutely zero risk involved: we are not going to war with Denmark, it is an important military and economic partner' (Sevunts, 2018). Thus, the dispute is instrumentalised on a political level; nevertheless, it is equally likely to be used as a tool in hybrid actions, e.g., to manipulate public opinion or to weaken the position of selected individuals or communities. It should also be noted that 'Previously neglected maritime boundary disputes are acquiring newfound economic, political, and academic significance. Rising sea levels, changing distributions of marine natural resources, and growing demand for those resources have combined to create a 'perfect storm' for policy-making, diplomacy, and research' (Byers & Østhagen, 2019).

To summarise, states that face unresolved maritime disputes should expect an adversary to take advantage of such conflicts.

Directly related to the issue of establishing maritime borders and unresolved disputes between states in this regard is the question of the law of the sea and international humanitarian law, which can also be used as a tool to achieve the objectives of a potential aggressor. Such a situation will occur when an actor, using the provisions of the law, creates situations that will cause difficulties for international consensus. Thus, the other actors do not have adequate situational awareness or tools to counter the situation (Lohela & Schatz, 2019).

Today, states and international organisations can identify ambiguous situations at sea according to the interpretation of the law as to the act itself. An example of this is Nord Stream 2, which the European Commission's report presents as *New Tools of Hybrid War*. According to the European Commission, this is an opportunity for the Russian Federation to influence markets by using dumping prices as a tool to discontinue LNG supplies (Ariev, 2018).

Another example of the instrumentalisation of maritime law in the context of achieving strategic objectives can be found in China's activities in the South China Sea. China's naval militia, the symbol *par excellence* of China's hybrid warfare doctrine, is used for this purpose. The officers of this formation, disguised as fishermen, attack ships passing through or operating in the South China Sea.

Another exemplification of Chinese hybrid actions is the construction of artificial islands to take control of disputed territories without provoking military escalation. In both cases, diplomatic and political activity conducted through information and disinformation activities in the international space justifies Chinese foreign policy as an essential element of its hybrid strategy (Miracola, 2018).

Other potential risks from hybrid impacts in the marine environment include:

- Illegal migration, including smuggling and human trafficking, and the associated terrorist risks, as the coastal location of most EU countries is a favourable factor for the development of such threats, so the 'use' of illegal

immigrants as a tool in hybrid operations should be taken into account in forecasting the changing safety environment;

- Disturbances in power generation systems;
- Activities in space, such as an attack on GPS satellites: although no serious events have been reported to date, disruptions in their functioning should be included in the research;
- Development of new technologies used in all areas of state activity: Their general availability means that their use could be disruptive to maritime security when not used for their original purpose. The interpenetration and combination of threats will create situations that are difficult to predict (Concept and Doctrine Centre UK, 2014, p. 3-17),
- Resurgent and aspiring superpowers will want to revise the existing international order and adapt it to their needs, not necessarily using lawfare.

Summary

Since ancient times, access to the sea has been essential in positioning states in geopolitical space. On the one hand, the maritime environment generates several opportunities, such as the establishment of trade and diplomatic contacts. However, on the other hand, it was a source of threats from both nature and man. The current conditions of the marine environment are similar. What has remained the same is the specificity of the sea and the asymmetry of human efforts concerning natural forces. Despite the enormous technological advancements and more efficient crossing of nautical miles, the sea remains a ruthless verifier of human powerlessness and smallness in the face of its power.

Moreover, competition in the maritime space between states and other users of the world's seas and oceans has intensified. It is becoming increasingly difficult to ensure security in the marine environment. On the other hand, it is a necessity, as maritime transport routes are the lifeblood of modern economies. It is difficult to imagine global transport functioning based on land or air transport alone. All of this leads to the conclusion that maritime security is critical for both the state and international organisations. In this article, the authors have identified the EU perspective on this issue. Employing quantitative analysis, they tried to prove the importance of these issues for the EU Member States. Moreover, it synthesises

the issue of EU maritime safety with the hybridity of the international safety environment widely discussed in recent years. As a result of their research, the authors have generated several conclusions and insights.

First, the question invariably remains legitimate: does singling out hybrid threats really represent an improvement in providing for the security of states and international organisations? Or is it just a new term for methods that have been proven and used for centuries? The authors believe that while the specifics of the actions themselves are not new, the conditions in which contemporary states and social groups operate are quite avant-garde. First and foremost, this is due to globalisation and the unprecedented use of information and communication technologies.

If we accept that it is legitimate to distinguish hybrid threats and actions, then the challenge is to understand them uniformly; the question of what are hybrid threats and actions de facto and what should be understood by them? remains valid. The interpretation of these concepts, especially within the European Union, should be based on consistent understandings as this determines how to counteract hybrid threats and the tools used. However, above all, it translates into greater awareness on the part of governments, international organisations, and societies. Currently, the semantics around hybrid threats are fuzzy and vague, leading to confusion and different interpretations of the same elements. So, there is an urgent need to harmonise the definitional aspects in this area, both within NATO and across the EU. This is particularly important given the increased cooperation between the two entities and between the Member States. Identical perception is an indispensability for building trust and cooperation between EU and NATO countries in countering hybrid threats. It is also an essential element in gaining the resilience of states and jointly preparing tools to deter potential adversaries.

Moreover, the article points out that although there is a tendency among states and international organizations to identify hybrid threats, according to the authors, one should also pay attention to which area of a state's function a given threat comes from for the requisite response. The adjective *hybrid* is meaningless on its

own. Identification of the area of state functioning (e.g., economic, social, or military) from which a given threat originates facilitates taking specific actions and implementing appropriate defense mechanisms. There should be algorithms for action by relevant services and other actors concerning hybrid threats. In the case of maritime safety, this is particularly important, as hybrid activities in this environment can cause significant financial losses and lead to threats to human life and health.

In this context, emphasis should be placed on the importance of identifying flaws in state security systems. It is worth noting that each Member State should identify its own weaknesses. This is due, among other things, to the fact that each of them operates in changing conditions, which depend on the relations between states and the type of interests they pursue in the international arena.

However, this does not exclude, and indeed imposes, the need for joint action in certain areas, particularly in the context of building capabilities to combat hybrid threats.

The exchange of information, combating disinformation, monitoring the situation, and initiating joint ventures are just some of the areas of the fight against hybrid threats in which cooperation is necessary. Building common analytical tools to recognize and identify hybrid threats will enable the development of a decision-making process and rapid response to such actions. The maritime space is an example of an environment in which cooperation between the actors who use it is vital. States and international organisations, and the EU in particular, must have adequate forces and resources to maintain the security of their own waters and have the capacity and capability for international cooperation. The ability to have a global impact on the maritime domain is an important factor in positioning the EU on the international level. If the EU's position is to be strengthened in the years to come, Member States should ensure that it could actively create global maritime safety.

The article also points out that EU safety should be viewed holistically when analysing hybrid threats, including both its external and internal dimensions. Internal security cannot be discussed for an entity if its immediate environment is unstable and generates threats. In such a view, maritime safety will affect both

planes, and hybrid threats will be one of the key factors influencing its level. The authors have identified selected potential areas of maritime safety that could become the object of adversarial attack. Each of them constitutes a challenge in terms of ensuring national security, especially in the situation of a lack of awareness among the ruling elite regarding the importance of the maritime space for the state. The possibility of terrorist attacks, piracy, organised crime, violations of airspace and territorial waters, and obfuscation of responsibility for these acts can lead to governments being held responsible for them. As the article has already reasoned, democratic states are particularly susceptible to this kind of influence. Therefore, work must be started on concrete tools to protect public spaces from false information. The use of tools to verify the veracity of information is not prohibited by media freedom. Democratic governments must pay more attention to information messages and, if necessary, respond quickly and decisively to emerging disinformation. According to the authors, this is one of the key priorities in the fight against hybrid threats.

Bibliography

NATO. (2020) 'AAP-6 Edition NATO Glossary of Terms and Definitions', NATO Terminology Office.

Mission Secure. (2021) *A Comprehensive Guide to Maritime Cybersecurity*. Mission Secure. Available at: https://www.missionsecure.com/resources/comprehensive-guide-to-maritime-security-ebook (Accessed: 09 August 2021).

Ariev, Volodymyr. (2018) 'Nord Stream 2 and Russian gas: new tools of hybrid war', Parliamentary Assembly, Council of Europe. [online] Available at: https://pace.coe.int/en/files/24764#trace-1 (Accessed 22. August 2021).

Bolzen, Stefanie. (2014) 'Die NATO muss auf grüne Männchen vorbereitet sein' [NATO has to Prepare for Little Green Men], *Die Welt – Politik – Ukraine-Krise*. [online] Available at: http://www.welt.de/politik/ausland/article131296429/Die-Nato-muss-auf-gruene-Maennchen-vorbereitet-sein.html/ (Accessed: 27 January 2015).

Byers, Michael, and Østhagen, Andreas. (2019) 'Settling Maritime Boundaries: Why Some Countries Find It Easy, and Others Do Not', in *The Future of Ocean Governance and Capacity Development: Essays in Honor of Elisabeth Mann Borgese (1918–2002)*. By International Ocean Institute – Canada. Leiden / Boston: Brill Njihoff. [online] Available at:

https://brill.com/view/book/edcoll/9789004380271/BP000030.xml (Accessed: 04 September 2021).

CIA. (2021) 'European Union', *The World Factbook*. [online] Available at: https://www.cia.gov/the-world-factbook/countries/european-union/ (Accessed: 08 August 2021).

Council of the European Union. (2019) 'Countering hybrid threats: Council calls for enhanced common action', Press Release, 10 December. [online] Available at: https://www.consilium.europa.eu/en/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/ (Accessed: 18 July 2021).

Daniels, Kelly, and Mitchell McLaughlin, Sara. (2017) 'Bones of democratic contention: Maritime disputes', *International Area Studies Review*. Volume: 20 issue: 4, pp. 293-310.

Dura, M. (2015) Wojna hybrydowa. Powtórka z historii [Hybrid warfare. Repetition of history]. *Defence 24*. 02. June 2015. [online] Available at: https://www.defence24.pl/wojna-hybrydowa-powtorka-z-historii (Accessed: 10 May 2021).

ESPO. (2019) Priorities of European ports for 2019 – 2024 (2019). Memorandum of the European Sea Ports Organization for the new Commission and European Parliament. [online] Available at: https://www.espo.be/media/Memorandum%20ESPO%20FINAL%20Digital%20version.pdf (Accessed: 07 August 2021).

European Commission. (2016) Joint Framework on countering hybrid threats a European Union response: JOIN (2016) 18 final. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (Accessed: 08 July 2021).

European Commission. (2017) A strategic approach to resilience in the EU's external action. Communication, JOIN (2017) 21 final, 07 June. [online] Available at: https://ec.europa.eu/knowledge4policy/publication/2017-joint-communication-strategic-approach-resilience-eus-external-action_en. (Accessed: 16 July 2021).

European Commission. (2018a) Action plan against disinformation. Communication, JOIN (2018) 36 final, 05 December. [online] Available at: https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf. (Accessed: 16 July 2021).

European Commission. (2020a) Communication from the Commission on the EU Security Union Strategy 2020. COM(2020) 605 final. [online] Available at: https://eur-lex.europa.eu/legal-

content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605 (Accessed: 26 August 2021).

European Commission. (2020) EU Security Union Strategy: connecting the dots in a new security ecosystem. European Comission. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379
(Accessed: 26 August 2021).

European Commission. (2018b) Joint communication to the European Parliament, the European Council and The Council 'Increasing resilience and bolstering capabilities to address hybrid threats., JOIN (2018) 16 final, 13 July. European Commission. [online] Available at: https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf. (Accessed: 16 July 2021).

European Commision. (2021) The EU Blue Economy Report 2021. Available at: https://blueindicators.ec.europa.eu/published-reports_en (accessed 08 August 2021).

European Council. (2018) European Council meeting (22 March 2018) – Conclusions. 23 March. [online] Available at: https://www.consilium.europa.eu/en/meetings/european-council/2018/03/22-23/ (Accessed: 18 July 2020).

European Council. (2019a) A new strategic agenda, 2019–2024. Brussels, 20 June. European Council [online] Available at: https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/ (Accessed: 18 July 2021).

Council of the European Union. (2014) 'European Union maritime security strategy', Council of the European Union. [online] Available at: http://register.consilium.europa.eu/doc/srv?l=PL&f=ST%2011205%202014%20INIT (Accessed: 09 August 2021).

European Port Performance Dashboard. (2012) 'European Port Performance dashboard (EPPD) and EPO Mission Statement Presentation' [online] Available at: https://www.espo.be/media/D.12.1%20European%20Port%20Performance%20dashboard%20(EPPD)%20and%20EPO%20mission%20statement%20presentation.pdf
(Accessed: 19 July 2021).

Freier, Nathan. (2009) 'Hybrid Threats and Challenges: Describe… Don't Define', *Small Wars Journal*. [online] Available at: https://smallwarsjournal.com/blog/journal/docs-temp/343-freier.pdf (Accessed: 04 May 2018).

Galeotti, Mark. (2018) '(Mis)Understanding Russia's two 'hybrid wars', *Eurozine*. [online] Available at: https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/ (Accessed: 28 January 2019).

Garamone, Jim. (2019) 'Military Must Be Ready to Confront Hybrid Threats, Intel Official Says', U.S. Department of Defence. [online] Available at: https://www.defense.gov/Explore/News/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intelligence-official-says/ (Accessed: 05 September 2021).

Ministry of Defence. (2014) Global Strategic Trends – out 2045 Fifth Edition. Swindon, UK: Development, Concept and Doctrine Centre UK.

Hybrid CoE. (2020) 'Hybrid threats as a concept', *hybridcoe.fi*. [online] Available at: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (accessed 23 February 2021).

Intelligence and Security Committee of Parliament. (2020) 'Russia', House of Commons. [online] Available at: https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf (Accessed: 12 August 2021).

Lohela, Tiia et al. (2019) 'Handbook on Maritime Hybrid Threats - 10 Scenarios and Legal Scans', Hybrid CoE Working Paper 5. Hybrid COE. [online] Available at: https://research.ulapland.fi/fi/publications/handbook-on-maritime-hybrid-threats-10-scenarios-and-legal-scans (Accessed: 22 August 2021).

Loiseau, Nathalie. (2019) 'Welcome words', Subcomittee for Security and Defence, European Parliament. [online] Available at: https://www.europarl.europa.eu/committees/en/sede/about (Accessed: 05 September 2021).

Miracola, Sergio. (2018) 'Chinese Hybrid Warfare', Italian Institute for International and Political Studies. [online] Available at: https://www.ispionline.it/it/pubblicazione/chinese-hybrid-warfare-21853 (Accessed 22 August 2021).

Mumford, Andrew. (2013) Proxy Warfare and the Future of Conflict. *RUSI Journal*, April/May 2013 Vol. 158, pp 40-46.

NATO. (2021) NATO's response to hybrid threats. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm (accessed 25.05.2021).

NATO Supreme Allied Commander. (2010) Bi-Strategic Commands (Bi-SC) Input to a New NATO Capstone Concept for the Military Contribution on Countering Hybrid Threats.

NATO Standard AJP-01 - Allied Joint Doctrine, Edition E Version 1 (2017) NATO Standardization Office.

National Ocean Service. (n.d.) 'What is the biggest source of pollution in the ocean?' National Ocean Service [online] Available at: https://oceanservice.noaa.gov/facts/pollution.html (accessed 02 September 2021).

Niedzielski, D., Zagrożenia hybrydowe. Podstawowe informacje i zdolności Sił Zbrojnych RP[Hybrid Threats. Basic information and capabilities of the Polish Armed Forces], Kwartalnik Bellona 2/2016, Wojskowy Instytut Wydawniczy, Warsaw 2016.

Parliamentary Assembly. (2018) Legal challenges related to hybrid war and human rights obligations. [online] Available at: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24762&lang=en (Accessed 25 May 2021).

Pohl, Benjamin. (2013) 'The logic underpinning EU crisis management operations', *European Security*, Vol. 22 No. 3. [online] Available at: http://dx.doi.org/10.1080/09662839.2012.726220 (accessed 13 July 2021).

Rácz, András. (2016) *Russia's Hybrid War in Ukraine Breaking the Enemy's Ability to Resist.* Helsinki: The Finish Institute of International Affairs.

Rashiti, Naim. (2019) Ten years after EULEX Key principles for future EU flagship initiatives on the rule of law. CEPS Papers in Liberty and Security in Europe No. 2019-07. [online] Available at: https://www.ceps.eu/ceps-publications/ten-years-after-eulex/ (accessed 09 July 2021).

Richborn-Kjennerud, Erik, and Cullen, Patrick. (2016) 'What is Hybrid Warfare?' Policy Brief 1/2016. Norwegian Institute of International Affairs.

European Comission. (2013) Safety of Offshore Oil and Gas Operations Directive. [online] Available at: https://ec.europa.eu/energy/topics/energy-security/offshore-oil-and-gas-safety/offshore-oil-and-gas-operations-directive_en (accessed 08 August 2021).

SEDE (2019) Activity report 2014-2019 of the European Parliament's subcommittee on security and defense (SEDE).

Available at: https://www.europarl.europa.eu/committees/en/sede/home/publications (accessed 19 June 2021).

Sevunts, Levon. (2018) Canada and Denmark set up a joint task force to resolve Arctic boundary issues. Available at: https://www.rcinet.ca/eye-on-the-arctic/2018/05/23/greenland-canada-hans-island-sea-boundary/(accessed 04 September 2021).

Shipyards' & Maritime Equipment Association of Europe. (2021) Available at: https://www.seaeurope.eu/ (accessed 21 July 2021).

Statistica. (2019-2021) 'Number of ships in the world merchant fleet as of January 1, 2022, by type', Statistica. [online] Available at: https://www.statista.com/statistics/264024/number-of-merchant-ships-worldwide-by-type/ (Accessed 07 August 2021).

Sun-Tzu. (2007) *The Art of War Sun-Tzu's Military Methods*. translated by Victor H. Mair, Columbia University Press.

Szubrycht, Tomasz. (2006) 'Współczesne aspekty bezpieczeństwa państwa' [Contemporary aspects of state safety], *Zeszyty Naukowe Akademii Marynarki Wojennej Rok* XLVII Issue 4 (167), Gdynia.

Traktat o funkcjonowaniu Unii Europejskiej - tekst skonsolidowany uwzględniający zmiany wprowadzone Traktatem z Lizbony (Dz.U.2004.90.864/2) [Treaty on the Functioning of the European Union - consolidated text taking into account the changes introduced by the Treaty of Lisbon]. [online] Available at: https://arslege.pl/komptencje-ue-dzielone-z-panstwami-czlonkowskimi/k40/a10643/ (accessed 20 July 2021).

Traktat o Unii Europejskiej (TUE) - tekst skonsolidowany uwzględniający zmiany wprowadzone Traktatem z Lizbony [Treaty on European Union (TEU) - consolidated text taking into account the changes introduced by the Treaty of Lisbon] (Dz. Urz. UE 2016 C 202). [online] Available at: https://oide.sejm.gov.pl/oide/index.php?option=com_content&view=article&id=14803&Itemid=945 (accessed 21 July 2021).

World Shipping Council. (2019) 'The Top 50 Container Ports', World Shipping Council. [online] Available at: https://www.worldshipping.org/top-50-ports. (accessed 19.07.2021).

World Health Organization. (2019) 'Health, the global ocean, and marine resources', World Trade Organization. [online] Available at: https://www.euro.who.int/__data/assets/pdf_file/0009/404496/SDG-14-policy-brief.pdf (accessed 30 January 2021).

Wójtowicz, Tomasz. (2016) 'Konflikt zbrojny na Ukrainie jako przykład wojny hybrydowej' [Armed conflict in Ukraine as an example of hybrid war], *Kultura i nauka, Zeszyty Naukowe* 20/2016, Wyższa Szkoła Europejska, Cracow, 2016.