Navigating Diffuse Maritime Information Settings: A Heuristic for Improved Analysis of Hybrid Threats

Lukas Albrecht
Institute for the Protection of Maritime Infrastructures
German Aerospace Center Bremerhaven, Germany
lukas.albrecht@dlr.de

Tjorven Harmsen
Institute for the Protection of Maritime Infrastructures
German Aerospace Center Bremerhaven, Germany
tjorven.harmsen@dlr.de

Abstract—**This article introduces a heuristic designed to improve the understanding and identification of hybrid threats. In recent years, hybrid threat scenarios in the maritime domain have increasingly drawn attention, posing significant challenges for authorities and security agencies due to their ambiguous and nonattributable nature. Maritime incidents highlight the inherent vagueness and complexity of such events, which complicate timely detection and categorization by responsible institutions. The heuristic presented in this article demonstrates that effectively addressing hybrid threats requires an integrative perspective, as can be found in the third wave of security research—one that clearly maps the relationships and connections among involved actors as well as their embeddedness in global structures. This comprehensive approach enables scholars to understand hybrid threats as interconnected, multi-layered phenomena and to derive resilience criteria for the practice of security actors.**

Keywords—hybrid threats, maritime security research, integrative approach, reflexive modernization

I. Introduction

Over the past years, the issue of hybrid threats in the maritime domain has gained substantial public interest due to incidents regarding maritime infrastructure and concerns over so-called shadow fleets. Especially, recent events involving damaged subsea cables have become points of focus and put maritime operations in the spotlight of the media and security agencies. Yet, despite increased frequency of suspected sabotage activity, solid evidence is hard to come by. The maritime domain appears to be a particularly vulnerable venue for hybrid threats, as it is usually very difficult to ascertain what has really happened on the high seas or underwater. Recent cases, like that of the ship Eagle S, that are suspected to sabotage maritime infrastructure in the Baltic, show how ascertaining the truth and the struggle for interpretative dominance come into conflict. This is particularly problematic for security authorities, as they will not know for sure how to categorize an occurring threatening event. This points to the need for a conceptual framework that goes beyond simplistic analysis and leaves room for ambiguity, while at the same time ensuring the authorities' ability to act. This article takes the first steps in this direction by presenting a heuristic for analyzing hybrid threats.

II. Defining Hybrid Threats in the Light of Three Waves of Security Research

To anchor our heuristics in the research literature, we place hybrid threats in the wider context of security research. Three waves of research can be distinguished here [1, 2]. From the perspective of the first wave, a threat generally is something that is described as an “objective reality” and can be measured as “universally valid” [1: 47]. While such a factual understanding makes sense for simple threats, it leads to an analytical dead end in the face of hybrid threats. This is because hybrid threat situations are characterized by a high degree of vagueness, ambiguity and diffuseness [3, 4]. Whether it is a clear threat or even a deliberate attack from an opponent cannot be determined on the basis of a single event, but depends on the context and the embedding in a series of events. This points to the need for a more comprehensive, processual understanding. The second wave of security research has already pointed out that threats not only exist as pure facts in the world, but are perceived and constituted by social observers [1: 48]. They are thus phenomena of perception, behavior, and construction by social actors such as the population or organizations. However, reducing hybrid threats to mere perceptual phenomena would not do any favors to authorities and organizations that strive for careful detection. We are therefore joining the third and latest wave of security literature: the integrative approach. This understanding of threat situations “goes beyond unambiguously objectivist or constructivist conceptions” as it is interested in how both “criteria reciprocally cause and presuppose each other” [1: 48]. The integrative approach therefore focuses from the outset on dynamics (instead of exclusively factual states or pure perceptual phenomena).

The third wave of research does not replace the previous two, nor does it contradict them. Rather, third-wave research is concerned with capturing the “reflexive” character of complex risk situations. This means that risks and the issue of threat are placed in a larger temporal, spatial and social context. The focus is not on a threat event “for itself”, but there is a shift in emphasis: It is no longer primarily “about the probability of damage […] but about the extent to which a system is at risk or vulnerable” [2: 42f., authors’ translation]. Questions therefore revolve directly around the topic of resilience and how to deal with damage “that is more or less irreversible and cannot be completely eliminated.” [2: 43, authors’ translation]. Similarly, hybrid threats cannot be completely resolved by security actors involved, because they are linked to a larger, not least geopolitical and global social situation. We therefore advocate a consistent categorization in this third, more comprehensive perspective of security research.

In this article, we contribute to formulating hybrid threats in the third integrative wave, which has not yet been done explicitly. We argue that hybrid threat situations inherently involve dynamic complexity and ambiguity, necessitating an approach that embraces ambiguity tolerance. To clarify this point, we begin by outlining the particular challenge posed by the diffuse nature of contemporary cases.

III. Current Examples of Diffuse Hybrid Threat Situations in the Maritime Domain

Our article pursues a conceptual concern. We therefore do not present an empirical methodology, but merely want to illustrate the situations we are aiming at by way of example.

Prominent cases of hybrid threats regarding maritime infrastructure include the ships Newnew Polar Bear, allegedly damaging the Balticonnector natural gas pipeline and telecommunications cables in October 2023 [5], the Yi Peng 3, allegedly damaging the BCS East-West Interlink und C-Lion1 submarine cables in November 2024 [6], and the Eagle S, allegedly damaging the Estlink 2 cable in December 2024 [7].

The case of the Eagle S illustrates the problematic nature of clearly establishing objective factors of reality according to the first wave, due to diffuse information regarding incidents in environments characterized by constrains to communication and situational awareness, like the high seas or underwater. After the grid operator reported a power outage at the same time the ship was passing the cable in the Gulf of Finland, Finnish security agencies escorted, boarded, and detained the ship. Meanwhile, the ship's missing anchor was recovered heavily damaged and serious maintenance deficiencies have been found, substantiating the suspicion of the ship deliberately dragging its anchor across the seabed [8]. As of now, the ship has been released with some crew members remaining under criminal investigation [9].

While allegations of sabotage have persisted since the beginning, strongly suggesting that "the anchor-drag incident was intentional, given how many manual tasks would have to be performed and then overlooked by the crew to cause it by accident" [10], recent media coverage has objected by stating that "evidence gathered to date – including intercepted communications and other classified intelligence – points to accidents caused by inexperienced crews serving aboard poorly maintained vessels" [11]. With security and hybrid threat experts immediately weighing in, dismissing media claims about the incident's accidental nature [12], the difficulty of these cases in appearing very diffusely becomes apparent.

In light of hybrid warfare trying to capitalize on ambiguity and diffuseness, the problem of attributing these events occupies agencies and leaves them in a state of uncertainty [13]. Especially in cases such as that of the Eagle S, the heterogeneity of international security actors, classified intelligence, and a plurality of (anonymous) contradictory sources complicates a solely objective facts-based view – presenting the maritime domain as almost impenetrable and posing an immense challenge to security agencies that want to attribute hard facts.

IV. A Heuristic for Improved Hybrid Threat Analysis

In the context of the above, the question remains open, for security actors as well es for researchers, as to how hybrid threat situations can be suitably identified and defined if they are based on ambiguity and diffuseness and thus a particularly high degree of uncertainty. Our answer is quite simple: Instead of insisting on clarity at the level of the initial event, the ambiguity of the situation should be taken seriously. Such an ambiguity-sensitive perspective is realized in the third wave of security research, which – as explained before – refers to an integrative view of the interweaving of causes and effects and can thus tackle dynamic processes in a more comprehensive perspective.

In order to create this "larger" framework for analysis, we expand the view of hybrid threat processes away from event-centeredness to a larger scale in spatiotemporal dynamics. To this end, we utilize theoretical figures from third-wave security research and allow these to form the main structure of our heuristics as "fields of analysis" (see table below). Following this, we place the emergence of hybrid threats in the context of social change, which since Beck can be described as "reflexive modernization" [14, 15]. The systems of modernity are mutually intertwined, so that even minor changes in one context can trigger major effects in others. "Risk" becomes the "normal state" here, in that every decision can have societal and global consequences. Modernity is "reflexive" as it is aware of its own consequences as well as its attempts to control threats in the form of risk.

We derive a total of six fields of analysis from this overarching theoretical framework. *Firstly*, when analyzing hybrid threats, it is important to recognize the pattern of reflexive modernity: Not everything is "new" or unexpected in hybrid threat situations, rather the contemporary social space that the threat event encounters is decisive – and about this there are established findings and expectabilities (compare point 1 of the following heuristic). *Secondly*, in order to actually delineate new aspects of hybrid situations, it is necessary to identify where common risk expectations were exceeded and to link this with concepts of dynamic uncertainty and not-knowing (see point 3 of the following heuristic; a fundamental distinction between risk and broader uncertainty can already be found in Knight [16]). *Thirdly*, with third-wave security research, it can be assumed that various actors are actively involved in the process of dealing with uncertainties and producing security. In the context of hybrid threats, particular attention must be paid to the geopolitical conflict situation, which determines that we are dealing with "allies" and "adversaries" even before the next threat event occurs. Security and uncertainty are co-produced by both sides and its many intermediaries (see point 3 in the following heuristic). *Fourthly*, and linked to the interpretation of the situation by different actors, the analysis must pay attention to how the expertise considered important for decision-making shifts (see point 4 of the following heuristic). *Fifthly*, the handling of hybrid situations by organizations leads to the institutionalization of practices and thus to the creation of new routines and standards that deserve closer attention (see point 5 of the following heuristics). Finally, and *sixthly*, decision-making structures have a reflexive character, which can also be mapped and which can exist in different trajectories at the same time (see point 6 of the following heuristics).

These six fields of analysis presented can now be provided with questions in order to guide the research process. Our heuristics for analyzing hybrid threats therefore take the form of a catalogue of quesitons.

TABLE I. A Heuristic for Improved Hybrid Threat Analysis

Field of Analysis	Key Questions
(1) Risk development through modernization	How do hybrid threats emerge as side effects of maritime globalization and/or technology development?
(2) Uncertainty and not knowing	Which aspects are beyond the scope of traditional risk analysis?
(3) Co-production of security	What role does the interpretation of the geopolitical situation play? Which state and non-state actors are involved in security management operations? How is responsibility shared?
(4) Change in expertise	Whose knowledge is considered legitimate for assessment? What conflicts are there in the interpretation?
(5) Institutionalization of uncertainty	What routines and standards emerge to deal with uncertainty?
(6) Reflexive rationalities	Which decision-making logics shape the behavior of actors: linear- planning or adaptive-learning?

Fig. 1. A Heuristic for Improved Hybrid Threat Analysis

Figure 1 shows the six fields of analysis with correspondingly listed questions. Following the rather abstract introduction, we will now explain the six dimensions in more detail:

(1) *Risk development through modernization:* Understanding hybrid threats as side effects of (maritime) globalization guides relevant authorities to examine aspects like *dependence on trade routes* and *the privatization of security* which shape risk contexts due to implementation of new practices in the maritime domain. Likewise, investigating how technological developments are creating new vulnerabilities moves issues e.g. regarding *submarine cables* and *ports and their supply chain* into the spotlight. Analyzing hybrid threat events through the lens of risk development in light of modernization is crucial when dealing with both technical or conceptional innovations that alter established practices and may create new weak points. For instance, outsourcing security to private companies opens up possible gateways for malevolent actors, and states' dependence on submarine data or power connections can be leveraged in a broader geopolitical context – see the destruction of parts of the Nord Stream 2 pipeline in 2022, which transported natural gas from Russia to Germany amidst Russia's ongoing war in Ukraine.

(2) *Uncertainty and not knowing:* As hybrid threat activities capitalize on uncertainty, traditional risk analysis frameworks struggle to provide a suitable framework for hybrid threat analysis. Calculations merely considering probabilities and impact values are inept to completely capture ambiguous events without a clear originator. Anticipating that different involved actors will have different assessments of the situations at hand, by asking *which aspects are beyond the scope of traditional risk analysis*, prevents analytical dead ends. E.g. in the cases of suspected Shadow Fleet vessels engaging in suspicious patterns in the Baltic – like slowing down, zig-zag movements in the vicinity of subsea cables, or ships' AIS tracking systems changing information or going dark – authorities will have to accept that ascertaining intentional action by identifiable malevolent actors may be infeasible, especially when no obvious damage has been caused.

(3) *Co-production of security:* Understanding security as a product of cooperation by asking for *shared responsibilities* and *the roles of non-state actors* allows for better strategic crisis management, in that it puts focus on and takes advantage of coordination with key stakeholders like shipping companies, tech providers, and operators. As sketched in the case of the Eagle S, the grid operator immediately reported the power outage to security authorities, so that they could take time-critical actions, like intercepting the suspected vessel and arranging further investigations. Implementing this involvement of cooperative stakeholders can result in e.g. setting up communication channels and inter-coordinated procedures beforehand. However, not only security practices, but also insecurity should be considered as co-produced. To this end, it makes sense to explicitly reflect on the geopolitical categorization of the situation prior to an occurring event. The changed geopolitical interpretation of the overall situation plays a decisive role – because it is only with the previous interpretation that an incident in infrastructure context almost automatically becomes a security case, whereas a few years ago it would have treated as a safety case.

(4) *Change in expertise:* With hybrid threats playing out in multiple dimensions – e.g. legal, political, economic, military – different expert disciplines offer unlike perspectives. Asking *whose knowledge to legitimately consider for assessment* crucially codetermines the interpretation of threat events. In the same vein, asking *what conflicts are there in the interpretation* sheds light on different aspects relevant to hybrid threat analysis. While the logic of a military expert, for example, suggests that the focus must increasingly be on deterring the enemy, political and social scientists are quick to point out the secondary effects and long-term consequences that can result from decisions in favor of "more security", such as the militarization of civil security or the increase in social inequality in other areas.

(5) *Institutionalization of uncertainty:* If we reflect on how organizations deal with hybrid events over a longer period of time, we can observe the "learning paths" respective actors have taken. A key question here concerns *what organizational routines and standards emerge to deal with uncertainty*. Standard operating procedures or other routines change in the context of dealing with hybrid threats. It is worth taking a closer

look at the "built-in growth dynamic" [2: 38], i.e. not only how this improves handling, but also which security gaps could be associated with the establishment and institutionalization of security routines. A suitable error culture is crucial for this.

(6) *Reflexive rationalities:* One aspect of the analysis that is related to the point just mentioned concerns the culture of uncertainty in the organizations involved. Risk sociologists speak of a "reflexive rationality" when a critical and adaptive attitude is adopted towards processes where security decisions are made [2, 14, 15]. This includes, for example, taking secondary effects into account at an early stage and anticipating side effects. When observing hybrid situations, the overarching question is *which decision-making logics shape the behavior of actors*, whether it is more a case of linear-planning or adaptive-learning. The focus here could be on aspects such as the use of scenario techniques, red teaming or situation centers with AI support. Different logics can also prevail at the same time, such as a deterrence logic on the one hand and dialogue on the other. Uncovering the coexistence of such sometimes contradictory logics and thus making areas of tension and conflicts of interest foreseeable, improves the analysis of situation progressions.

V. Advantages of an integrative analysis of hybrid Threat processes

In complex and diffuse situations such as hybrid threats, an ambiguity-tolerant approach is required. As we have tried to show, the third wave of security research can help to formulate such an understanding and provide researchers and practitioners involved with suitable questions. In this section, we once again emphasize the advantages of an integrative approach compared to the traditional objectivist approach of the first wave and the subjectivist approach of the second wave. This approach is "integrative" not least because it does not contradict the previous waves, but takes them up and processes them into a more dynamic understanding.

Objective components of threat assessment and crisis management can focus on identifying the various types of hybrid threats authorities may encounter. For example, this could include a combination of cyberattacks on navigation systems, disinformation campaigns aimed at confusing the public, and the use of irregular naval forces to conduct hostile activities, all of which complicate maritime security efforts. The subjectivist view increases sensitivity to how authorities generate and communicate information about hybrid threats, and how this information is perceived by the public and other stakeholders. For instance, maritime authorities may issue warnings about potential cyberattacks on port infrastructure, but public misunderstanding or distrust could lead to over- or underestimation of the threat. The integrative view takes a holistic approach, analyzing the entire process of hybrid threats. The threat is therefore not attributed to an isolated event, but rather takes a non-linear course over a longer period of time. This perspective is crucial as it considers how the different components of hybrid threats interact and evolve. For example, a combination of cyberattacks and disinformation about a naval operation might create a situation where maritime authorities struggle to distinguish between real and perceived threats, ultimately affecting the response and policy-making processes.

An integrative understanding enables researchers as well as practitioners to view hybrid threats as complex, interconnected phenomena. This facilitates a comprehensive assessment of the threat situation and a coordinated response to various threat elements. By understanding the interactions between different threats, authorities can recognize patterns that indicate an escalation of hybrid threats. This enables early identification and countermeasures before a threat develops further. An integrative approach promotes cooperation between different public or private institutions (such as operators of critical maritime infrastructures), as it focuses on the overall threat situation and its interactions and various interpretations. Authorities from different areas, such as the military, domestic policy and cyber security, can thus work together better and develop a coherent strategy despite having a fragmented perspective.

Understanding threats through the lens of the integrative concept means dealing with uncertainty and not-knowing rather than calculable risks, and allows to analyze hybrid threat events as dynamic processes with side effects rather than single events. At the same time, our classification in the theoretical figures of reflexive modernization also reveals expected elements that are inherent in the structure of the systems concerned. Ultimately, an integrative understanding expands our understanding of complex threats, emphasizes the importance of interdisciplinary cooperation, and raises awareness for the wide range of implications of security decisions.

VI. Conclusion and Further Research

Hybrid threats pose new challenges both for security organisations and for academic conceptualizaiton. In view of the ambiguity and diffuseness of (maritime) hybrid threat situations, it is difficult to ascertain the nature of possible hybrid threat events. With our contribution, we want to take the pressure off the responsible authorities and researchers to focus their analysis too quickly on objective recording. The radical openness of the process must be taken seriously – which, in turn, provides the advantage of being able to adapt flexibly to the further development of the threat situation. In our article, the integrative approach is proposed as a heuristic that enables a stepwise analysis. Further research should focus on exploring this approach in case studies that examine suspected cases of hybrid threats across time and space in more detail.

References

[1] M. Voss and D. F. Lorenz, "Sociological Foundations of Crisis Communication," in *The Handbook of International Crisis Communication Research*, A. Schwarz, M. W. Seeger and C. Auer, Eds., Hoboken, New Jersey, United States: Wiley Blackwell, 2016, pp. 45-55.

[2] W. Bonß, "Zwischen Normalisierung und Veränderung. Zur Zukunft der zivilen Sicherheitsforschung," in *Vielfältige Sicherheiten. Gesellschaftliche Dimensionen der Sicherheitsforschung*, N. Eschenbruch, S. Kaufmann and P. Zoche, Eds., Berlin, Germany: LIT, 2021, pp. 37-55.

DOI: 10.5281/zenodo.17120684

[3] E. Bajarūnas, “Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond,” *European View*, vol. 19, no. 1, pp. 62–70, March 2020, https://doi.org/10.1177/1781685820912041.

[4] J. Daniel and J. Eberle, “Speaking of hybrid warfare: Multiple narratives and differing expertise in the “hybrid warfare” debate in Czechia,” *Cooperation and Conflict*, vol. 56, no. 4, pp. 432–453, March 2021, https://doi.org/10.1177/00108367211000799.

[5] K. Armstrong and V. Sri-Pathma, “Finland investigates suspected sabotage of Baltic-connector gas pipeline,” *BBC News*, October 10, 2023. [Online], Available: https://www.bbc.com/news/world-europe-67070389. [Accessed March 10, 2025].

[6] M. Bryant, “We assume damage to Baltic Sea cables was sabotage, German minister says,” *The Guardian*, November 19, 2024. [Online], Available: https://www.theguardian.com/world/2024/nov/19/baltic-sea-cables-damage-sabotage-german-minister. [Accessed March 10, 2025].

[7] E. Lehto and A. Sytas, “Finland boards oil tanker suspected of causing internet, power cable outages,” *Reuters*, December 26, 2024. [Online], Available: https://www.reuters.com/world/europe/finland-police-investigate-role-foreign-ship-after-power-cable-outage-2024-12-26/. [Accessed March 10, 2025].

[8] “Finland Detains Suspected Sabotage Ship for Serious Maintenance Issues,” maritime-executive.com. https://maritime-executive.com/article/finland-detains-suspected-sabotage-ship-for-serious-maintenance-issues. [Accessed March 10, 2025].

[9] “Finland Releases Tanker but Detains Three Crew from December Cable Incident,” maritime-executive.com. https://maritime-executive.com/article/finland-releases-tanker-but-detains-three-crew-from-december-cable-incident. [Accessed March 10, 2025].

[10] “Suspected Sabotage Ship's Anchor Shows Signs of Extreme Damage,” maritime-executive.com. https://maritime-executive.com/article/suspected-sabotage-ship-s-anchor-shows-signs-of-extreme-damage. [Accessed March 10, 2025].

[11] G. Miller, R. Dyxon and I. Stanley-Becker “Accidents, not Russian sabotage, behind undersea cable damage, officials say,” The Washington Post, January 19, 2025. [Online], Available: https://www.washingtonpost.com/world/2025/01/19/russia-baltic-undersea-cables-accidents-sabotage/. [Accessed March 10, 2025].

[12] K. Kuuskoski, “Asiantuntija tyrmää uudet väitteet Itämeren kaapeli-vaurioista: ”Kyllä tämä on aika isoa peliä”,” Ilta Sanomat, January 29, 2025. [Online], Available: https://www.is.fi/kotimaa/art-2000010974584.html. [Accessed March 10, 2025].

[13] METIS, “Scenarios of Russian influence until 2030,” *Study No. 42 December 2024*. Available: https://metis.unibw.de/assets/pdf/metis-study42-2024_12-rus_eastflank.pdf. [Accessed June 10, 2025].

[14] U. Beck, *Risk Society: Towards a New Modernity*, SAGE, 1992.

[15] U. Beck, *World Risk Society*, Polity, 1999.

[16] F.H. Knight, *Risk Uncertainty, and Profit*, Boston MA; Hart, scheffer and Marx; Houghton Mifflin, 1921.

DOI: 10.5281/zenodo.17120684