# Assessing hybrid threats to critical infrastructure through morphological analysis and escalation phases

**Daniel Hofmann**
German Aerospace Center (DLR)
Institute for the Protection of Maritime Infrastructures
daniel.hofmann@dlr.de

**Jan Stockbrügger**
German Aerospace Center (DLR)
Institute for the Protection of Maritime Infrastructures
jan.stockbruegger@dlr.de

**Frank Sill Torres**
German Aerospace Center (DLR)
Institute for the Protection of Maritime Infrastructures
Frank.SillTorres@dlr.de

## ABSTRACT

Hybrid activities increasingly threaten critical maritime infrastructures, such as subsea data cables and pipelines. Operating below the threshold of open military conflict, they challenge traditional damage- and intensity-based approaches to threat assessment. Their strategic relevance often lies less in direct physical damage than in political impact, ambiguity, and gradual escalation dynamics. This paper develops an analytical framework combining morphological classification with a phase-based escalation model. The morphological analysis differentiates key dimensions such as strategic and operational intentions, target structures, means of action, and contextual factors including ambiguity and degree of control. Building on this, the phase model enables events to be categorized within a dynamic escalation process, distinguishing between cumulative and impact-driven escalation pathways. This approach provides a structured framework for assessing hybrid threats in the maritime domain and enables a differentiated interpretation of grey zone threat activities and escalation pathways.

### Keywords

Hybrid threats, Critical infrastructure protection, Risk analysis, Morphological analysis, Escalation dynamics

## INTRODUCTION

Russia's war of aggression against Ukraine has marked a turning point in European security policy. Systematic political and material support for Ukraine means that Europe's critical infrastructure is increasingly targeted by Russian hybrid warfare activities. For example, the International Centre for Counter-Terrorism reported 151 Russian hybrid attack incidents in Europe between February 2022 and February 2026 (Lanchès & Rekawek, 2026), while Germany registered over 300 sabotage incidents against its infrastructure in 2025 (Bewarder et al., 2026).

Maritime infrastructures such as ports, offshore wind farms, and subsea data and electricity cables have been at the center of the debate over hybrid threats due to their economic and military importance, especially after the September 2022 attack on the Nord Stream pipelines in the Baltic Sea. Offshore wind farms are vital sources of green energy, and ports facilitate global trade and commodity flows. The sea is also an important site for military

operations and logistics. For example, German and other European ports are central hubs and deployment areas for NATO units, and regional naval bases help secure NATO's North Sea and Baltic flanks. Germany and other countries are highly dependent on these systems, and infrastructure failures can have far-reaching economic, social, and security consequences, including cascading effects. (Bueger & Liebetrau, 2023).

Protecting maritime infrastructures is a major challenge. Logistics and supply chains are highly complex, port infrastructures are dispersed over large areas, and offshore facilities are located far from the coast, where they are exposed to attacks and sabotage. (Tecklenburg et al., 2025). In other words, maritime infrastructures are highly vulnerable targets (Bueger & Liebetrau, 2021).

Analysts therefore increasingly discuss hybrid attack and influence strategies against maritime infrastructures (Larsson, 2024). Hybrid warfare, also sometimes referred to as grey-zone warfare, is a form of strategic competition that deliberately operates below the threshold of open military conflict and that combines military, economic, informational, and civilian instruments (Morris et al., 2019). Hybrid threat activities are characterized by ambiguity, gradual escalation, and political influence, while at the same time avoiding escalation thresholds to reduce the risk of open military conflict (Mumford & Carlucci, 2023; Suchkov, 2021). Countries including China, Russia, and Iran often rely on non-state actors such as militia forces to ensure plausible deniability and distance themselves from hybrid attack activities. Iran, for example, has armed and supported militias in Yemen to attack Red Sea shipping (Haugstvedt, 2021; Levy et al., 2026), and China has deployed seaborne militias and fishing boats in its maritime disputes with regional states (McLaughlin, 2022). States also obscure attacks as unintentional accidents or criminal activities. Russian-affiliated tankers, for example, are suspected of having intentionally damaged subsea cables with their anchors (Ringbom & Lott, 2024).

The debate on hybrid warfare has advanced significantly in recent years. The concept is increasingly invoked in policy debates, and some scholars argue that it is overused, has lost analytical value, and has become a political tool to shape policy debates rather than helping analysts investigate new forms and strategies of conflict (Libiseller, 2023). Others, however, have tried to further develop the concept as an analytical toolkit. For example, conceptual work has focused on core elements of hybrid warfare, such as ambiguity (Mumford & Carlucci, 2023), or on developing the concept as part of broader escalation models to study international conflict (Person et al., 2024).

This paper develops an analytical instrument for defense and security analysts to evaluate hybrid threat scenarios and activities. It contributes to the debate on hybrid attacks from operational and tactical perspectives. The paper does not aim to provide a new perspective on what constitutes a hybrid attack or on how specific actors, such as Russia or Iran, have used hybrid attack strategies. Instead, the aim is to develop an analytical toolbox for security and defense analysts that enables them to better investigate and systematically evaluate hybrid attack activities, especially against maritime infrastructures, and to identify their specific conflict dynamics and escalation logics.

To do so, the authors develop two interconnected analytical models. The first model enables analysts to assess specific hybrid attack incidents and scenarios based on clearly defined analytical categories designed to capture the core elements of hybrid attacks, including the attacker's strategic and operational objectives, the tools and platforms used in an attack, the temporal structure of activities, and the level of ambiguity, among others. The second model then maps these categories to a phase model of conflict escalation, allowing analysts to place a hybrid threat activity into one of four phases of escalation, from low-scale to high-intensity warfare. Taken together, these models provide a comprehensive, integrated, and systematic evaluation of hybrid attack incidents and their escalation level, thereby helping analysts and policymakers decide how to respond to such activities.

The paper proceeds as follows. The next section provides an empirical overview of hybrid activities in Europe and highlights the need for structured analytical approaches. The subsequent section introduces the methodological framework, including the morphological analysis used to characterize hybrid activities. This is followed by a section presenting the phase model of hybrid conflict escalation and associated escalation pathways. The final sections present the results and discuss the findings, concluding with implications for future research and operationalisation.

## ANALYZING HYBRID ACTIVITIES IN EUROPE

The proliferation of hybrid incidents in recent years shows that these threats are not merely theoretical scenarios. They are already observable, security-relevant phenomena. In this section the authors discuss two analytical representations of hybrid threat activities to illustrate the need for more comprehensive analytical frameworks. The map of The Economist, 2025, based on data from the International Institute for Strategic Studies (Edwards & Seidenstein, 2025), includes suspected and documented hybrid activities from 2018 to 2025, both on land and at sea. Categorizing attacks based on the targeted infrastructures, they show that hybrid threat incidents are not limited to individual sectors, and that they affect a wide range of infrastructures. These include energy and communication infrastructures, undersea data cables, transport and logistics systems, industrial production sites and government facilities. The presentation aims to empirically contextualize these observable activities, providing insights about the prevalence, spatial distribution, and sectoral breadth of hybrid interference in Europe.

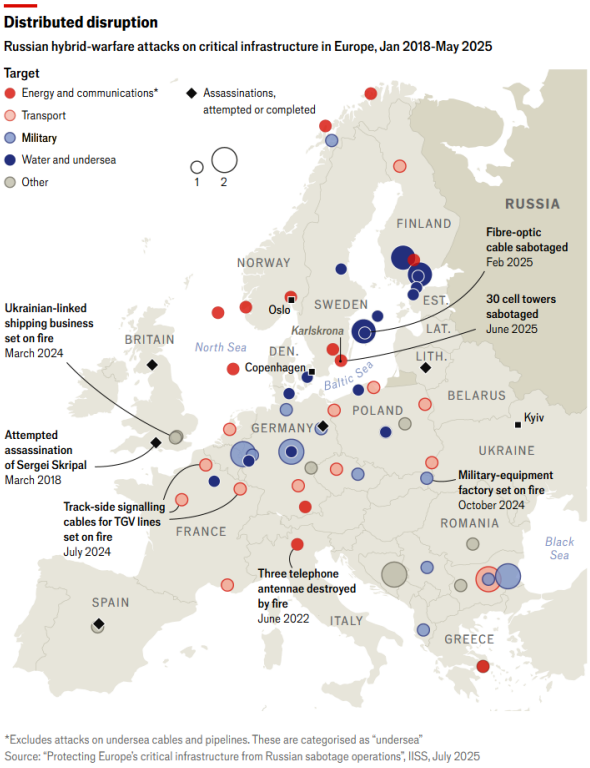


**Figure 1. Overview of documented hybrid activities in Europe (2018–2025).**

The Institute for the Study of War's (ISW) map, on the other hand, provides an event-based perspective on hybrid activities in Europe. The map presents documented individual events and their spatial distribution and accumulation within a limited period of time. Instead of organizing hybrid threat events based on targeted infrastructures and sectors, moreover, it organizes them according to specific activity types, such as airspace violations, espionage activities, maritime blockades, acts of sabotage, and other security-related incidents. These events are "phase zero operations", a heuristic indication of an escalation logic below open military strikes and war-like activities. Indeed, hybrid activities often remain below classic military escalation thresholds and are characterized by ambiguity, limited impact, and difficult attribution (Morris et al., 2019).

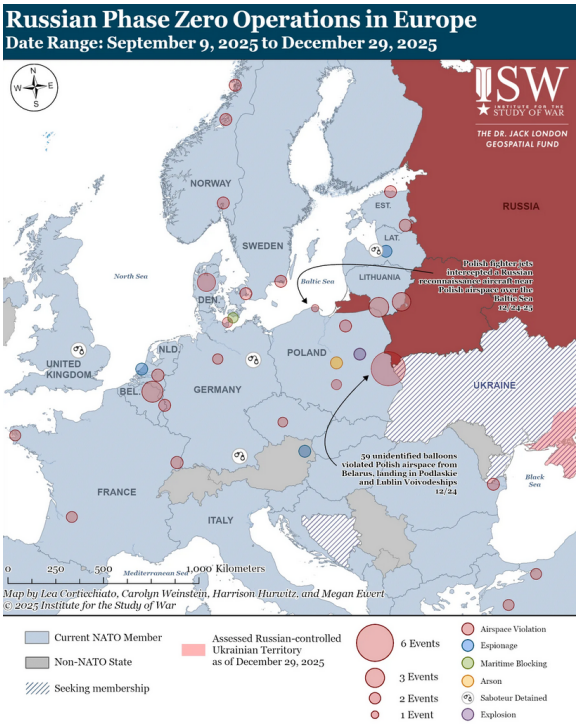


**Figure 2. ISW presentation of documented Phase 0 activities in Europe. (ISW, 2026)**

In short, the two analytical cartographic representations help empirically contextualize observable activities and illustrate recurring patterns in hybrid warfare based on the nature of events and infrastructure sector they target. However, they do not provide a detailed analytical framework for analysts to study hybrid attacks in terms of specific operational parameters that characterize such activities, including their operational and strategic goals or the level of ambiguity. Moreover, the two analytical maps do not classify the escalation level or the escalation trend of individual events and activities. The ISW map's categorization as "phase zero operations" implicitly signals an escalation logic, but it does not include a model of how that escalation could unfold, thereby lacking tools for analysts to identify such escalation logics. This underscores the need for an analytical framework that can systematically capture gradual transitions and consolidation processes within a specifically designed phase model for hybrid warfare, helping analysts to locate observable events in specific conflict phases and to illuminate transition zones between different escalation stages. This paper aims to develop such a model.

## METHODOLOGICAL FRAMEWORK

### Limits of classical models

Traditional security analysis methods are often primarily aimed at analyzing variation in physical damage or a linear increase in the intensity of violence. When analyzing hybrid activities, however, such an approach reaches its limits, as the strategic significance of these attacks often lies less in the direct physical damage that they produce than in the political impact they trigger. Hybrid scenarios are aimed at perception, decision-making processes and reaction patterns and deliberately operate in the area of ambiguity. Even attack or sabotage events with very limited physical impact can have considerable strategic effects, especially if they create uncertainty and influence public attitudes and political processes. The systematic categorization of hybrid attacks therefore requires an analytical approach that systematically distinguishes between purpose, means, context and political impact.

### Morphological analysis of hybrid events

The morphological analysis enables a structured description of hybrid scenarios without early evaluation or escalation assumptions. Complex scenarios are broken down into clearly defined categories of purpose (intention), action (operational implementation), means (effective means) and context (control, event character). This differentiation creates a systematic classification scheme that makes different events comparable, increasing transparency and revealing their structural attributes. Morphological analysis goes back to Fritz Zwicky and is used to systematically structure complex problem spaces (Zwicky, 1967). In its further development as General Morphological Analysis, it was operationalised in particular for processing complex, multidimensional policy problems (Ritchey, 2006).

The application of this approach offers several analytical advantages:

- Separation of incident description and evaluation: incidents can first be recorded and analyzed in a structured manner before political or escalation-related conclusions are drawn.
- Increased comparability: Different incidents can be analyzed and compared systematically using identical categories.
- Transparency of assumptions: Analytical categories and structures are clearly stated.
- Connectivity: The scheme enables the integration of further qualitative assessments, quantitative risk analyses and integration into escalation and phase models.
- Multidimensional perspective: Intentions, means and context are considered separately, allowing for the analysis of hybrid dynamics in a more differentiated way than in purely damage-oriented approaches.

The method thus serves to describe hybrid activities in a structured way. Building on existing morphological approaches, the schema is supplemented by escalation-relevant dimensions and embedded in a dynamic context. This creates an analytical grid that makes hybrid activities systematically recognizable along their strategic logic and conflict dynamics and forms the basis for the subsequent categorization into analytical dimensions and escalation phases.

Table 1 provides an initial overview of the extended morphological analysis framework used in this paper. It is based on seven categories that capture core dimensions of hybrid threat activities, including the strategic and operational intention of the attacker, the target, the means or instruments used in the attack, the level of ambiguity and a state's degree of control over the attack, and the temporal character of the attack. These categories enable a structured description of hybrid events and activities without evaluating their political significance. Next, we describe and analyze each of these categories in detail.

**Table 1. Analytical categories of the extended morphological analysis framework for hybrid attacks**

| Category | Description |
|---|---|
| Strategic goal | Overarching political goal of the activity |
| Operational goal | Direct technical or physical impact goal of the activity or operation |
| Target | Affected infrastructure, institution or function |
| Means of impact | Means or instruments used in the event or operation |
| Degree of control | Degree of state control or indirect influence over actors who carry out an operation |
| Temporal structure | Chronological and timing dimension of incidents or operation (singular, episodic, systematic) |
| Ambiguity | Degree of attribution and openness to interpretation |

In addition to these structural categories, ambiguity plays a central role in hybrid activities and is treated in this framework as a cross-cutting category that influences all other analytical dimensions.

Table 1 summarizes the core analytical categories of the morphological framework used to describe hybrid activities. While the individual categories draw on established concepts, their structured combination and integration into a coherent analytical framework represent the central contribution of this paper. In particular, the table highlights how different dimensions such as intention, means of impact, degree of control and ambiguity interact, enabling a systematic analysis of hybrid activities beyond isolated case descriptions. While the framework is organized into distinct analytical categories, the last category, ambiguity, differs from the others in that it operates across the framework and influences how the remaining categories are interpreted.

The categories developed in Table 1 are interrelated, as will be outlined further below. For example, operational goals follow from strategic goals and lead to the selection of specific targets, means of impact, a certain degree of state control, and temporal structure of hybrid threat activities. This cross-cutting role of ambiguity will be elaborated in more detail in a dedicated section below. Figure 3 further illustrates how these categories interact, with ambiguity shaping their interpretation across different analytical dimensions.

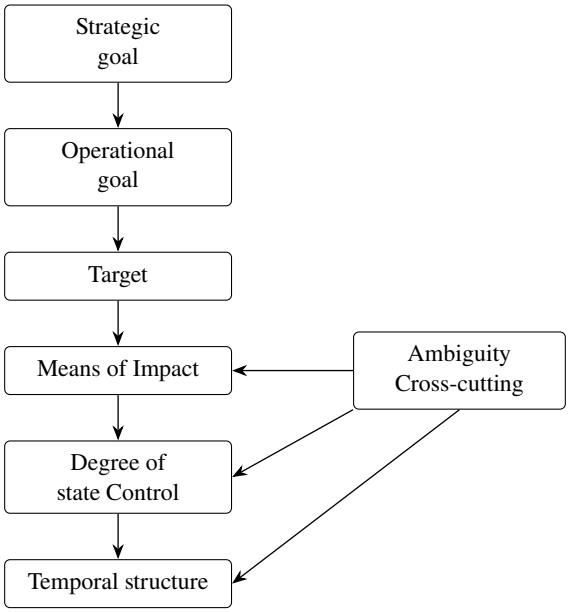


**Figure 3. Model overview: category structure and cross-cutting assessment through ambiguity.**

### Category 1: Strategic goal

Analyzing goals and intention in the context of hybrid scenarios requires differentiated considerations. As a rule, actors in hybrid competitions pursue strategic goals, and the specific action at the operational level represents the means of realizing these goals. The strategic goal thus describes an actor's central motive or objectives when planning and carrying out a hybrid activity. In order to realize this goal, an operational action is required, which manifests itself in physical, technical or information measures. This distinction between these two levels, strategic and operational, is analytically significant, as identical operational actions can serve different strategic objectives.

The category "strategic intention" thus describes the broader political or military objectives that an actor is pursuing with a hybrid activity. Based on the literature, one can identify five distinct strategic objectives. "Testing", for example, refers to operations aimed primarily at triggering a response from the defender with the aim of studying it to collect information about an actor's operations behavior and thresholds. "Signaling", moreover, refers to operations aimed at demonstrating the attacker's presence or specific infrastructure vulnerabilities, while "deterrence" describes operations aimed at showing an adversary the potential costs of its actions. Table 2 provides an overview of the different strategic goals in hybrid attack operations.

**Table 2. Strategic goals in hybrid operations**

| Strategic goals | Description |
|---|---|
| Intelligence gathering | Systematic collection of information on targets, processes, vulnerabilities and response patterns |
| Testing | Collecting information about incident response behavior for future operations |
| Signaling | Demonstrating presence, reach or vulnerability |
| Destabilization | Undermining trust, stability or decision-making processes |
| Deterrence | Highlighting the costs or risks of future action |
| Escalation | Deliberately intensifying confrontation |

### Category 2: Operational goals

This category describes the immediate objective of a specific hybrid threat activity or operation. It focuses on the event-related technical or physical objectives of an operation and connects the strategic perspective with the tactical-operational level. For example, "reconnaissance" operations are mainly aimed at intelligence gathering and gaining access to information. At the strategic level, "reconnaissance" operations contribute to the strategic goal of "testing" or "intelligence gathering". They are different from "sabotage" operations, which are aimed at interfering in a critical system, or "disruption" operations, which are designed to produce a temporary impairment of a such a system. These two operational goals often contribute to the strategic goals of "signaling," "destabilization" and "deterrence", while the strategic goal of "destruction" operations is often conflict "escalation". Operations aimed at "manipulation", that is the covert influencing of data, sensor technology or perceptions without producing direct physical damage, are often strategically aimed at "destabilizing" an adversary by undermining trust in its institutions and capabilities.

**Table 3. Operational goals in hybrid operations**

| Operational goal | Description |
|---|---|
| Reconnaissance | Access to information and intelligence without direct physical effect |
| Manipulation | Covert influencing of data, sensor technology or perception without direct physical damage |
| Disruption | Temporary impairment of functions or processes |
| Damage | Physical or technical damage with limited system impact |
| Sabotage | Targeted interference and functional impairment of critical systems |
| Destruction | Major physical or technical damage |

### Category 3: Target

The category "target" describes the affected object, system or infrastructure that is the focus of a hybrid threat activity. The type of object or infrastructure targeted in a hybrid activity can provide insights into the attacker's strategic intentions or priorities and enable a comparative categorization of different events and activities. In this paper, we divide targets into four functional infrastructure categories: Energy (e.g., offshore wind farms), information and sensor systems (e.g., subsea data cables and maritime sensors such as radar systems), maritime transportation (e.g., ports), and military-related infrastructure (e.g., naval bases and fuel and ammunition storage).

**Table 4. Target categories of maritime critical infrastructures in the morphological analysis approach**

| Target category | Goal | Description |
|---|---|---|
| Energy infrastructure | Offshore wind turbines | Individual components with local system impact |
| | Converter platform | Central energy conversion facility with high system relevance |
| | Offshore substation | Central energy distribution facility with high system relevance |
| | Power cable | Linear energy connection with grid node function |
| | Energy cluster | Spatially concentrated energy infrastructure |
| | Offshore industrial platform (oil/gas) | Offshore facility for energy production with systemic supply function |
| | Offshore hydrogen-infrastructure | Offshore facilities for the production, processing or connection of hydrogen |
| | Offshore pipeline | Subsea pipeline for energy or material transport with high supply relevance |
| Information and sensor systems | Data cable | Linear data connection with communication function |
| | Monitoring systems (radar, cameras, weather) | Sensor-based IT/OT infrastructure |
| | Maritime navigation-infrastructure (AIS, GNSS etc.) | Technical systems for traffic management and positioning in the maritime domain |
| Maritime transport-infrastructure | Port basins/access channels | Maritime access infrastructure |
| | Locks/canals | Critical waterway connection |
| | Cargo handling facilities | Key logistical infrastructure |
| | Logistics storage areas (containers/raw materials) | Port-adjacent storage and buffer infrastructure for goods and strategic materials |
| Military-relevant infrastructure | Fuel & ammunition storage | System-critical supply infrastructure |
| | NATO-relevant terminals | Militarily relevant logistics infrastructure |
| | Naval base | Military base infrastructure |

The target infrastructure and system categories also include an analytical description of infrastructure subsystems and components in terms of how important they are for the functioning of an infrastructure. For example, an attack on an offshore wind farm could target a wind turbine or a subsea electricity cable. These subsystems vary in terms of their systemic relevance and leverage effect. While isolated components primarily generate local effects, network-relevant connections, central nodes or spatially concentrated infrastructures have the potential for supra-regional or systemic effects. The loss of a wind turbine does not have a very large effect on the functioning of an offshore wind farm, but destroying its central electricity converter station does. Identifying the specific subcomponent of an infrastructure that is targeted in an attack is therefore important to assess the attacker's strategic and operation objectives as well as subsequent escalation levels. Table 4 summarizes the targeted infrastructures and their subsystem components and effects.

### Category 4: Means of impact

The means of impact describe the operational instruments, systems, or tools used in a hybrid threat activity at the operational implementation level. Individual means of action do not develop their effect in isolation, but in combination with other means or in interaction with structural vulnerabilities. For example, a maritime hybrid attack could involve a gun and an explosive device to destroy an offshore wind turbine. Technical systems also sometimes act as carrier systems for other means of action, for example when a drone is launched from a vessel. The type of means used in a hybrid threat activity allows for conclusions to be drawn about the level of capability. An attack involving an unmanned underwater vehicle indicates a high level of capability, while attacks with small arms indicate a much lower capability.

### Category 5: Degree of state control

States do not act openly in hybrid threat activities. Instead, they rely on proxies and influence or control the actions of other actors to stage hybrid attack activities. The degree of a state's influence or control over another actor conducting hybrid attacks represents a central analytical dimension, as it significantly influences the political attributability and thus the ambiguity of an event. The more (visible) control a state has over a hybrid threat actor, the less it can claim "plausible deniability" and distance itself from its activities. The degree of state control is divided into several types (see Table 5).

**Table 5. Classification of degrees of state control in hybrid activities**

| Degree of state control | Description |
|---|---|
| Directly state-led | Action is openly carried out by state actors |
| State-controlled | Civilian or non-state actors directed and supported by a state |
| State tolerated | Non-state actors act independently, but the state tacitly supports their activities |
| Autonomous | No recognizable state control or approval |

The characteristics shown in table 5 differ in particular in terms of their political attributability and their potential for escalation. Direct state actions are planned, ordered or executed directly by state actors. This results in high attributability, low ambiguity and potentially rapid political escalation. In state-controlled operations, states coordinate and support the activities of civilian or non-state actors. This can also take the form of technology or knowledge transfer or the sharing of intelligence for specific operations. For the state actor, operating through non-state actors minimizes their political exposure, enhances plausible deniability, and limits the risk of escalation. This form of ambiguity is a key part of hybrid grey zone activities. In the case of actions tolerated by the state, the state does not actively support the operations of a hybrid threat actor, even though it provides some support for its other activities and does not intervene to prevent its hybrid threat activities. Attribution is much more difficult in such cases, meaning that the state can claim "plausible deniability". Ambiguity thus remains high, and political reactions and security responses are often restrained, minimizing the risk of escalation. Autonomous or criminal acts take place without recognizable state control or approval. In these cases, the strategic and even operational importance of an operation is usually limited, even though a state actor might benefit from such operations indirectly.

### Category 6: Temporal structure

The temporal structure describes the chronological dynamic and dimension of events and their influence on political perception and reaction patterns. Table 6 provides an initial overview of how events can be categorized accordingly.

**Table 6. Chronological classification of events**

| Event character | Description |
|---|---|
| Singular | One-off, isolated event without recognizable pattern |
| Episodic | several similar and potentially interrelated events over a limited period of time |
| Systematic | Repeated events with a clearly recognizable logic and pattern |

Singular events occur only once and are not part of a specific pattern. They are therefore often interpreted as an accident or isolated incident and generally do not lead to major escalation, provided there is no exceptionally high

damage or symbolic effect. Such incidents are usually politically manageable for actors and their adversaries. Episodic events, on the other hand, refer to a situation when several similar events occur within a limited period of time, suggesting a pattern of activities that receives media and public attention. As a result, political pressure to act and respond to such incidents increases, including efforts to strategically reassess the situation. Systematic events, finally, are repeated and structurally similar events or patterns of events with a clearly recognizable logic and objective. This leads to strong political pressure and necessitates a strategic reassessment, potentially leading to a major response to punish and deter the adversary responsible for these operations. Thus, systematic events increase the risk and likelihood of conflict escalation.

### Ambiguity as a cross-cutting category

Unlike the preceding categories, ambiguity is not treated as a separate descriptive element alone, but as a cross-cutting analytical dimension that shapes the interpretation of all other categories. Ambiguity describes the extent to which multiple plausible explanations exist for a hybrid threat event and how difficult it is to attribute responsibility to a specific actor. In hybrid conflict scenarios, ambiguity is not merely a by-product but often a deliberately created condition used to shape political perception and decision-making. As a cross-cutting analytical dimension, ambiguity affects all other categories of the morphological framework. It shapes the interpretation of strategic and operational intentions, influences the assessment of means and capabilities, and determines the degree to which events can be politically attributed. Two ideal-typical forms of ambiguity can be distinguished:

High ambiguity:

- Difficult attribution
- Internal disagreement among decision-makers
- Delayed political reactions
- Reduced pressure for immediate response

Low ambiguity:

- Clear attribution
- Rapid political categorization
- Increased pressure to act
- Limited scope for de-escalation

Ambiguity therefore does not primarily determine the physical impact of an event, but rather the political room for manoeuvre of affected actors. It can act both as an amplifier and as a dampener of escalation dynamics and plays a central role in transitions between escalation phases. The degree of ambiguity is closely linked to the attribution of actions to specific actors. The means used and the level of capability are important indicators for assessing the origin of an attacker and thus the degree of ambiguity. The categorization of ambiguity is based on the attributability of the means used and the extent to which the origin and responsibility of an actor can be clearly traced and demonstrated technically, operationally and politically under realistic conditions. To operationalise ambiguity within the model, a qualitative scale is introduced capturing the degree of attributable responsibility for a hybrid threat activity:

- **Very high**: Multiple plausible explanations exist, and there is very limited evidence for clear attribution.
- **High**: Attribution is difficult but in principle possible based on available evidence.
- **Medium**: Attribution remains uncertain, but technical, operational or political indicators provide partial evidence.
- **Low**: Responsibility can be attributed with a high degree of confidence and minimal interpretative uncertainty.

The variation in attribution levels reflects differences in the traceability of actions, the complexity of the means used, and the availability of evidence linking an event to a specific actor. Table 7 provides an overview of how different types of means and operational approaches relate to varying levels of ambiguity. The classification is based on the extent to which actions can be attributed to a specific actor under realistic conditions.

**Table 7. Operational tools of hybrid maritime activities with ambiguity assessment**

| System | Description | Ambiguity |
|---|---|---|
| Large civilian vessel | Cargo ships, tankers, ferries | High |
| Service/support vessel | Maintenance, offshore, port service providers | High |
| Government research vessel | Formally civilian, state-affiliated background | Medium |
| Small civilian craft | Sailing boats, yachts, recreational boats, fishing vessels | Very high |
| Unmanned surface vehicles (USV) | Unmanned or remotely controlled surface vehicles | High |
| Unmanned underwater vehicles (UUV) | Autonomous or remotely operated systems | High |
| Unmanned aerial vehicles (UAV) | Remotely piloted or autonomous aerial platforms | High |
| Divers/combat swimmers | Manual intervention, placement of devices | High |
| Cyberattacks | IT/OT systems, control systems, networks | High |
| Navigation and radio signal disruption/ -manipulation | GPS jamming/spoofing, AIS manipulation | Very high |
| Insider/logistics processes | Internal actors, manipulated processes or supply chains | High |
| Explosives/kinetic means | Open physical violence | Low |

### Using the model to evaluate a hypothetical hybrid threat event

Next, we briefly illustrate our model using a hypothetical case. A civilian vessel (e.g. general cargo vessel, tanker or research vessel) repeatedly moves in the immediate vicinity of offshore wind turbines or converter platforms. The approach takes place without any recognizable technical emergency. The scenario can be categorized as follows using the categorization scheme described above:

**Table 8. Scenario example**

| Category | Assignment |
|---|---|
| Strategic intention | Testing/signalling, showing presence |
| Operational intention | Intimidation, reconnaissance, demonstration of access proximity |
| Target | Critical energy infrastructure |
| Means of impact | Civilian ship |
| Ambiguity | Very high |
| Degree of control | Currently not assignable |
| Temporal structure | Initially singular, transition to episodic upon repetition |

The expected physical impact of such operations is very small or non-existent, as the ship does not damage the infrastructure. Strategically, the incident primarily produces political signaling effects, in particular through media coverage and increased political attention. If such incidents are repeated, leading to a discernible pattern, pressure to reassess the situation and respond more forcefully grows - even if there is no physical damage. The example shows how even low-intensity incidents can increase the risk of conflict escalation.

## PHASE MODEL OF HYBRID CONFLICT ESCALATION

The phase model operationalises the analytical categories introduced in the morphological framework by describing how their configurations change over time, leading to specific phases within a conflict. Rather than representing a simple increase in intensity, escalation is understood as a transformation of key dimensions such as ambiguity, degree of control and event character. Accordingly, each phase reflects a characteristic configuration of these analytical categories, allowing escalation processes to be interpreted as structured shifts rather than isolated developments. Escalation of hybrid activities does not necessarily follow a linear increase in intensity or violence. Instead, hybrid conflicts can evolve along different escalation paths depending on how political pressure is generated and perceived.

Hybrid activities rarely escalate abruptly but typically evolve within an existing strategic context. Their aim is to gradually realize political intentions and, if necessary, to bring about a controlled escalation. Escalation often unfolds over extended periods and is not triggered by a single event, but by a sequence of actions. As a result, individual events may appear limited in isolation, while their political impact emerges through the interaction of multiple incidents. This understanding of escalation as an ongoing competitive process also corresponds to Germany's National Security Strategy, which increasingly describes the security policy environment as a permanent systemic competition with hybrid forms of influence (Auswertiges Amt, 2023).

Traditional escalation models often do not adequately capture such gradual developments, as they primarily focus on clearly identifiable thresholds or singular events. More recent approaches instead conceptualize escalation as a dynamic and competitive process unfolding through a sequence of analytically distinct states (Radin, 2024; Douglass et al., 2024). When analyzing hybrid threat activities, it is therefore necessary to systematically differentiate between states of escalation and to structure transitions between them. In particular, activities below the threshold of open military conflict require distinct analytical categories in order to capture gradual changes in conflict dynamics.

The phase model enables the systematic description of escalation states and the categorization of hybrid activities according to their level of escalation. This allows for comparing events, identifying potential correlations, and assessing escalation dynamics in a structured manner. The identification of thresholds and transitions, combined with consistent event categorization, supports strategic assessment and enhances the situational picture.

The model treats escalation as a process rather than a single event. The individual phases are analytical constructs that enable events to be categorized in a structured and systematic way. Transitions between phases are fluid and reflect the cumulative political impact of events rather than abrupt changes. However, escalation does not necessarily follow these phases in a linear manner. Hybrid conflicts may skip phases, move directly between non-adjacent phases, or even de-escalate. The phase model is therefore not intended as a deterministic sequence, but as an analytical tool to support the identification of escalation states and transitions. Table 9 provides an overview of the escalation phases and their underlying political logic. A more detailed description of each phase is provided in the following section.

**Table 9. Phase model of hybrid conflict escalation**

| Phase | Description | Ambiguity | Political Logic |
|---|---|---|---|
| Phase 0 | Preparation/grey zone | Very high | Testing, shaping, normalization |
| Phase 1 | Active hybrid confrontation | Medium | Pressure, patterns, political debate over response |
| Phase 2 | Open military force | Low | Decision, reaction, deterrence |
| Phase 3 | High-intensity war/systemic conflict | None | Resolution, survival, reorganization |

The phases reflect systematic shifts in key analytical dimensions, particularly decreasing ambiguity, increasing visibility of actors, and the transition from isolated to systematic events.

The phase model builds on the hybrid incident analysis model introduced earlier. Different combinations of analytical values for each of the categories in that model lead to different escalation phases. Phase 0 is typically characterized by high ambiguity, low visibility of actors and predominantly singular or weakly structured events. In contrast, Phase 1 emerges when repeated incidents form recognizable patterns, ambiguity decreases and political pressure increases. Phase 2 is associated with low ambiguity, clearly attributable actors and the use of conventional military means, while Phase 3 reflects fully systemic conflict conditions with minimal ambiguity and sustained, large-scale operations. The phase model builds directly on the analytical categories introduced in the morphological framework. Each phase can be understood as a characteristic configuration of these categories, particularly with regard to ambiguity, degree of control and event character.

**Table 10. Comparison of the phases of hybrid conflict escalation**

| Aspect | Phase 0 - Preparation | Phase 1 - Active hybrid confrontation | Phase 2 - Open military confrontation | Phase 3 - High-intensity war |
|---|---|---|---|---|
| Character | Grey zone below the threshold of war | Hybrid confrontation with pattern formation | Limited, open military conflict | Unlimited and systemic conflict |
| Ambiguity | Very high | Medium (decreasing) | Low | Very low / strategically irrelevant |
| Temporal structure | Isolated | Episodic/ systematic | Continuous/ operational | Systemic persistent |
| Typical means | Sabotage, cyber, intelligence, civilian means | Coordinated hybrid means, proxies | Conventional armed forces | Whole-of-state warfare |
| Objective | Testing, shaping, normalizing | Generating political pressure | Forcing decisions | Enforcement of strategic objectives |
| Political effects | Delay of decision-making | Pressure for positioning | Clear response logic | Existential alliance logic |
| Escalation logic | Avoidance of clear thresholds | Calculated risk | Deterrence and counterreaction | Largely uncontrollable escalation dynamics |

The different phases reflect systematic shifts in key analytical dimensions, particularly ambiguity, degree of control and event character. Progression across phases is therefore not defined by isolated incidents, but by changes in the configuration of these categories. These shifts become visible through decreasing ambiguity, increasing visibility and attribution of actors, and a transition from isolated to structured and repeated events.

*Phase 0: Preparing & Testing response behavior*

Phase 0 is the first escalation phase. It represents an early configuration of the analytical categories introduced in the morphological framework, characterized by high ambiguity, low political pressure, and limited attribution. Hybrid activities remain below the threshold of open conflict and are typically perceived as isolated or ambiguous events. The high degree of ambiguity reduces immediate pressure to respond to the threat and allows political actors to delay categorization and counter-measures. Rather than triggering escalation, activities in this phase primarily aim at shaping political and strategic conditions while testing reaction thresholds.

**Table 11. Phase 0 - Preparation and strategic shaping**

| Category | Description |
|---|---|
| Core features | Persistent, low-intensity activities<br>The conflict remains below the threshold of open military violence<br>Intention to escalate remains unclear<br>The focus lies on shaping political conditions rather than specific decisions<br>Objective: shaping political and strategic conditions while simultaneously avoiding open escalation |
| Typical means | Sabotage with limited physical impact on infrastructure<br>(e.g., cables, energy systems, logistics)<br>Cyber operations below escalation thresholds<br>Intelligence gathering<br>Demonstration of presence<br>Influence activities, information and disinformation campaigns<br>Legal/economic leverage<br>Airspace, maritime, and border provocations |
| Typical characteristics | Very high level of ambiguity<br>Plausible alternative explanations (accident, coincidence, criminal activity)<br>Civilian or covert means and operations dominate<br>No clear red lines<br>Politically difficult to address |
| Political effects | Testing reaction thresholds<br>Observation of political, legal, and military responses<br>Normalization of incidents<br>Gradual erosion of decision-making processes<br>Avoidance of clear escalation thresholds |
| Examples | Suspected sabotage or disruptions of maritime infrastructure<br>GPS spoofing incidents<br>Unexplained technical failures. |

In terms of the morphological framework, this phase is defined by high ambiguity and predominantly singular or weakly connected low-intensity events. These characteristics limit clear attribution and reduce the likelihood of conflict escalation, while enabling actors to shape the strategic environment over time. The table illustrates how this configuration creates a situation in which hybrid activities can be systematically conducted without triggering strong political or military responses. In particular, the combination of high political ambiguity and low operational visibility (e.g., the availability of alternative explanations for an incident) allows actors to test reaction thresholds and observe responses without committing to military and political escalation. This highlights that escalation in hybrid conflicts does not necessarily depend on the intensity of single events, but on how the targeted country interprets and processes incidents politically and over time.

*Phase 1: Active hybrid conflict*

In Phase 1, escalation is no longer driven by isolated incidents but by the accumulation and repetition of hybrid activities. Escalation thus emerges from pattern formation rather than from the intensity or impact of individual events. A transition from Phase 0 to Phase 1 is particularly likely when recurring, targeted activities develop into recognizable patterns. As a result, political pressure to respond to these activities increases significantly. Ambiguity remains a defining feature in this phase but starts to decrease as patterns across events become more visible and difficult to dismiss as isolated incidents. At the same time, repetition and coordination increase the visibility of actors and indicate a shift in the temporal structure of escalation. Examples of this phase can be observed in repeated incidents targeting energy infrastructure, logistics hubs, or maritime routes, where individually limited events accumulate into recognizable patterns and generate increasing political and public pressure for response.

**Table 12. Phase 1 - Active hybrid conflict and pattern formation**

| Category | Description |
|---|---|
| Core features | Increasing frequency & target orientation<br>Transition from isolated incidents to recognizable patterns<br>Ambiguity persists but decreases through pattern formation and recurring signals<br>The conflict remains below the threshold of open military conflict<br>Political pressure to respond to incidents increases |
| Typical characteristics | Recognizable incident repetition and pattern formation (episodic to systematic)<br>More sensitive targets<br>Clearer signaling<br>Intensifying public political debate about the need to respond (countermeasures and deterrence) |
| Typical means | Coordinated acts of sabotage<br>Combination of physical, digital, and informational operations<br>Increased use of proxies and civilian platforms<br>military- and defense-related infrastructure targeted<br>Simultaneous events across multiple domains |
| Political effects | Pressure to take a position<br>Strain on alliance solidarity<br>Triggering alliance defense consultations (e.g. NATO article 4)<br>Increasing expectations regarding deterrence and protective measures<br>Reduced de-escalation space |
| Examples | Repeated incidents at energy or logistics hubs<br>Systematic disruptions in border regions<br>Simultaneous physical and digital attacks |

In terms of the morphological framework, this phase is characterized by a gradual reduction in ambiguity, a transition from singular to sequential or patterned incidents, and an adversary's increasingly visible involvement in these threat incidents. The table illustrates how repetition and coordination of hybrid activities create a shift from isolated interpretation towards pattern-based assessment. As patterns become recognizable and ambiguity is increasingly difficult to sustain, leading to growing political pressure to respond to the incident. This highlights that escalation in hybrid contexts can emerge without a single triggering event, but instead through the cumulative political interpretation of repeated activities over time.

### *Phase 2: Open military confrontations*

Phase 2 marks the transition from hybrid confrontation to openly attributable military action. Escalation is no longer primarily driven by ambiguity or pattern formation, but by the clearly identifiable and attributable use of force. This transition occurs when recurring hybrid and covert activities evolve into overtly coercive military measures, leading to a further reduction of political and operational ambiguity. As a result, ambiguity no longer serves as a stabilising element, and decision-makers are increasingly forced to respond to these incidents. Unlike Phase 1, where responses can still be delayed, Phase 2 is characterized by the necessity of political and military reaction. The crossing of the hybrid threshold therefore represents a qualitative shift in escalation dynamics rather than a mere increase in intensity. This phase can be illustrated by the rapidly decreasing use of plausible deniability as a political tool, leading to open yet still sporadic military actions that can be clearly attributed to an adversary, such as cross-border strikes, naval engagements, or the deployment of regular armed forces against critical infrastructure, where ambiguity is significantly reduced and actors often take responsibility for military strikes.

**Table 13. Phase 2 - Open military confrontations and crossing of the hybrid conflict threshold**

| Category | Description |
|---|---|
| Core features | Transition from hybrid to open military violence |
| | The grey zone is largely left behind |
| | Escalation occurs qualitatively through open attribution rather than merely through increased intensity. |
| | The conflict remains limited to specific areas or domains |
| Typical characteristics | Low ambiguity |
| | Clearly identifiable state or military actors |
| | Deployment of regular armed forces |
| | Public political attribution |
| | Military situational awareness dominates analysis |
| Typical means | Conventional military operations |
| | Air, maritime, or land attacks |
| | Blockades and exclusion zones |
| | Attacks on military infrastructure |
| | Use of armed drones |
| | Electronic warfare as a supporting measure |
| Political effects | Pressure on countries to clarify their position in the conflict |
| | Activation of collective security mechanisms (e.g. NATO article 5) |
| | Escalation management replaces ambiguity management |
| | Public expectations for response increase significantly |
| Examples | Cross-border military attacks |
| | Open naval and aerial engagements |
| | Military blockades or enforcement operations |
| | Open attacks on a state's military targets |

In terms of the morphological framework, this phase is defined by low ambiguity, high visibility of responsible state actors, and clearly attributable actions. Events are no longer perceived as isolated or pattern-based, but as deliberate and openly conducted military operations. The table illustrates how this configuration fundamentally changes the interpretation of events. The reduction of ambiguity and the clear attribution of actions eliminate the possibility of delayed or ambiguous responses, thereby forcing immediate political and military decision-making to counter the threat. While limited ambiguity may still persist in specific issues such as intent or the involvement of proxies, it no longer plays a central strategic role in shaping escalation dynamics.

*Phase 3: High-intensity war and systemic conflict*

Phase 3 is the highest escalation level, in which conflict evolves into a systemic and high-intensity confrontation across military, economic, political, and societal domains. This phase typically emerges when military operations initiated in Phase 2 expand significantly in scope, intensity, and strategic objectives, transforming a limited military conflict into a broader and sustained war. Unlike previous phases, escalation is no longer characterized by ambiguity, pattern formation, or threshold management. Instead, it is dominated by large-scale and open warfare and military mobilization. Examples of this phase include large-scale military conflicts in which sustained operations across multiple domains occur, such as combined maritime, air, and land campaigns, often accompanied by economic sanctions and information warfare, leading to systemic impacts on international security structures.

**Table 14. Phase 3 - Systemic conflict escalation**

| Category | Description |
|---|---|
| Characteristic features | Extensive escalation of the conflict |
| | The conflict becomes existential or systemic |
| | The conflict no longer exhibits a primarily hybrid character, |
| | as the open use of military force becomes the dominant form of conflict. |
| | Military, economic, and societal domains are involved |
| Typical characteristics | Ambiguity largely loses its strategic relevance |
| | Open and clearly recognisable wartime conditions |
| | Whole-of-government mobilisation |
| | Military logic increasingly dominates political processes |
| | The international order is significantly affected |
| Typical means | Large-scale military operations |
| | Combined arms formations |
| | Strategic air and maritime strikes |
| | Destruction of critical infrastructure |
| | Comprehensive economic coercive measures and sanctions regimes |
| | Information warfare across all levels |
| Political effects | Security architecture comes under pressure |
| | Alliances are tested existentially |
| | Domestic political mobilisation |
| | Long-term geopolitical reordering |
| | Diplomacy primarily serves to limit war expansion |
| Examples | Large-scale military invasions |
| | Multi-front wars |
| | Open alliance conflicts |
| | Systemic large-scale wars |

In terms of the morphological framework, this phase is defined by very low ambiguity, clearly identifiable actors, and sustained, system-wide conflict dynamics across multiple domains. The table illustrates how escalation culminates in a configuration where ambiguity is no longer a relevant factor, and where political and military responses are driven by clearly attributable actions and strategic necessity rather than interpretation. This phase highlights that hybrid escalation can ultimately transition into a systemic conflict environment, in which escalation dynamics are no longer governed by ambiguity or gradual pressure accumulation, but by open conflict and large-scale strategic competition.

### Two escalation pathways

Escalation of hybrid activities does not necessarily occur through a linear progression and an increase in the intensity or violence and the level of destruction. Instead, hybrid conflicts can escalate in different ways: through the proliferation of hybrid threats and activities over a longer period of time, through the extraordinary effect of a single incident, or through a combination of both. Against this background, two analytically distinguishable escalation pathways are described, which explain different transition logics between escalation phases.

*Escalation through effect*

**Table 15. Characteristics of escalation through effect**

| Category | Description |
|---|---|
| Character | Temporally singular or abrupt event with disruptive political impact |
| | Politically immediately highly consequential |
| | De-escalation space strongly constrained |
| Typical triggers | High casualty numbers |
| | Massive material damage |
| | Central symbolic targets |
| | Violation of fundamental security or sovereignty norms |
| | Exceptionally strong media and political attention |
| Political effects | Immediate pressure to respond to threat |
| | Accelerated decision-making processes |
| | Public expectation of strong response |
| | Ambiguity management is replaced by escalation management |

Such escalation is typically triggered by events that fundamentally alter political perception, forcing immediate interpretation and response. The abrupt nature of these incidents reduces the relevance of prior ambiguity and accelerates escalation dynamics, often leading to rapid shifts between escalation phases.

*Escalation through repetition*

**Table 16. Characteristics of escalation through repetition**

| Category | Description |
|---|---|
| Character | Temporally cumulative and sequential |
| | Individual events are limited in impact when considered in isolation |
| | Political effects emerge through pattern formation |
| | De-escalation space gradually decreases through cumulative effects |
| Typical triggers | Repeated incidents targeting comparable objectives |
| | Increasing frequency of hybrid activities |
| | Recognizable target orientation across multiple events |
| | Combination of multiple hybrid instruments over time |
| | Growing public and political attention |
| Political effects | Transition from assessment of single incidents to incident patterns |
| | Gradually increasing pressure to respond to threat |
| | Strain on decision-making and coordination processes |
| | Increasing expectations for countermeasures |
| | Preparation of alliance defense consultations (e.g. NATO article 4) |

In contrast to escalation by effect, the escalation pressure here arises primarily from the cumulative effect of repeated, individually limited events. The escalation path through repetition describes a dynamic mechanism by which hybrid activities can gradually escalate towards phase 1 and expands the phase model to include an explicitly procedural escalation perspective.

**Table 17. Comparison of the escalation paths of hybrid activities**

| Dimension | Escalation through effect | Escalation through repetition |
|---|---|---|
| Core logic | Shock-based escalation | Cumulative escalation |
| Temporal structure | Discontinuous | Sequential and cumulative |
| Typical triggers | High casualties, symbolic targets, norm violations | Repeated incidents against similar or strategically relevant targets |
| Political dynamics | Immediate pressure to respond | Gradually increasing pressure to respond |
| Role of ambiguity | Decreases rapidly due to attack sophistication and impact | Decreases gradually due to pattern formation |
| De-escalation space | Rapidly constrained | Gradually constrained |
| Escalation phases | Can skip escalation phases | Often leads to escalation phase 1 |

Table 17 summarizes the two escalation logics identified in this paper. The comparison illustrates that escalation does not necessarily follow a linear increase in intensity, but can emerge either through sudden high-impact events or through the gradual accumulation of smaller incidents. While both logics are grounded in existing research, their systematic distinction and analytical comparison represent a key contribution of this paper.This distinction is particularly relevant for analyzing hybrid threats, as it highlights different mechanisms of political pressure generation and helps explain why seemingly similar events can lead to different escalation trajectories.

## RESULTS

The proposed classification model shows that hybrid escalation cannot be adequately described as a linear increase in intensity. Instead, the analysis reveals two dynamics: a gradual build-up of political pressure through repeated low-intensity events and rapid escalation triggered by high-impact incidents. By combining the morphological framework with escalation pathways and the phase model, hybrid activities can be systematically categorized. Escalation dynamics are shaped by the physical impact of events and their interpretation over time. Repetition and pattern formation play a central role in generating pressure to act, even without high-intensity incidents. The combined phase and pathway approach distinguishes between isolated anomalies and strategically relevant developments, supporting a more precise assessment of hybrid dynamics in maritime critical infrastructures. Repeated disruptions of maritime infrastructure can indicate a transition from Phase 0 to Phase 1, as incidents evolve into patterns that increase political pressure to respond. In contrast, singular high-impact events may trigger a rapid transition to higher escalation phases.

## DISCUSSION AND CONCLUSION

The phase model describes hybrid escalation not as a linear increase in military intensity, but as a transformation of political and strategic decision-making conditions over the course of a conflict. Escalation dynamics emerge from systematic changes in key analytical categories such as ambiguity, repetition, and attribution. This linkage between the morphological framework and the phase model enables hybrid activities to be analyzed both structurally and dynamically. The model allows categorizing hybrid activities in the maritime environment more precisely and to move beyond purely intensity-based assessments. By combining a phase model with escalation pathways, it supports the analysis of both gradual and abrupt escalation dynamics in complex grey zone situations.

The phases should be understood as flexible analytical constructs rather than rigid states. Real conflict dynamics may oscillate between phases or exhibit characteristics of multiple phases simultaneously. Escalation is therefore not one-dimensional, as repetition and impact represent distinct and partially independent drivers. At the same time, the application of the framework depends on the availability and interpretation of information. In real-world scenarios, incomplete or conflicting data may limit the precision of categorization, particularly in early phases characterized by high ambiguity. Moreover, the systemic impact of hybrid activities remains highly context-dependent, as political perceptions, actor interdependencies, and strategic interpretations influence whether events accelerate or dampen escalation. Overall, the proposed approach provides a robust conceptual foundation for the structured assessment of hybrid threats in the maritime domain and offers a basis for future empirical validation.

## REFERENCES


Auswertiges Amt. (2023). *Nationale sicherheitsstrategie: Wehrhaft. Resilient. Nachhaltig*. Retrieved February 15, 2026, from https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf

Bewarder, M., Diehl, J., & Flade, F. (2026, February). BKA zählt mehr als 320 Sabotage-Verdachtsfälle.

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, *42*(3), 391–413.

Bueger, C., & Liebetrau, T. (2023). Critical maritime infrastructure protection: What's the trouble? *Marine Policy*, *155*(July), 105772.

Douglass, R. W., Gartzke, E., Lindsay, J. R., Gannon, J. A., & Scherer, T. L. (2024). What is escalation? Measuring crisis dynamics in international relations with human and LLM generated event data. *arXiv preprint arXiv:2402.03340*.

Edwards, C., & Seidenstein, N. (2025). *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure* [IISS]. Retrieved February 26, 2026, from https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/

Haugstvedt, H. (2021). Red Sea Drones: How to Counter Houthi Maritime Attacks.

ISW. (2026). *Russian Phase Zero Operations in Europe, Date Range: September 9, 2025 to February 2, 2026* [Institute for the Study of War]. Retrieved February 25, 2026, from https://understandingwar.org/map/russian-phase-zero-operations-in-europe-date-range-september-9-2025-to-february-2-2026/

Lanchès, J., & Rekawek, K. (2026, February). More of the Same. Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare Revisited.

Larsson, O. L. (2024). Sea blindness in grey zone preparations. *Defence Studies*, *24*(3), 399–420.

Levy, D., Pinko, E., & Shamir, E. (2026). Asymmetric war at sea: The doctrine of Iranian Revolutionary Guard Corps Navy (IRGCN). *Journal of Strategic Studies*, 1–35.

Libiseller, C. (2023). 'Hybrid warfare' as an academic fashion. *Journal of Strategic Studies*, *46*(4), 858–880.

McLaughlin, R. (2022). The Law of the Sea and PRC Gray-Zone Operations in the South China Sea. *American Journal of International Law*, *116*(4), 821–835.

Morris, L. J., Mazarr, M. J., Hornung, J., Pézard, S., Binnendijk, A., & Kepe, M. (2019). *Gaining competitive advantage in the gray zone: Response options for coercive aggression below the threshold of major war*. RAND Corporation.

Mumford, A., & Carlucci, P. (2023). Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, *8*(2), 192–206.

Person, R., Kulalic, I., & Mayle, J. (2024). Back to the future: The persistent problems of hybrid war. *International Affairs*, *100*(4), 1749–1761.

Radin, A. (2024). *A vocabulary of escalation* (Research Report No. RRA1933-1). RAND Corporation. Santa Monica, CA.

Ringbom, H., & Lott, A. (2024). Sabotage of Critical Offshore Infrastructure: A Case Study of the Balticconnector Incident. In A. Lott (Ed.), *Maritime Security Law in Hybrid Warfare* (pp. 155–194). Brill | Nijhoff.

Ritchey, T. (2006). Problem structuring using computer-aided morphological analysis. In *Journal of the operational research society* (pp. 792–801, Vol. 57).

Suchkov, M. A. (2021). Whose hybrid warfare? How 'the hybrid warfare' concept shapes Russian discourse, military, and political practice. *Small Wars & Insurgencies*, *32*(3), 415–440.

Tecklenburg, B., Stockbruegger, J., Niemi, A., & Sill Torres, F. (2025). Securing maritime infrastructures: A framework to evaluate physical protection measures for offshore wind farms. *Environment Systems and Decisions*, *45*(4), 67–.

The Economist. (2025). *Russia is violating Europe's skies with impunity*. https://www.economist.com/europe/2025/09/28/russia-is-violating-europes-skies-with-impunity

Zwicky, F. (1967). *Discovery, invention, research through the morphological approach*. Macmillan.