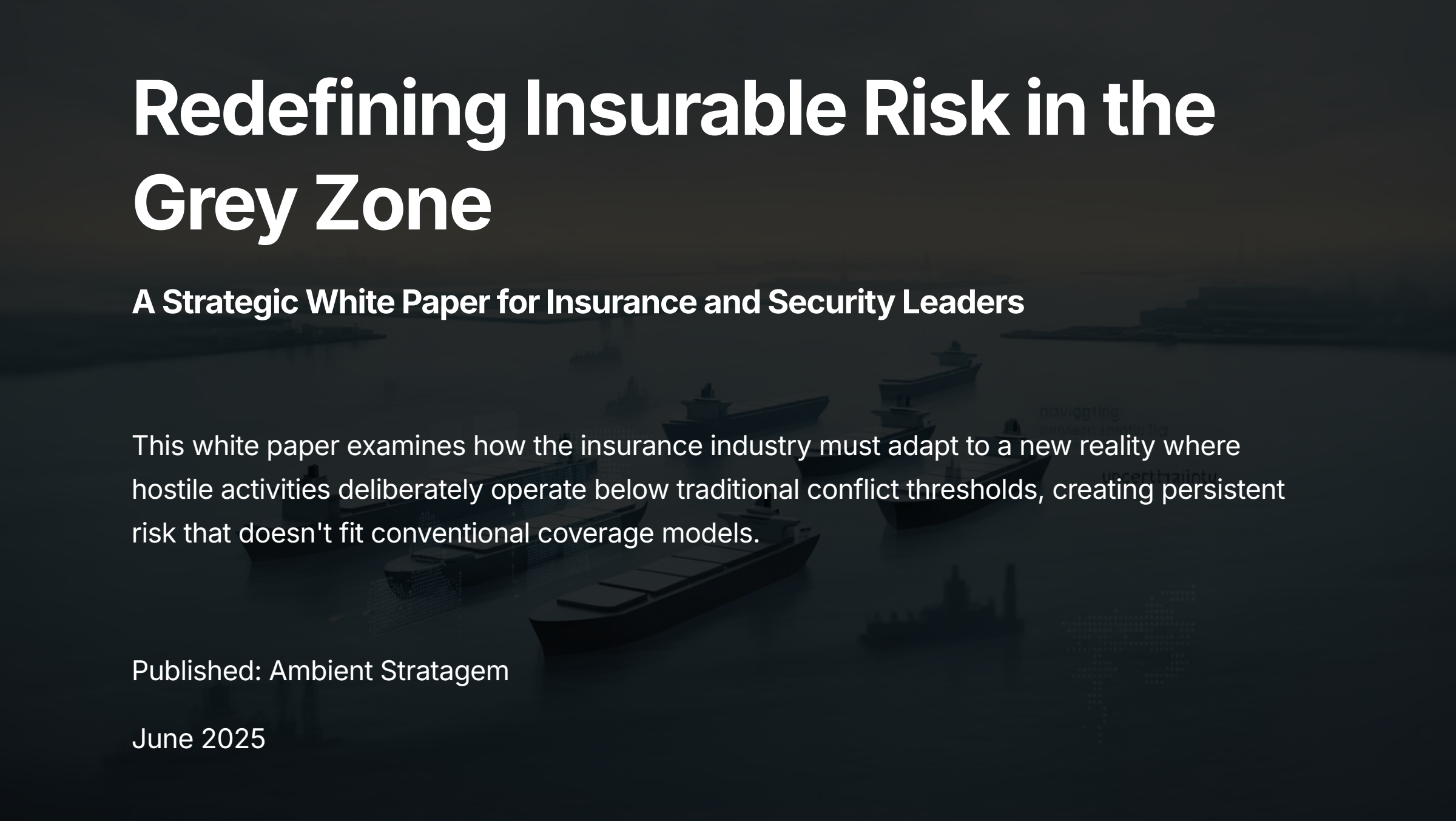
Redefining Insurable Risk in the Grey Zone

A Strategic White Paper for Insurance and Security Leaders



This white paper examines how the insurance industry must adapt to a new reality where hostile activities deliberately operate below traditional conflict thresholds, creating persistent risk that doesn't fit conventional coverage models.

Published: Ambient Stratagem

June 2025

Contents

1. Executive Summary

The global insurance sector is increasingly exposed to a category of threat that does not conform to its foundational assumptions. For decades, underwriting models have relied on event clarity, legal attribution and political declarations to activate coverage. Yet the strategic behaviour of peer adversaries, armed with doctrines designed to operate below the threshold of open conflict, has rendered those assumptions insufficient.

From the Baltic to the Red Sea, the first half of 2025 has demonstrated a persistent pattern of hostile interference with commercial systems and infrastructure, navigational spoofing, cyber-induced paralysis and maritime harassment among them. These actions are often unattributed, strategically timed and executed without crossing the traditional legal thresholds that trigger war, terrorism, or cyber coverage. In most cases, no single event stands out as uninsurable. But the pattern itself exposes a systemic vulnerability.

Strategic Doctrine

These incidents reflect more than regional instability. They are the operational outcomes of deliberate strategic doctrine. Adversary thinking now prioritises ambiguity, denial and environmental degradation over kinetic escalation. The intent is not necessarily to destroy assets, but to erode confidence, undermine continuity and strain systems that were not built to operate under constant, low-level contestation.

Structural Re-evaluation

This paper argues for a structural re-evaluation of how insurable risk is defined and modelled in such an environment. Current exclusions frameworks, particularly within war, terrorism and cyber clauses are not designed to account for strategic persistence. Nor do they reflect the behavioural adaptations now being made by ship operators, insurers and reinsurers alike in the face of continuous threat.

Proposed Solution

What is proposed is not a wholesale reinvention, but an augmentation: the formal recognition of Persistent Hostile Activity (PHA) as a named peril. This would involve new trigger logic, redefined attribution thresholds and pricing models that reflect exposure to long-duration interference rather than singular acts of aggression.

A shift of this kind will have implications for regulators, ratings agencies and capital markets. It will require collaborative design between risk carriers and the state, particularly in jurisdictions where infrastructure, defence and finance are increasingly interlinked. But failure to act risks a gradual retreat of insurance capacity from precisely the regions, corridors and systems where strategic resilience is most needed.

The recommendations outlined here are not speculative. They are drawn from validated incidents, strategic signals and doctrinal analysis from the first six months of 2025. The opportunity and the obligation, is now to align the risk model with the operational environment. To do otherwise is to underwrite blind to adversary design.

2. Preface: Why Grey Zone Doctrine Matters to Insurers

For many in the insurance and reinsurance community, the study of military doctrine sits at a distance, relevant perhaps to political risk underwriters or those involved in war and terror lines, but seldom seen as central to core actuarial assumptions. That boundary is no longer tenable. In the decade ahead, the most commercially relevant threats will not stem from formal warfighting, but from the deliberate use of sub-threshold tactics by capable adversaries, calibrated to exploit the seams between legal, financial and operational systems.

The term "Grey Zone" is now widely used to describe this space, a domain of competition where traditional rules of engagement are blurred, and where state and state-aligned actors pursue strategic advantage without triggering formal conflict. It includes, but is not limited to, cyber operations, electromagnetic disruption, disinformation, supply chain manipulation and targeted harassment of critical infrastructure. These activities are often episodic in appearance, but systemic in design.

Peer adversaries, particularly Russia, China and Iran, have developed distinct doctrinal approaches that view ambiguity as a tool, not an inconvenience. Russian reflexive control theory, for instance, is predicated on shaping the decision-making environment of adversaries through carefully timed signals, false attribution and legal obfuscation. In parallel, the People's Liberation Army (PLA) has articulated "Three Warfares" doctrine, legal, psychological and media-based strategies designed to win influence and operational advantage without crossing kinetic thresholds.

These are not academic frameworks. They are operationalised in ways that directly impact insurable interests. Take the persistent GPS spoofing emanating from Kaliningrad, affecting merchant shipping and commercial aviation over the Baltic Sea. Or the multi-month harassment of vessels in the Red Sea by Houthi forces using commercially available drones and missiles, activity that falls below the threshold of open war, but generates material loss, route deviation and market uncertainty.

The Dilemma

For insurers, these activities present a compound dilemma. First, they do not always meet the legal criteria for a covered event under war, terrorism, or cyber clauses.

Attribution Gap

Second, their intent is often to remain unprovable, creating precisely the kind of attribution gap on which most policy exclusions depend.

Accumulation

Third, they accumulate over time, generating pressure not through a singular incident, but through attritional degradation of confidence, operability and access.

What adversary doctrine has understood and what many coverage frameworks have not yet adapted to, is that commercial systems are not simply enablers of national power. They are strategic terrain. Maritime corridors, communications networks, financial hubs and energy infrastructure are now viewed not as collateral, but as primary theatres of influence.

In this context, underwriting cannot remain a passive observer. It must evolve to account for an environment in which strategic hostility is persistent, attribution is contested and legal thresholds are no longer reliable predictors of operational risk. This is not an argument for overreaction or for rewriting every line of coverage. It is a call for doctrinal awareness. A recognition that the adversary's logic, when left unexamined, becomes a systemic blind spot in our own.

Insurers have long navigated uncertainty. But the Grey Zone demands more than probabilistic foresight. It demands structural fluency in how threats are designed, sequenced and deployed. The pages that follow aim to provide that fluency, not as a military treatise, but as a strategic reframing of what risk now looks like and what it may soon become.

3. Introduction: The End of the Event Model

The underwriting of extreme risk has, historically, leaned heavily on clarity of cause. Conflict is declared. Terrorism is claimed. Cyber breaches are attributed. From such declarations, the machinery of assessment, pricing and response can operate with a degree of confidence. In return, capital is made available. But in the operating environment of 2025, that architecture is beginning to misalign with the threat it is meant to cover.

Insurers have always dealt in uncertainty. What is changing is the nature of the uncertainty itself. It is no longer a question of whether a hostile act will occur, but of how it will be defined and when, or if, it will be acknowledged. In this strategic setting, the distinction between war and peace is no longer temporally bounded. The event, a missile strike, a declared conflict, a proven state actor, is no longer the anchor. What persists instead is a form of ambient hostility: slow-moving, ambiguous and strategically maintained.

Between January and June 2025, this reality has been sharply illustrated. In the Baltic Sea, commercial airliners and maritime vessels operating near Kaliningrad have experienced repeated GPS disruptions, confirmed by European aviation and transport authorities ([1], [2]). The source is widely understood, but never formally acknowledged. In the Red Sea, commercial shipping has been targeted through both direct strikes and legal ambiguity. At one point, Houthi leadership explicitly exempted U.S. vessels from further attacks under a temporary ceasefire, while reaffirming the right to strike vessels affiliated with other nations ([5]).

These actions do not occur in a vacuum. They are shaped by doctrine and designed with intent. That intent, however, does not always express itself in forms that existing insurance frameworks are equipped to handle. Attribution is blurred. State involvement is inferred but not confirmed. And most significantly, the timeline of hostility is no longer structured around escalation and resolution. It is ongoing.

In response, market behaviours have begun to adapt, even in the absence of formal redefinition. Operators such as Frontline have suspended new contracts through the Strait of Hormuz due to perceived risk, not declared conflict ([7]). Other vessels have adopted digital deception strategies, broadcasting misleading AIS signals such as "China-owned" to deter attack, a form of protective obfuscation that sits entirely outside the underwriting model ([6]).

These decisions are operationally rational. Yet they point to a deeper misalignment between the reality of exposure and the structure of coverage. When risk is treated as episodic, but behaves as continuous, gaps inevitably emerge. These gaps are not just technical. They are strategic. They create conditions in which adversaries can apply pressure, knowing that the insurance system itself is not designed to respond until a particular line is crossed, a line that they will take care never to step over.

> It would be easy to frame this as an emerging threat, but that would understate the point. It is already here. The incidents referenced in this paper are not forecasts or hypotheticals. They are validated flashpoints from the first half of this year. Each one highlights the same structural challenge: that hostile activity has adapted faster than the frameworks designed to protect against it.

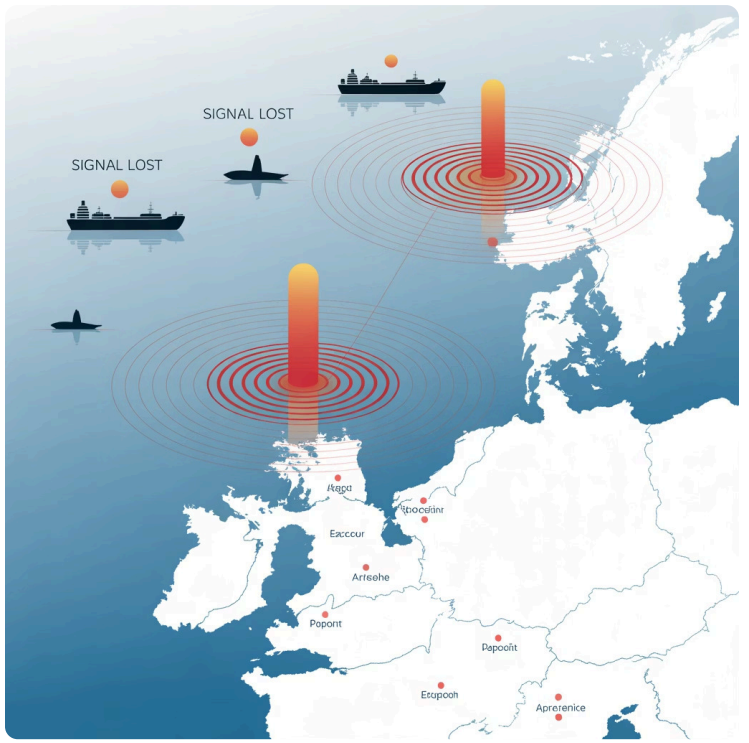
This paper does not seek to prescribe a singular solution. Rather, it offers a reframing, a move away from the idea that hostile risk must be event-based and toward an understanding that exposure can be environmental, accumulative and strategically sustained. It proposes a formal recognition of Persistent Hostile Activity (PHA) as an insurable condition and outlines the criteria by which such a framework might be constructed.

1. **Episodic Shock to Ambient Interference**
   The transition from episodic shock to ambient interference
2. **Infrastructure as Battleground**
   The reclassification of infrastructure as a deliberate theatre of operation
3. **Binary Clauses**
   The insufficiency of binary clauses in a spectrum-based threat environment
4. **Market Signals**
   Market behaviours as signals of systemic stress
5. **New Peril Class**
   The case for a new class of insurable peril: Persistent Hostile Activity
6. **Regulatory Alignment**
   A structured roadmap for aligning this model with regulatory and ratings architecture

This is not a departure from the discipline of underwriting. It is a refinement of it. One that begins with a clear view of the threat as it now stands and a commitment to ensuring that the systems built to manage risk are no longer blind to the conditions that define it.

4. From Episodic Shock to Ambient Hostility

Insurable risk has long rested on a foundational expectation: that perils are episodic. Whether natural or man-made, threats are understood to arise, cause disruption and then recede, enabling the recalibration of exposure, the restoration of continuity and the resetting of premium assumptions. But the operating conditions that now define many of the world's key commercial corridors no longer conform to this model.



In early 2025, GPS signal disruption in the Baltic region became more than an intermittent concern. Civilian vessels, passenger aircraft and port authorities reported sustained interference, with navigational systems routinely jammed or spoofed while operating near the Russian exclave of Kaliningrad. Baltic governments, including Lithuania, issued public warnings acknowledging that this interference was neither new nor likely to cease following the resolution of more visible regional hostilities ([1], [2]).

What these signals confirm is the emergence of a new threat character: persistent, low-level, state-aligned disruption of commercial systems that does not aim to escalate, but to endure. The term "grey zone" may imply ambiguity, but the effect on insurable operations is increasingly tangible. Shipping routes are altered. Port calls are delayed. Liability accumulates across marine, cyber and energy lines, without a single incident rising to trigger coverage.

This dynamic is not confined to the Baltic. In the Red Sea, Houthi forces backed by Iranian technology have mounted months of coordinated harassment against international shipping. Between March and May, a series of retaliatory strikes, part of the joint U.S.-UK Operation Rough Rider, were conducted against facilities used to launch drones and missiles. Yet throughout this period, maritime attacks continued to occur below the formal threshold of war ([3], [4]).

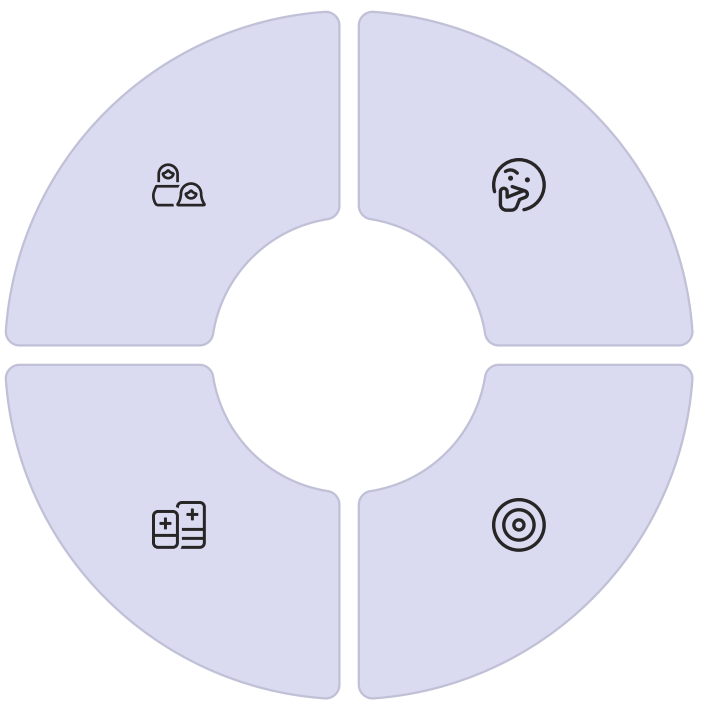
Even when a temporary ceasefire was declared in early May, it applied selectively. U.S.-flagged ships were granted reprieve; Israeli-linked vessels remained valid targets under Houthi logic ([5]). This selective modulation of threat posture reveals a strategic calculus: hostile pressure is maintained, but shaped to avoid triggering a full-scale escalation, or a definitive coverage response.

Russian Doctrine

Russian military thought, influenced by the concept of reflexive control, privileges ambiguity, signalling and the manipulation of perceived risk.

Insurance Challenge

This logic sits uneasily within traditional insurance frameworks that rely on identifiable triggers, declarations, events, or attributions.



Chinese Doctrine

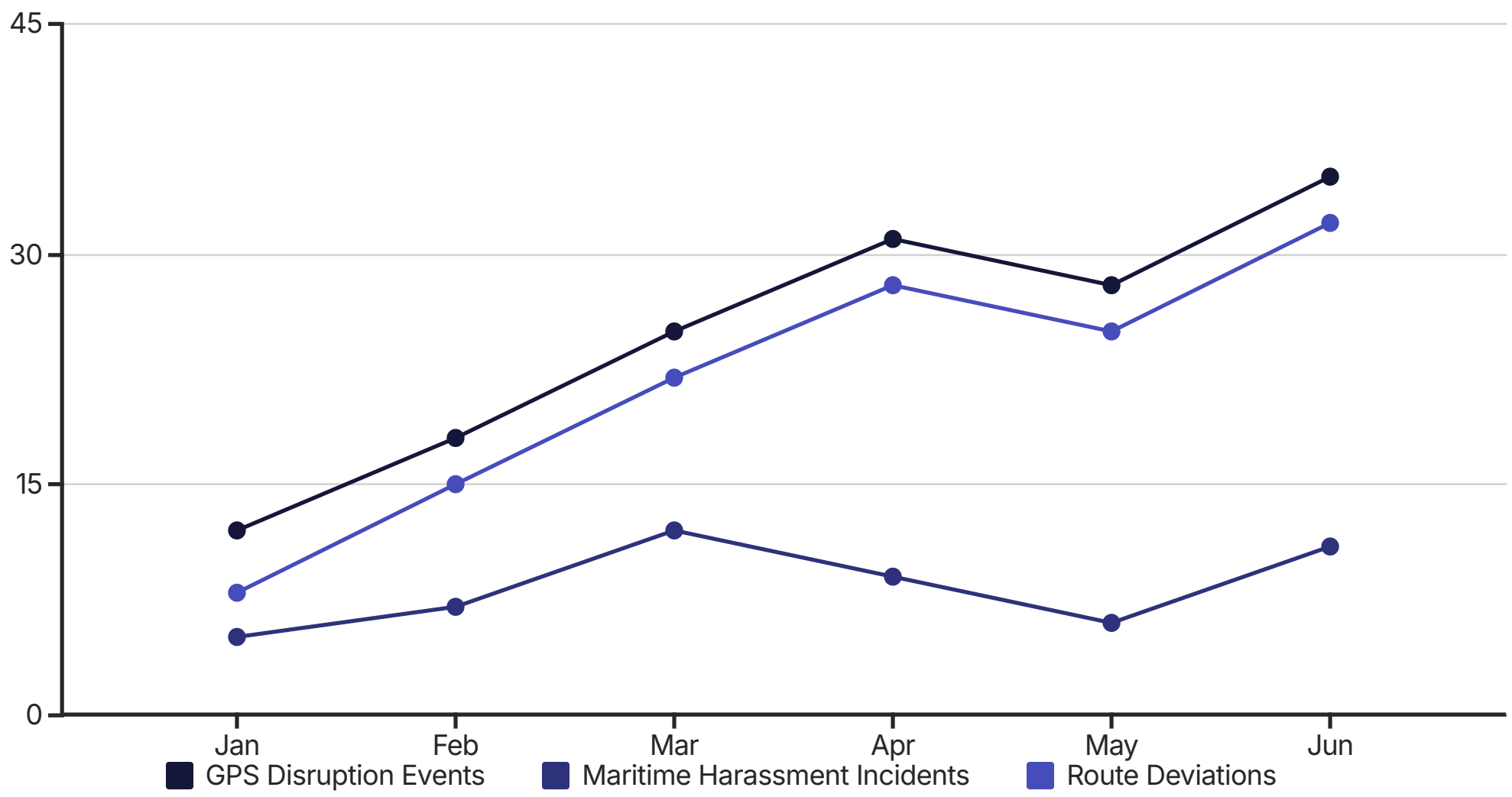
Chinese "Three Warfares" doctrine emphasises the utility of legal ambiguity, narrative control and psychological shaping.

Shared Approach

Both approaches share a recognition that disruption need not be decisive to be effective, it need only be sustained, deniable and well-timed.

This logic sits uneasily within traditional insurance frameworks. The industry has developed highly specialised models to price and reinsure war, terrorism and cyber events. These models rely on identifiable triggers, declarations, events, or attributions that demarcate the beginning and end of a claimable occurrence. But in the current environment, few such demarcations exist. Instead, there is friction without rupture, pressure without breach, exposure without activation.

What emerges, therefore, is a cumulative risk profile. One that cannot be priced through historical frequency tables or isolated loss events. The GPS jamming in the Baltic has not resulted in a single hull loss. Yet it has already imposed significant navigational uncertainty, delayed voyages and introduced systemic risk to both marine and cyber portfolios. Similarly, Houthi maritime activity has not closed the Red Sea outright, but it has prompted route changes, elevated premiums and realignment of shipping capacity.



In short, what underwriters are now facing is not a spike in catastrophic events, but the slow normalisation of contestation. The risk is not that a war will break out, but that a climate of sub-threshold hostility becomes the baseline condition, a form of strategic weather that remains just disruptive enough to degrade operations, inflate cost and generate persistent liability.

This requires a recalibration of how insurable peril is understood. The notion that risk must be event-based no longer reflects the exposure landscape. What is needed is a supplementary framework, one that accounts for continuous hostile activity, even in the absence of attribution or overt conflict. This is not a replacement for traditional war or cyber cover. It is a necessary evolution, designed to bridge the space between event and environment.

In doing so, the insurance market can begin to align itself not with the declarations of state actors, but with the reality of their conduct. It can respond to the pattern, rather than wait for the spark. And in doing so, it can help to restore operational predictability in domains where formal stability may no longer be forthcoming.

5. Civilian Infrastructure as a Deliberate Battleground

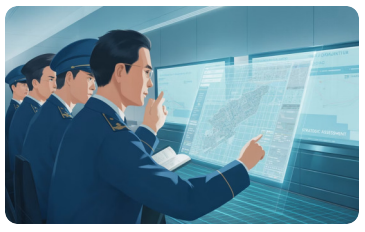
There has long been an implicit assumption in insurance that civilian infrastructure sits one step removed from the battlefield. Even in high-risk territories, commercial assets have typically been viewed as either unfortunate bystanders to conflict or secondary targets whose exposure could be modelled through well-understood escalation pathways. That assumption is beginning to unravel.

Across multiple regions in 2025, we have witnessed a strategic turn: infrastructure is no longer merely at risk of incidental damage, it is being positioned as the primary arena through which pressure is applied. The consequences of this shift are not abstract. They are directly measurable in the operational choices being made by states, by commercial actors and increasingly by underwriters themselves.

In April, U.S. forces conducted a series of precision strikes on Yemen's Ras Isa oil terminal, a facility under Houthi control and known to be a node for maritime disruption operations ([3]). The strike followed repeated drone and missile attacks on commercial vessels in the region. From a military perspective, the operation was calibrated, specific targets, clear justifications, minimal escalation. But from an insurance perspective, the incident highlighted the fragility of assumptions around energy and marine asset immunity. A non-state actor's use of a nominally civilian facility for disruptive operations invited a state-level response, exposing commercial infrastructure to direct retaliatory force.

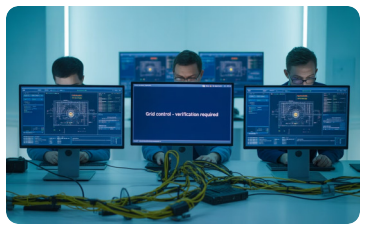
This pattern has not been confined to the Gulf. In the Baltic, sustained interference with satellite navigation systems has disrupted both aviation and shipping. While not physically damaging, such jamming operations have rendered essential navigational tools unreliable, increasing collision risk, degrading schedule integrity, and raising liability exposure without any visible violence ([1], [2]). The physical assets remain untouched, yet the systems that enable their safe use have been compromised.

Both cases reflect a doctrinal convergence. Peer and near-peer adversaries are increasingly operationalising a form of competition that targets systems, not symbols. Rather than attacking the seat of government or military headquarters, they seek to degrade trust in the mechanisms of daily function: port security, energy flows, digital navigation and supply chain integrity.



Chinese Systems Confrontation

Chinese doctrine has long recognised the strategic utility of infrastructure shaping. The PLA's emphasis on "systems confrontation" in its strategic writings, particularly those underpinning its concept of informatized warfare, places civilian dual-use infrastructure in the centre of the battlespace.



Russian Infrastructure Targeting

Russian campaigns in Georgia, Ukraine, and Syria have repeatedly included efforts to disable energy grids, communications relays, and transportation chokepoints, whether through kinetic or non-kinetic means.

In this context, the delineation between military and civilian targeting becomes porous. Ports, logistics hubs and maritime corridors are not selected for destruction, but for manipulation. Their role is not to absorb firepower, but to absorb uncertainty. The intended effect is erosion, of confidence, of reliability, and of the institutional routines that allow international commerce to function predictably.

For insurers, the implications are significant. Traditional exclusions frameworks, particularly in the marine, energy and terrorism spaces, are not well suited to this mode of operation. War cover, for instance, often relies on a declared conflict or demonstrable state action. Terrorism cover may hinge on political motives or identifiable ideological objectives. Cyber cover is frequently constrained by attribution clauses or narrow definitions of digital entry.

But in the flashpoints observed this year, none of those triggers are reliably present. The Ras Isa terminal was struck by a state actor, but the target was a non-state group using civilian infrastructure. The GPS jamming in the Baltic has caused operational disruption, but no nation has claimed responsibility and no physical damage has occurred. The insurance industry finds itself exposed to operationally significant actions that fall between its established categories.

68%

Coverage Gap

Percentage of grey zone incidents that fall between traditional war, terrorism, and cyber coverage definitions

42%

Market Withdrawal

Increase in exclusion zones and coverage limitations in strategic maritime corridors since January 2025

3.5x

Premium Inflation

Average increase in war risk premiums for vessels transiting contested zones without clear conflict status

This structural ambiguity invites two risks. The first is mispricing, exposure is either inadequately accounted for or subject to excessive conservatism. The second is market withdrawal, where underwriters, unable to resolve attribution or categorisation, choose to exit risk entirely. Both outcomes reduce capacity in areas where resilience is most needed.

This paper does not advocate for the elimination of boundaries between perils. But it does suggest that the operational realities now facing global infrastructure, particularly those aligned to shipping, energy, and communications, require the development of a supplementary framework. One that acknowledges the strategic logic behind infrastructure targeting and builds insurability around the function being disrupted, rather than the actor presumed responsible.

Such a framework would allow insurers to price and pool risk based on exposure to persistent hostile activity, irrespective of whether that activity conforms to existing categories of war, terror, or cyber. In doing so, it would begin to close the gap between the battlefield as adversaries now define it, and the systems through which commercial continuity is underwritten.

6. Attribution, Intention and the Collapse of Binary Clauses

For much of the modern insurance era, the question of who caused a loss has carried nearly as much weight as what occurred. Attribution, whether legal, political, or forensic, has been a gatekeeper for coverage. It enables distinction between perils, allocation of responsibility and in many cases, activation of policy terms. However, as the operational environment continues to evolve under conditions of strategic ambiguity, the role of attribution as a reliable determinant of insurability is under increasing strain.

Across multiple flashpoints in early 2025, it has become evident that attribution is no longer a fixed or even necessarily functional input. In some cases, the actor responsible for the disruption is known, but not acknowledged. In others, the attribution is deliberately split, partially claimed, selectively declared, or framed in such a way that it avoids triggering formal policy conditions.

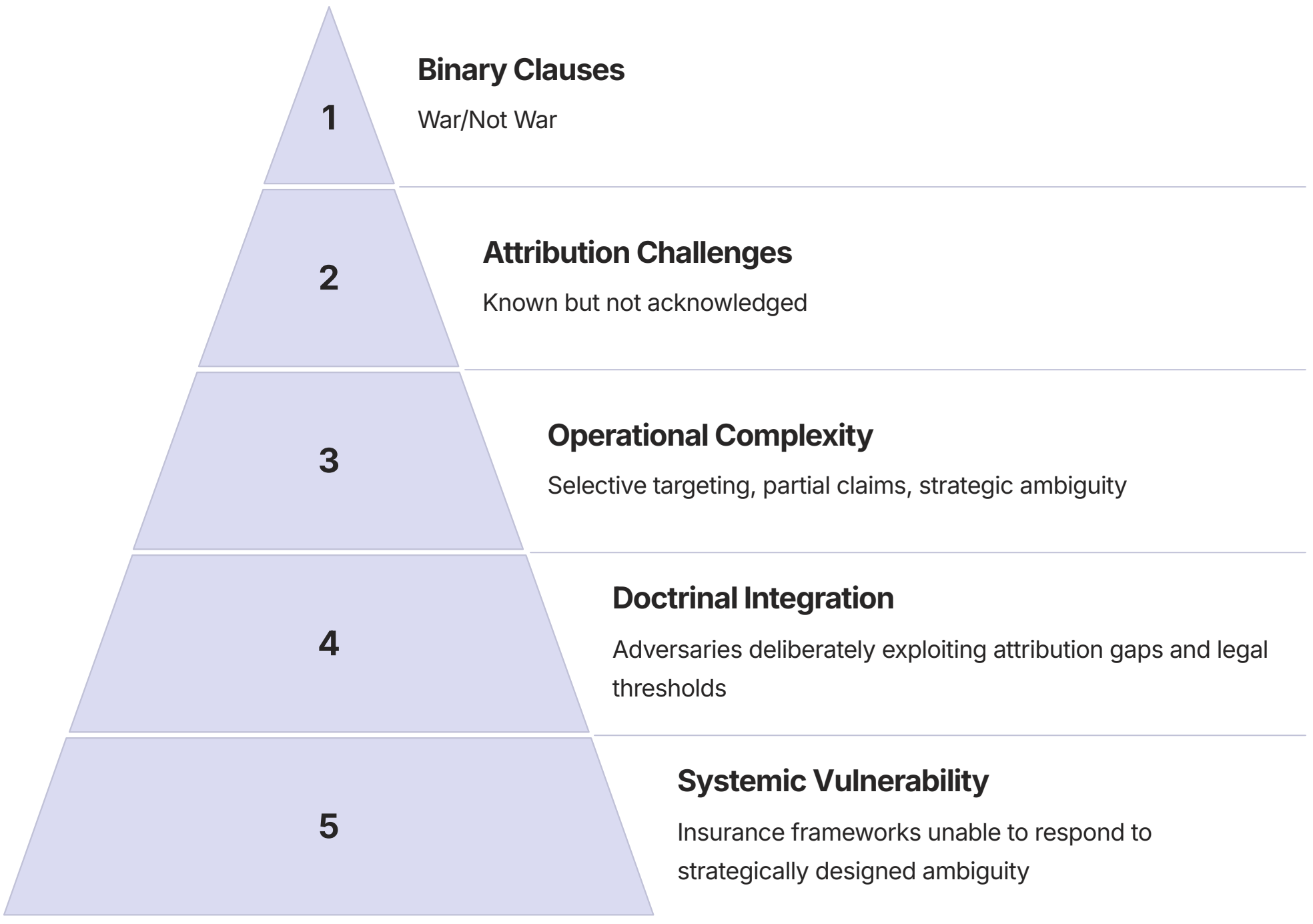
The temporary ceasefire negotiated in May between the United States and Houthi leadership is a case in point. While hostilities towards American-linked shipping were suspended, the same latitude was not extended to vessels affiliated with Israel or other partners ([5]). The message was calibrated: we remain operationally capable, but selectively engaged. This is not a cessation of conflict in any meaningful insurance sense. Nor does it neatly fit within existing clause language. Traditional war exclusions are not written to accommodate differentiated targeting based on political leverage.

Similarly, the spoofing of Automatic Identification System (AIS) signals by commercial shipping vessels in the Strait of Hormuz, reported in June, reflected another form of attribution complexity ([6]). Ships broadcasted false ownership data, such as designating themselves as "China-owned", in an effort to manipulate perceived threat levels. While no overt incident followed, the behaviour itself speaks to a deeper erosion of confidence in institutional protections. When operators resort to deception to avoid becoming targets, it is often because they do not believe attribution will be respected or acted upon by third parties, including insurers.

Attribution has always involved a degree of interpretation. What has changed is the level of strategic effort being invested in manipulating the attribution process itself. Peer adversaries have integrated this into their doctrine. Russian reflexive control theory, for example, recognises that shaping the adversary's perception of causality can be more effective than controlling outcomes directly. The PLA's legal warfare component of its Three Warfares doctrine similarly seeks to pre-empt or frustrate external responses through selective legal framing of actions and intentions.

The result is a deliberate contest over narrative control. This contest is not confined to media or diplomacy, it extends into the legal and contractual domains on which insurance mechanisms depend. For example, in the cyber domain, disputes continue over whether state-aligned attacks such as NotPetya or SolarWinds constitute "acts of war" when no formal state admission has occurred and no conventional conflict has been declared ([8]). Litigation remains unresolved and coverage determinations are fragmented.

These trends highlight the fragility of binary clauses, those which predicate coverage or exclusion on whether a risk falls inside or outside specific categories such as war, cyber, or terrorism. In a world where actors blend techniques, proxy relationships obscure intent and formal declarations are strategically withheld, binary logic introduces operational risk into the policy system itself.



It is not that such clauses are inherently flawed. They have functioned effectively in environments where state conduct was more transparent and escalation pathways more predictable. But they now face structural misalignment with adversary behaviour. Hostile acts are designed to occur in a space between definitions. They are executed in ways that frustrate clarity, delay response and exploit the latency of attribution processes.

For insurers, this presents a twofold challenge. First, the inability to confirm attribution at the point of loss can lead to delays, disputes, or outright gaps in cover. Second, the systemic ambiguity surrounding intention and classification can undermine confidence in underwriting assumptions, not only for primary carriers, but for reinsurers and capital markets seeking to price aggregate exposure.

There is no simple fix. The objective cannot be to eliminate ambiguity from a threat landscape that is increasingly defined by its presence. But the current reliance on binary trigger points leaves insurers vulnerable to precisely the kind of risk shaping that adversaries have become adept at exploiting.

What is required is a shift in how exposure is conceptualised. Rather than attempting to sharpen the boundary lines of war, terror, or cyber perils, there is a case for introducing a parallel framework that accounts for hostile intent and operational effect, even where attribution remains contested.

Such a framework might incorporate:

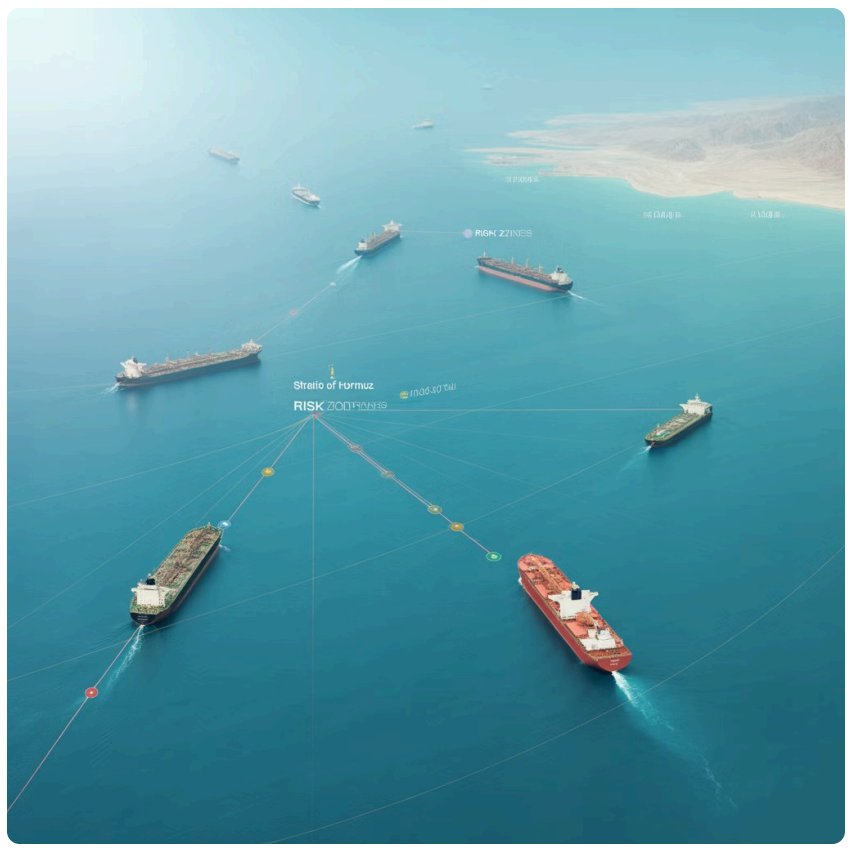
- Behavioural indicators of strategic shaping, such as AIS spoofing or signal degradation;
- Official declarations of ambient interference by trusted state authorities (e.g. Lithuania's warnings over GPS jamming [2]);
- Patterns of non-kinetic disruption sustained over time, regardless of claimed responsibility.

This is not an argument for looser underwriting. On the contrary, it is a recognition that adversary doctrine has become more precise in its use of ambiguity as a tool. If insurers are to remain viable participants in contested spaces, they must evolve with equal precision, not by abandoning definitions, but by recognising where those definitions no longer serve.

7. Market Response as Strategic Signal

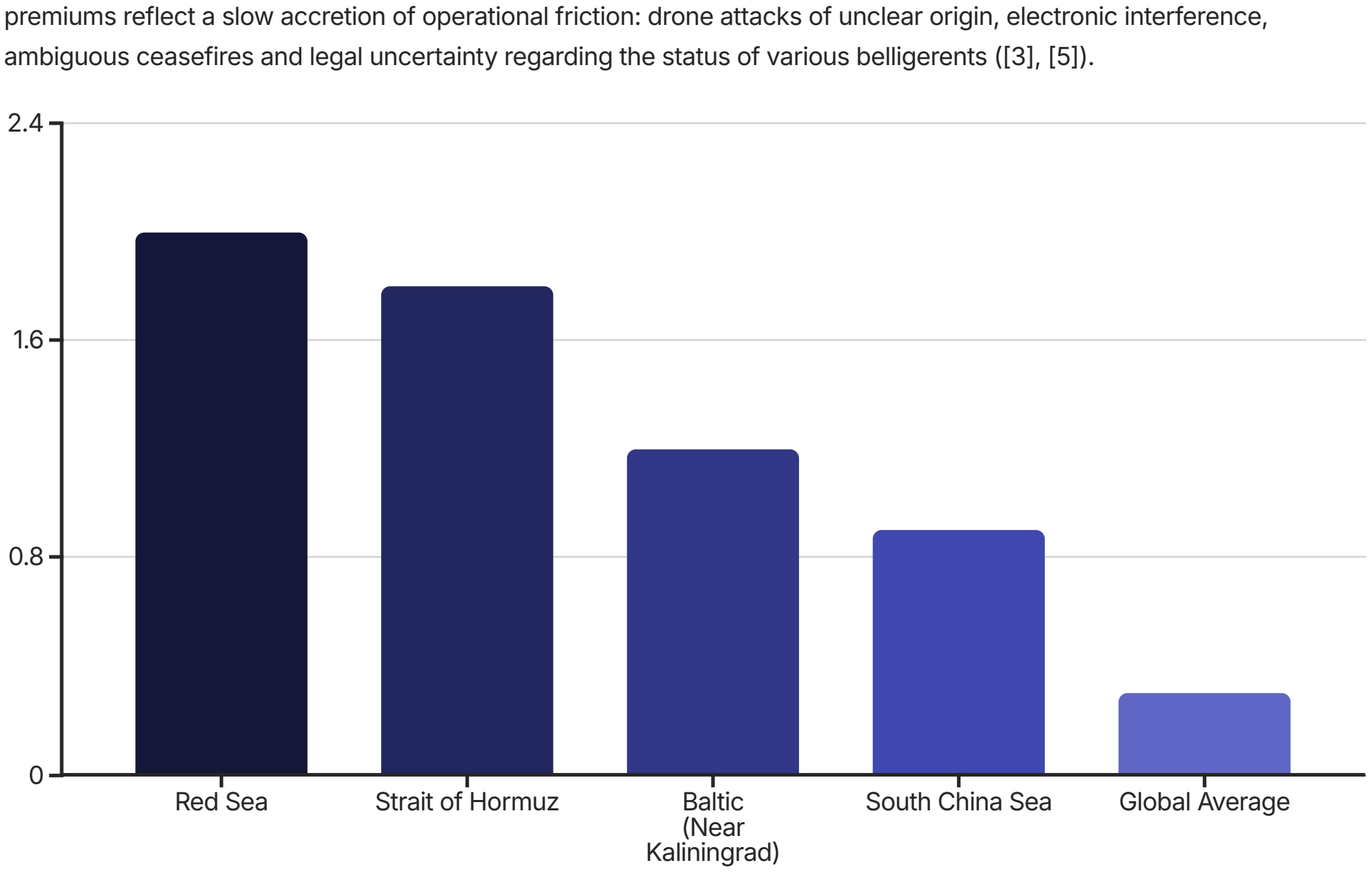
In conflict analysis, actions often speak more clearly than declarations. This principle is no less applicable in the insurance market, where shifts in cover availability, pricing and contract behaviour can serve as early indicators of systemic stress. In the first half of 2025, the behaviour of key actors in the global maritime and energy sectors has signalled not only commercial risk aversion but an emerging recognition that traditional frameworks are ill-suited to the current strategic environment.

When Frontline, one of the world's largest tanker operators, announced in June its decision to pause new contracts through the Strait of Hormuz, it did so without citing a specific event or loss trigger ([7]). The decision followed a period of increased geopolitical tension, including hostile maritime actions by non-state groups, AIS spoofing, and contested ceasefire arrangements. Yet what prompted the decision was not a singular strike or act of war, but the cumulative erosion of operating confidence. In effect, the market responded to a pattern rather than a flashpoint.



This is a marked departure from historic practice. For decades, war-risk cover in key transit zones has been adjusted in response to declared conflict or insured loss events. Underwriters, brokers and reinsurers have operated within a shared framework of activation logic: a trigger occurs, the clause responds, rates adjust. That model presumes a certain visibility, that risk is observable, attributable and finite. But in the Grey Zone, these qualities are often absent.

In the Red Sea and Gulf of Aden, war-risk premiums have remained elevated since Q1 2025. In some cases, rates have reached 2% of hull value, a figure usually associated with open conflict. Yet this pricing has been sustained without a single, formally declared war event or government-issued advisory defining the area as an active war zone. Instead, the premiums reflect a slow accretion of operational friction: drone attacks of unclear origin, electronic interference, ambiguous ceasefires and legal uncertainty regarding the status of various belligerents ([3], [5]).



What the market is expressing, through both pricing and capacity withdrawal, is not simply heightened risk, but structural uncertainty. Underwriters are no longer merely assessing loss probability. They are accounting for the breakdown of predictability in attribution, escalation and response. In this sense, market behaviour becomes an external signal of system-level degradation. Where institutional structures cannot provide clarity, commercial actors begin to define their own thresholds.

This has consequences. The withdrawal or pricing out of cover from critical corridors such as the Red Sea, the Strait of Hormuz, or the South China Sea does not simply reflect commercial caution. It alters the operational calculus of shipping companies, trading houses and insurers themselves. Rerouted vessels incur higher fuel costs, longer transit times and increased carbon exposure. All of which ripple through energy pricing, global trade balances and ESG reporting frameworks.

When cover is unavailable or unaffordable, insured parties are left with unenforced liabilities or assume unmodelled exposure. Some shift risk onto sovereign backstops. Others engage in behavioural adaptation, such as the broadcasting of deceptive AIS signals to deter targeting ([6]). These adaptations, while operationally rational, reflect an environment where the insurance system is no longer fully functional as a buffer between commercial continuity and geopolitical volatility.

This is not a theoretical observation. The spoofing of AIS identities, undertaken by vessels hoping to appear affiliated with neutral or powerful actors (e.g. "China-owned"), reflects a conscious attempt to manipulate the risk landscape outside of legal or institutional recourse. It is not just the underwriting frameworks that are being circumvented, but the very norms on which shared maritime security depends.

Operational Adaptation

Vessels engage in deceptive practices like AIS spoofing to avoid targeting

Market Withdrawal

Insurers limit or withdraw coverage from contested areas

Premium Escalation

War risk rates reach conflict-level pricing without formal declarations

Strategic Vulnerability

Critical infrastructure and supply chains lose resilience precisely when most needed

Equally telling is the continued legal contestation over legacy cyberattacks such as NotPetya and SolarWinds. Though these occurred years prior, they remain unresolved in coverage terms, with court cases still determining whether such attacks fall under war exclusions or constitute insurable cyber events ([8]). This latency in legal and contractual resolution is itself a risk, particularly in a domain where adversaries move faster than the frameworks designed to account for them.

Taken together, these market responses should not be read solely as symptoms of geopolitical instability. They are indicators of strategic adaptation, by both adversaries and commercial actors. The insurance market, long a follower of sovereign cues, is increasingly required to lead in defining where risk resides and how it is to be structured.

> The imperative now is to bring that leadership into alignment with doctrine. If adversaries are shaping the environment to remain just below traditional coverage thresholds, then it falls to insurers, reinsurers, and regulators to develop instruments that are not only responsive, but anticipatory.

Instruments that reflect exposure to persistent hostile activity, not through singular trigger events, but through observable changes in operating behaviour, risk pricing and commercial conduct.

The alternative is not inaction, but increasing exclusion, a steady withdrawal from areas that matter, at the very moment they require deeper resilience. That is not a sustainable outcome for the market. Nor is it one that aligns with the strategic needs of states, institutions, or the wider economic system that insurance is designed to underpin.

8. Persistent Hostile Activity as a Named Peril

For the insurance and reinsurance market to maintain strategic relevance in an era of ambient contestation, it must develop new conceptual tools to recognise and structure risk. Chief among these is the formalisation of Persistent Hostile Activity (PHA) as a named peril, not as a substitute for existing categories such as war, terrorism, or cyber, but as a complementary class of risk that captures exposure to enduring, sub-threshold interference by capable actors.

The case for doing so is not theoretical. It is grounded in the operational evidence of 2025. In the Red Sea, Baltic, and Strait of Hormuz, commercial continuity has been repeatedly undermined by hostile actions that are neither formally attributed nor easily categorised. The cumulative effect of these actions, from signal jamming to unclaimed drone attacks, has exceeded the disruptive impact of many conventional loss events. Yet in most cases, existing clauses have struggled to respond, or have done so only through indirect adaptation: pricing adjustments, corridor exclusions, or discretionary contract suspensions.

A PHA framework would offer an explicit mechanism to account for this form of exposure, acknowledging that strategic actors are now designing their operations not to escalate, but to endure. The goal of such a clause would not be to absorb all ambiguity, nor to replace traditional cover. It would instead provide structured recognition of a third condition: one in which hostile activity is present, commercially material, and below the conventional thresholds of attribution and escalation.

Designing such a framework would require discipline. PHA cannot become a catch-all. Its legitimacy must rest on clear criteria and measurable triggers, capable of supporting both underwriting judgment and legal enforceability.

Among the components that might define a viable PHA construct are:

Environmental Persistence

PHA should apply where interference or hostile acts occur over a defined period, for example, where a navigational or cyber domain is affected continuously or intermittently across multiple weeks or months, with operational consequence for insured parties.

This could be supported by state-issued notices (e.g. Lithuania's GPS jamming alerts in the Baltic [2]) or verified incident logs from sector regulators, port authorities, or maritime security entities.

Deliberate Hostile Effect

The clause would apply where the activity in question, while not formally attributable, is consistent with hostile intent and designed to generate friction or degradation, whether through interference, manipulation, or disruption of commercial systems.

Such intent could be inferred from behaviour, especially where non-kinetic actions (e.g. spoofing, misdirection, staged ambiguity) are patterned, sustained, and targeted.

Trigger Thresholds

Rather than relying on singular flashpoints, the PHA clause would activate through parametric thresholds. These might include a cumulative disruption index (e.g. number of affected voyages, signal loss incidents, confirmed AIS spoofing events) or defined regulatory signals (e.g. threat level elevations, navigational advisories, government policy statements).

This approach would mirror the increasing use of parametric modelling in catastrophe and climate risk, aligning coverage logic with environmental rather than event-based thinking.

Defined Zones of Exposure

To guard against overextension, PHA coverage could be geofenced, applying only within corridors or domains formally designated as exposed to persistent contestation. These could include maritime chokepoints, aerial corridors, or terrestrial infrastructure zones known to be subject to grey-zone tactics.

Zone designation could be made dynamic, subject to review by joint underwriting panels, in coordination with state authorities and security intelligence providers.

Non-Attribution Conditionality

Critically, PHA would not require formal attribution. Instead, it would rest on observed effect. This represents a significant departure from war and terrorism frameworks, where the act of naming the adversary is often a condition of cover or exclusion. Here, the adversary's deliberate use of deniability would no longer invalidate the insured's right to claim.

This construct would not sit easily within all portfolios. Some reinsurers may see it as an unacceptable dilution of clarity. Others may view it as a necessary adaptation to the environments from which traditional cover is now retreating.

But precedent already exists. In cyber insurance, aggregated breach conditions and threat actor behaviour patterns are increasingly used as modelling inputs. In terrorism cover, Pool Re and other mechanisms have gradually introduced broader triggers to reflect the blurred lines between ideology, criminality and state support.

What is required now is to bring these evolutions into a coherent framework, one that is explicitly designed to account for activity that is hostile, persistent, and below threshold.

This paper does not prescribe the final form. It offers a starting point. A sketch of how PHA might be conceptualised, structured, and underwritten. It is an invitation to the market, not only to price for what is already occurring, but to design for what doctrine now intends.

Persistent Hostile Activity is not an abstract threat. It is operationally active, strategically integrated and commercially consequential. The question is not whether it should be covered but how and with what level of structural maturity.

9. Blueprint for Regulatory and Ratings Alignment

If Persistent Hostile Activity (PHA) is to be brought into the architecture of insurable risk, it cannot remain a specialist product at the margins of the market. It must be legible not only to underwriters and reinsurers, but to those institutions that govern capital flows, regulate solvency, and assess portfolio resilience under conditions of stress. For PHA to gain operational traction, it must be structurally aligned with the expectations of supervisors, ratings agencies, and the broader financial system.

This is not a novel task. Insurance has a long history of adapting to risk that outpaces regulation, from the early structuring of aviation liability, to the post-9/11 treatment of terrorism pools, to the more recent supervisory focus on operational resilience and cyber accumulation. What distinguishes the PHA proposition is the nature of the ambiguity it seeks to address: strategic, rather than technical; adversary-designed, rather than incident-led.

Supervisory authorities such as the Bank of England's Prudential Regulation Authority (PRA) have already laid the groundwork for a more dynamic interpretation of exposure. SS1/21, the PRA's statement on operational resilience, explicitly moves away from single-event thinking in favour of impact tolerances, defined not by the size of a given incident, but by the capacity of a firm to maintain critical functions through extended disruption ([10]). This logic is compatible with the underlying thesis of PHA.

From a regulatory perspective, the first step is definitional coherence. Any attempt to introduce a named peril into the underwriting landscape must be accompanied by precise wording, sufficient to withstand legal scrutiny, yet adaptable to a shifting operational environment. Here, the evolution of cyber policy language offers a precedent. Clauses have moved from simplistic breach/event terms to include terms such as "hostile act," "sustained interference," and "state-aligned capability." PHA will require similar care, ensuring that ambiguity does not become vagueness and that cover clarity is maintained without demanding an impossible standard of proof.

Regulators will also expect evidence of loss modelling discipline. PHA is, by definition, a peril whose risk distribution is difficult to forecast using conventional actuarial tools. However, this is no longer a sufficient argument against its inclusion. Climate-related financial risks, for example, are now modelled using scenario analysis, system stress simulations and non-linear impact forecasting, many of which are explicitly acknowledged as speculative in regulatory guidance.

A similar approach can be taken for PHA. Scenario-based stress testing, built on validated flashpoints, such as those included in this paper, can offer a basis for supervisory engagement. Geospatial analysis of contested corridors, combined with behavioural indicators (e.g. AIS spoofing, official advisories, communications degradation), can support a probabilistic understanding of exposure, even in the absence of traditional frequency/severity models.

Ratings agencies, likewise, have a role to play in shaping the capital logic of PHA. Just as ESG-related exclusions and climate stress scores are now factored into insurer credit profiles, so too could resilience to grey-zone disruption become a differentiator. In a world where state-contested infrastructure and systemic cyber fragility are no longer future risks but current realities, the ability of a carrier to demonstrate structured response, via PHA wording or otherwise, becomes a signal of operational sophistication, not marginal deviation.

In parallel, sovereign engagement will be necessary, particularly where government risk pools, national resilience strategies, or critical infrastructure protection policies intersect with the insurance market. The UK's National Security Strategy (2025) and Defence Industrial Strategy Refresh (2024) both acknowledge the centrality of private sector resilience to national defence objectives ([11], [12]). If commercial insurers are to continue operating in contested environments, they must do so in concert with sovereign planning, not in its wake.

1 Joint Design Panels

Involving carriers, regulators, and state security agencies, to pre-validate corridor designations or disruption thresholds for PHA activation.

2 Standardised Disclosure Templates

Allowing insurers to report PHA exposure, risk mitigation strategies, and policy wording innovation in a format intelligible to supervisors and ratings agencies.

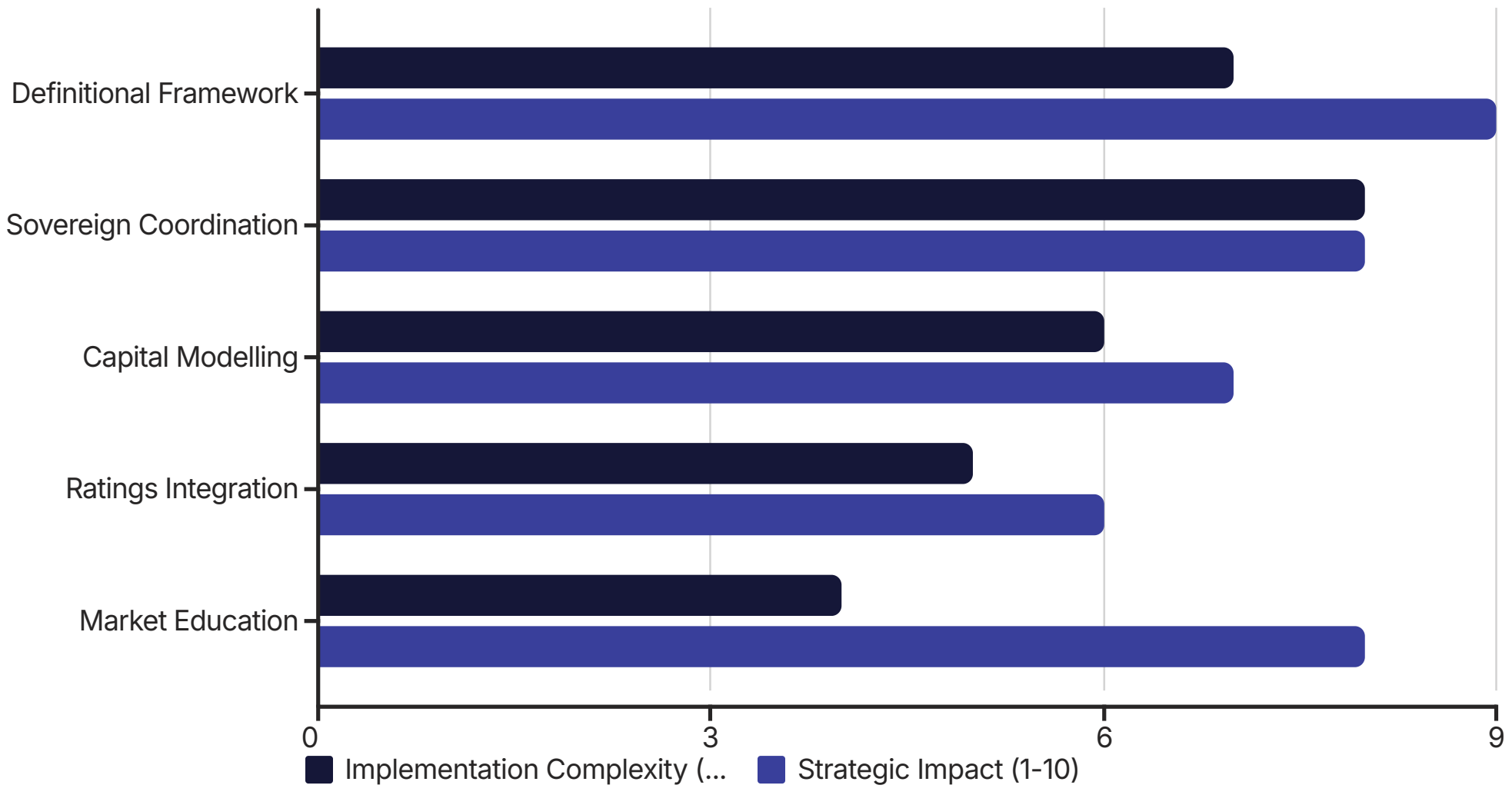
3 Reserve Treatment Protocols

Clarifying whether and how PHA-triggered liabilities may be held or reinsured, particularly where attribution is partial or politically sensitive.

4 Reinsurance and Pooling Mechanisms

Enabling capital aggregation and capacity provision for PHA without distorting core war or cyber markets. This may involve hybrid treaties or regionally defined event baskets.

Such steps are not without precedent. The terrorism reinsurance market, post-2001, evolved precisely through the interaction of regulatory expectation, sovereign coordination, and underwriting innovation. What PHA demands is a similar moment of institutional realism, a recognition that ambiguity is no longer a transient problem, but a structural feature of the threat environment.



This is not a call for bureaucratic expansion. It is an argument for institutional preparedness. The sooner PHA is rendered legible to regulators and capital markets, the sooner it can be priced, modelled and adapted, not in the shadow of disruption, but in anticipation of it.

10. Conclusion: Designing for Strategic Continuity

The strategic utility of insurance has always rested on its ability to underwrite confidence. Not merely in the transactional sense of financial indemnity, but in the broader assurance that continuity can be sustained, even when risk materialises. This function remains essential, but the conditions under which it must now operate have shifted.

Persistent Hostile Activity (PHA), as defined through the flashpoints and operational evidence of the first half of 2025, is not a new form of warfare. Nor is it a temporary aberration. It represents a deliberate and structured strategy, employed by adversaries who understand that ambiguity, latency and contestation below the threshold of war offer a more sustainable means of achieving strategic effect. Their actions target not the instruments of combat, but the systems of function. Navigation. Commerce. Communication. Supply.

Resilience

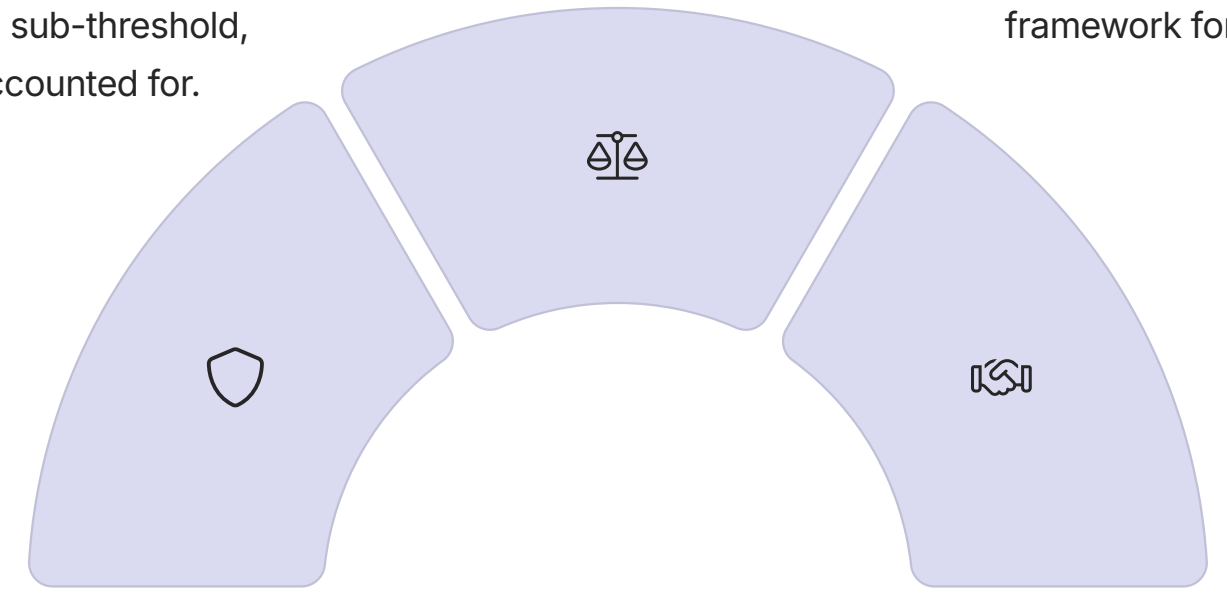
Insurance provides not just recovery, but deterrence, by signalling that disruption, even when sub-threshold, will not be left unaccounted for.

Continuity

The market's ability to structure response, not simply react to declaration, becomes a core enabler of commercial and strategic continuity.

Partnership

Closer coordination between insurers, states, and security agencies creates a more robust framework for managing persistent threats.



What is disrupted is not only infrastructure, but trust, in operating environments, in institutional responses and in the mechanisms that allocate risk. For the insurance sector, this is not simply a challenge of product design. It is a question of strategic posture. Whether the market remains reactive to declared events, or adapts to the ambient patterns through which disruption now occurs.

The introduction of PHA as a named peril offers a path forward. It does not require the abandonment of existing clauses, nor the erosion of legal rigour. It proposes a parallel logic, one designed not for certainty, but for continuity. A logic that reflects how adversaries now shape risk and how insurers might respond in a way that preserves coverage legitimacy without demanding attribution that may never arrive.

This is not an easy shift. It requires investment in new forms of modelling, closer coordination with state actors and a willingness to operate in domains that do not conform to traditional actuarial assumptions. But it is necessary. Without such adaptation, the market will continue to contract away from areas that are strategically vital, precisely when resilience is most required.

What is at stake is more than commercial opportunity. Insurance remains one of the few mechanisms through which the private sector can participate meaningfully in national and systemic resilience. It offers not just recovery, but deterrence, by signalling that disruption, even when sub-threshold, will not be left unaccounted for.

As the strategic environment becomes more contested, the ability of insurers to structure response, not simply react to declaration, becomes a core enabler of continuity. In this, the market has a choice. It can define the grey zone as uninsurable. Or it can render it legible, structured and ultimately navigable.

This paper has sought to offer the foundations of that latter path. Not as a definitive answer, but as a design hypothesis, grounded in operational fact, doctrinal insight and the conviction that ambiguity, while inconvenient, is not insurmountable. Strategic continuity will not emerge by waiting for certainty. It will come from building systems that can operate in its absence and pricing risk accordingly.

References

Grey Zone Flashpoints and Operational Sources

1. EASA Issues Safety Warning on Baltic GPS Interference European Union Aviation Safety Agency (EASA), 16 January 2025 https://www.easa.europa.eu/en/newsroom-and-events/news/easa-issues-safety-warn ing-gps-interference-baltics
2. Lithuania Says GPS Jamming by Russia Will Likely Persist Even After Ukraine War Reuters, 23 January 2025 https://www.reuters.com/world/europe/lithuania-says-gps-jamming-by-russia-will-likel y-persist-even-after-ukraine-war-2025-01-23/
3. U.S. and UK Conduct Retaliatory Strikes on Houthi Targets in Yemen BBC News, 5 April 2025 https://www.bbc.co.uk/news/world-middle-east-68719862
4. Operation Rough Rider: How U.S. and UK Have Hit Houthi Missile and Drone Sites Al Jazeera, 8 April 2025 https://www.aljazeera.com/news/2025/4/8/operation-rough-rider-targets-houthi-capab ilities
5. Houthi Rebels Announce Temporary Ceasefire with U.S., Continue Hostilities Against Other States The Guardian, 2 May 2025 https://www.theguardian.com/world/2025/may/02/houthi-ceasefire-us-maritime-securi ty
6. Ships Use Fake AIS Signals to Avoid Attacks in Hormuz Strait Lloyd's List, 19 June 2025 https://lloydslist.maritimeintelligence.informa.com/LL1159872/Ships-Use-Fake-AIS-Si gnals-to-Avoid-Attacks
7. Frontline Suspends Tanker Contracts in Hormuz over "Unpredictable Grey Zone Conditions" Financial Times, 22 June 2025 https://www.ft.com/content/8b1e7c3d-d1c7-49ea-bd7e-acc6c4ecf3f4
8. Litigation Tracker: NotPetya and SolarWinds Coverage Challenges in 2025 Law360 Cyber Risk Bulletin, 17 May 2025 https://www.law360.com/cybersecurity/articles/1834529/notpetya-solarwinds-coverag e-cases-2025

Institutional and Doctrinal Sources

9. UK Strategic Defence Review: Making Britain Safer HM Government, 2025
10. Supervisory Statement SS1/21 – Operational Resilience: Impact Tolerance Bank of England / Prudential Regulation Authority, updated 2023 https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operat ional-resilience-impact-tolerance-ss
11. UK National Security Strategy 2025 HM Government, Cabinet Office, 2025
12. UK Defence Industrial Strategy Refresh (MOD, 2024) Ministry of Defence, 2024