Invisible Conflict: The Rise of Silent Strategic Warfare

Published: Ambient Stratagem

July 2025

Contents

Preface

The strategic landscape is undergoing a transformation, subtle in form but significant in consequence. What was once considered preparatory activity has matured into a distinct mode of conflict. Cyber operations, narrative distortion, and economic coercion now operate not as precursors to war but as instruments of national policy in their own right. These are not abstract threats. They are being deployed, deliberately and continuously, by actors whose doctrine privileges ambiguity, deniability, and systemic pressure.

This paper does not suggest that conventional military force has been displaced. Rather, it asserts that the environment in which force is applied is increasingly being shaped in advance, through operations that fall below traditional thresholds of warfare but achieve tangible strategic effect. The grey zone is no longer a transitional space between peace and war. It is the arena in which modern strategic competition plays out daily.

Drawing upon documented incidents from June 2024 to June 2025, this white paper synthesises the emerging architecture of silent strategic warfare. The analysis is grounded in observed adversary actions and doctrinal developments. It avoids speculation, favouring evidence drawn from credible, traceable sources. Its purpose is not alarm but clarity: to outline how silent operations are evolving, what risks they pose to sovereign resilience, and what adjustments may be required in defence and security doctrine.

This is not a manifesto. It is a strategic briefing in written form, deliberate, substantiated, and aligned with the responsibilities of those charged with safeguarding national and allied interests in a contested age.

Executive Summary

This white paper addresses the rise of silent strategic warfare, a form of state-aligned, non-kinetic conflict involving cyber disruption, narrative manipulation, and economic coercion. These activities are not confined to the margins of security policy; they are being deployed deliberately to shape the operational environment before conventional escalation occurs. The evidence is now substantial, and the doctrinal signals from adversaries are increasingly explicit.

From China's establishment of the PLA Cyberspace Force in April 2024, tasked with offensive cyber operations and psychological warfare【1) , to Russia's ongoing sabotage and influence campaign across Europe【2】, state actors are using silent pressure to weaken cohesion, test defences, and prepare the battlespace. Iran's cyber interference with maritime infrastructure【3】 and covert Israeli drone sabotage enabling precision strikes【4】 illustrate that these tactics are not limited to the information domain, they directly affect physical outcomes.

Non-kinetic shaping has become an institutionalised first move, not a contingency

Adversaries are systematically deploying cyber, narrative, and economic pressure as standard doctrine rather than exceptional measures.

Attribution ambiguity is used to suppress deterrence and delay response

Operations are designed to frustrate clear attribution, creating uncertainty that inhibits timely and proportionate countermeasures.

Narrative control is doctrinal, not decorative, particularly in Russian and Chinese practice

Information operations are treated as primary battlespace shaping rather than supplementary messaging.

Hybrid precision operations now fuse cyber and kinetic effects, often without declaration

Non-kinetic tools are increasingly integrated into conventional military operations as enablers and force multipliers.

Resilience must be reframed as a deterrent posture, not simply a recovery function

The ability to withstand and operate through disruption becomes a strategic signal that deters adversary action.

Importantly, many of these actions fall below formal thresholds of armed conflict. Yet they consistently yield strategic effects: degrading trust, delaying response, and eroding the clarity of escalation boundaries. The adversary advantage lies in coordination. Operations are synchronised across cyber, narrative, and economic fronts, whereas Western responses remain fragmented, reactive, and often siloed by domain or mandate.

The paper concludes that current doctrinal frameworks must be recalibrated. Silent warfare is not merely a prelude, it is a permanent feature of contemporary strategic competition. The requirement is not escalation, but pre-emptive clarity: of posture, of narrative, and of sovereign authority to act within the ambiguous space now actively contested.

Section 1: From Kinetics to Control – The Strategic Role of Silent Pressure

1.1 Introduction

The past decade has seen a subtle but significant transition in the way conflict is prepared, prosecuted, and perceived. Kinetic operations remain central to national defence strategies, but the conditions in which they occur are increasingly shaped by non-kinetic action. Where physical terrain once dominated military doctrine, the contested domains of information, cyberspace, and economic systems now act as the true first movers of confrontation. This shift has not occurred overnight, nor is it yet universally doctrinally codified, but it is visible in the structure and behaviour of those actors most committed to leveraging ambiguity and disruption for strategic advantage.

This section explores the increasing institutionalisation of what might be termed "silent pressure", a form of state-aligned, non-kinetic shaping that blurs the threshold between peace and conflict. The analysis draws on recent examples from China, Russia, and Iran, where formal doctrine and operational practice reveal a coordinated approach to infrastructure disruption, psychological operations, and economic coercion. These actions are not isolated provocations. They are strategic acts in their own right, designed to shape outcomes well before a formal escalation occurs.

1.2 Institutionalising the Pre-Kinetic Domain – The PLA Cyberspace Force

A striking example of the institutionalisation of silent warfare is the People's Republic of China's decision to establish the PLA Cyberspace Force as a standalone command in April 2024. This restructuring removed cyber operations from the broader Strategic Support Force (SSF) and granted them independent strategic authority, with mission sets including offensive cyber, defence of cyber sovereignty, and psychological operations【1】.

Doctrinally, this move signals that cyberspace is no longer treated as a supporting capability, it is a warfighting domain with its own tempo, targets, and rules of engagement. In PLA thinking, cyber operations are intended not just to disable systems but to exert pressure at scale across societal and economic layers. Their official statements indicate a preoccupation with shaping public cognition, disrupting adversary command structures, and asserting control over the narrative environment. Crucially, the Cyberspace Force is positioned not to react to external threats, but to act proactively, setting conditions, generating dilemmas, and testing adversary thresholds before conventional forces are engaged.

This reorganisation reflects an increasingly common pattern among authoritarian systems: formalising non-kinetic capabilities into integrated structures, with defined missions, legal justifications, and centralised control. Such moves embed ambiguity into doctrine, allowing states to act decisively in domains where attribution is difficult and response cycles are slow.

1.3 The Russian Model – Synchronised Sabotage as Strategic Routine

Russia's approach differs in structure but not in intent. Over the past year, the Russian state and affiliated actors have conducted a series of hybrid operations across Europe that combine sabotage, disinformation, and psychological manipulation. These include the May 2024 arson attacks on retail outlets in Warsaw, the June 2024 disinformation stunt involving mock coffins near the Eiffel Tower, and the December 2024 sabotage of undersea communication cables near the UK and Baltic states【2】.

While these incidents are often treated as discrete events in the media, a doctrinal reading places them within a strategic rhythm. Russian grey-zone operations are not necessarily designed to cause immediate material damage. Rather, they are intended to impose cost, create friction, and normalise disruption. Their hallmark is plausible deniability, but the effects are cumulative. In aggregate, such actions erode institutional trust, divert resources, and soften the informational terrain in advance of more overt acts of coercion.

Importantly, these are not purely opportunistic events. Reporting from Geopolitical Monitor and the open-source timeline compiled by Wikipedia indicate sustained coordination between state entities such as the GRU and a constellation of proxy groups and criminal intermediaries【2】. This networked structure enables rapid response and persistent pressure, while insulating Moscow from direct attribution. The effect is doctrinal: Russia has, through practice if not formal publication, operationalised hybrid disruption as a standing element of statecraft.

1.4 Economic Systems as Pressure Points – The Iranian Maritime Campaign

Iran's behaviour in the Gulf region provides a parallel example of non-kinetic strategic action aimed at economic systems. In March 2025, the cyber group LabDookhtegan, widely attributed to Iranian state alignment, conducted signal jamming and network disruption that affected over 100 maritime platforms, including commercial ships and offshore oil infrastructure【3】. The operation did not result in physical destruction, yet it triggered significant economic and logistical repercussions.

The maritime domain is particularly susceptible to this form of silent pressure. Communication networks, positioning systems, and data relays are critical to both civilian and military operations, yet their defence is often fragmented across commercial providers and international regulatory bodies. Iran's actions exploited this seam, demonstrating that cyber interference can achieve cost imposition, strategic messaging, and economic leverage without triggering overt military response.

Iranian doctrine has long incorporated concepts of asymmetric disruption, particularly in response to superior conventional forces. However, what is notable in this instance is the degree of coordination and the targeting of infrastructure with high economic and geopolitical value. The campaign functioned as both a demonstration of capability and a form of strategic signalling, projecting risk into a vital trade corridor and influencing regional posture without open confrontation.

1.5 Implications for Western Doctrine

How should existing doctrine treat non-kinetic acts that precede traditional conflict but still achieve strategic effect?

Western frameworks must evolve to recognize and respond to actions that fall below traditional thresholds yet deliver significant impact.

What mechanisms exist, or need to be built, to detect, attribute, and deter such actions without inadvertently escalating conflict?

New capabilities for rapid attribution and proportionate response must be developed within existing legal and ethical constraints.

How can democracies, with their decentralised decision-making and pluralistic media environments, organise themselves to remain resilient?

Democratic systems must find ways to maintain their values while developing the speed and coherence needed in contested information space.

Each of these examples, Chinese restructuring, Russian hybrid campaigns, Iranian maritime disruption, points to a shared understanding among adversaries: the shaping of strategic outcomes no longer begins with force projection. It begins with system-level interference, often executed silently, but always with intent.

For Western militaries and policymakers, this raises pressing questions. These are not rhetorical inquiries. They point to foundational challenges in how liberal democracies conceptualise threat, assign responsibility, and maintain deterrence in a world where strategic pressure may be applied silently, asymmetrically, and continuously.

References (for Section 1):

[1] People's Liberation Army Cyberspace Force, established April 2024. Summary overview: Wikipedia, corroborated by Jamestown Foundation briefings.

[2] Russian hybrid warfare in Europe, incidents spanning May 2024 – June 2025. Timeline: Wikipedia; strategic overview: Geopolitical Monitor.

[3] Cyberwarfare and Iran, LabDookhtegan maritime signal interference, March 2025. Incident overview: Wikipedia.

Section 2: Hybrid Precision – When Cyber Becomes a Combat Enabler

2.1 Introduction

Silent operations are often conceptualised as acts of interference, cyber intrusions, disinformation campaigns, or low-grade economic pressure. Yet an emerging pattern suggests that these tools are increasingly being employed not only to disrupt or distract, but to enable. Specifically, to set the conditions for precision kinetic strikes, tactical dominance, or strategic surprise. When used in this way, non-kinetic tools cease to be background activity and become active components of military effect.

This section examines three recent examples where cyber and covert digital operations have functioned not as standalone gestures, but as tightly integrated enablers of more traditional forms of state action. These operations reflect a shift in adversary posture, from experimentation to standardisation and underscore the challenge of preserving escalation control in a battlespace where sequencing is deliberately obscured.

2.2 The Israeli Model – Pre-Strike Sabotage in the Shadows

In June 2025, Israeli forces conducted a series of targeted airstrikes on Iranian missile and air defence infrastructure. What made these strikes notable was not their precision alone, but the fact that they followed and were reportedly enabled by a covert sabotage operation conducted via drones attributed to Mossad【4】.

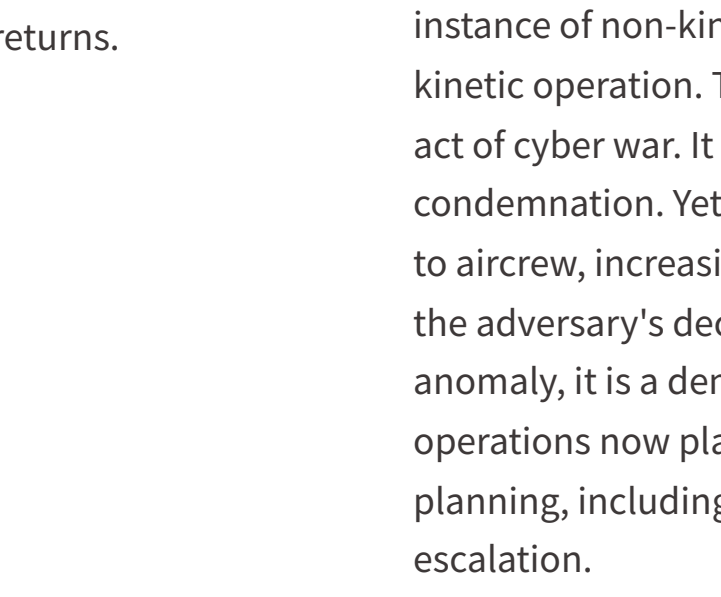
According to multiple open-source briefings and regional reporting, small aerial platforms were used to interfere with air defence radar arrays and command nodes shortly before the kinetic phase commenced. The drones are understood to have either disabled key nodes or introduced logic interference within air surveillance systems, creating blind spots or false returns.

From a doctrinal perspective, this represents a clear instance of non-kinetic shaping integrated directly into a kinetic operation. The operation was not framed as an act of cyber war. It attracted no international condemnation. Yet its effect was decisive: reducing risk to aircrew, increasing target fidelity, and compressing the adversary's decision-making window. This is not an anomaly, it is a demonstration of the role silent operations now play in the full spectrum of combat planning, including at the most sensitive threshold of escalation.

2.3 Operation Sindoor – Multimodal Retaliation by Design

Drone Swarms

Pre-programmed aerial platforms conducted surveillance, suppression, and tactical harassment across the border.



Cyber Disruption

Targeted operations against Pakistani communication infrastructure degraded command and control capabilities.

Narrative Campaign

Coordinated information operations sought to isolate Pakistani state legitimacy regionally and internationally.

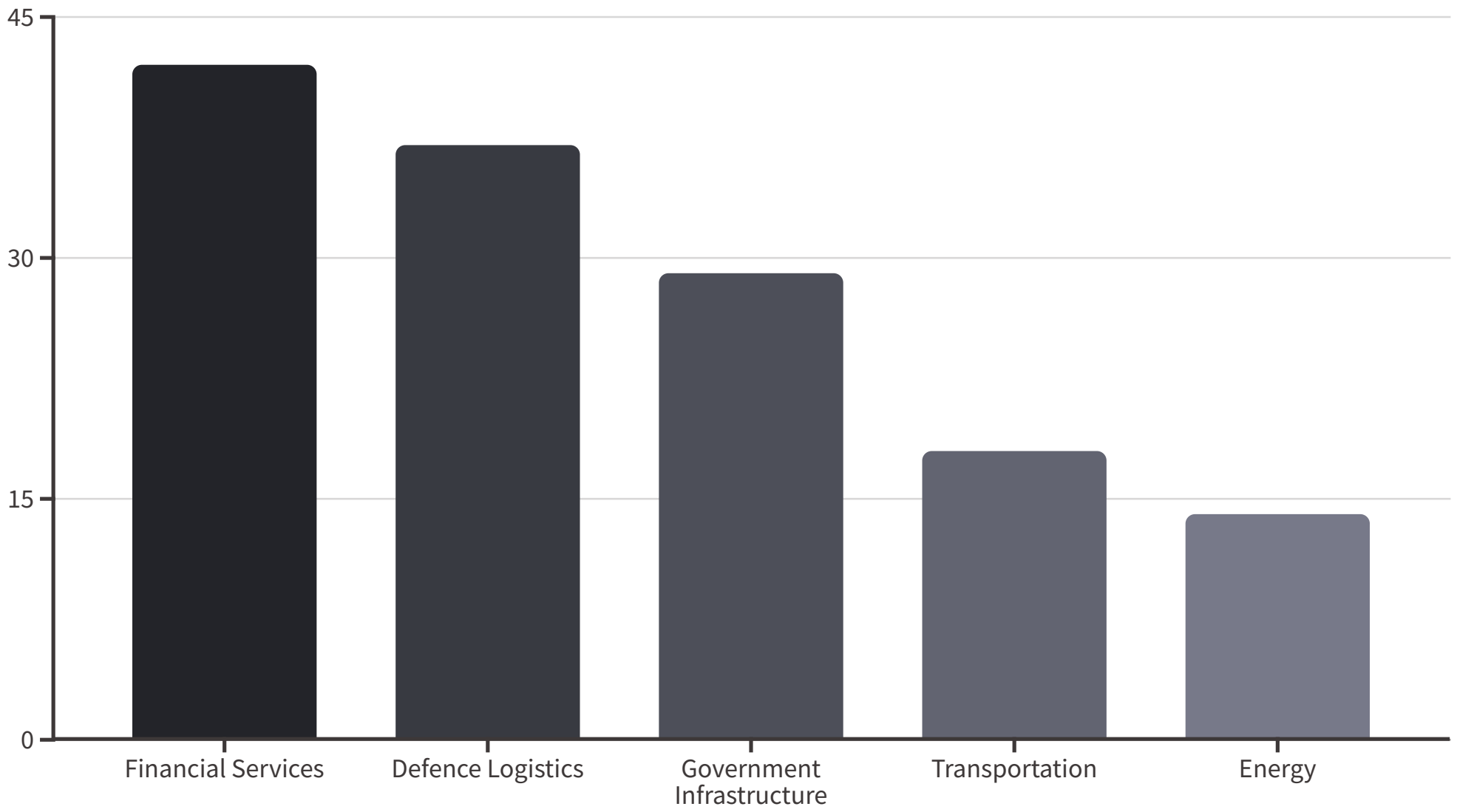
A similarly structured campaign occurred the previous month during India's Operation Sindoor, launched in response to a mass-casualty terrorist attack originating from across the Pakistan border. The operation employed swarms of drones, coordinated cyber disruption, and disinformation counter-campaigns【5】. Reports indicate that cyber operations were conducted against key Pakistani communication infrastructure, while drone swarms, likely pre-programmed with battlefield logic, conducted surveillance, suppression, and tactical harassment.

This was not a case of cyber as retaliation. Nor was it simply a technological upgrade to conventional doctrine. It was a fusion of effects. The cyber component disrupted response coordination; the drone component filled targeting and ISR gaps; the narrative campaign sought to isolate Pakistani state legitimacy in the region and internationally.

What is doctrinally significant here is the coherence of intent. Each domain was brought to bear in sequence and in synchrony, not simply in parallel. This reflects a level of integration more commonly associated with Western joint targeting frameworks but executed in a sub-threshold, rapid-turnaround context. It suggests that hybrid precision is no longer the preserve of advanced NATO allies, and that operational fluency across domains is a spreading norm.

2.4 Hacktivist Interference – Strategic Disruption via Proxy

Not all enablers wear state insignia. In June 2025, a surge of DDoS attacks targeting U.S. defence-linked sectors was observed, attributed to nationalist-aligned hacktivist groups including Mysterious Team Bangladesh, Mr. Hamza, and Keynous+【6】. The attacks disrupted financial services, defence logistics providers, and parts of government infrastructure. While the attacks were not complex in technical terms, they achieved a measurable effect: operational friction at scale.



These groups operate in a doctrinal grey area. They claim ideological independence, yet their targeting consistently aligns with the strategic interests of states such as Iran, Russia, and others. Whether acting under explicit direction or implicit encouragement, they represent a form of distributed strategic pressure that states can deploy or endorse without assuming the burden of attribution or response.

What is notable in this instance is the temporal alignment. The spike in attacks occurred shortly after high-profile international incidents involving Iran—suggesting a supportive or retaliatory function. In doctrinal terms, this indicates that even loosely affiliated cyber actors can form part of a broader enabling fabric, softening or signalling ahead of state action. Western doctrine, which tends to treat such actors as security anomalies, may need to adapt to treat them instead as semi-integrated elements within hostile strategic architectures.

2.5 The Shift from Tools to Tactics

Across these examples, covert sabotage, integrated multimodal retaliation, and proxy interference, a shared logic is visible. Cyber and silent tools are not being used merely to support kinetic operations. They are being integrated into their design. This suggests a doctrinal maturity among adversaries who increasingly understand that the conditions of battle are not just physical, but cognitive, temporal, and systemic.

This has implications for force design, campaign planning, and legal thresholds. The use of silent enablers complicates traditional sequencing. Attribution may lag effect. Political decision cycles may outpace operational tempo. More concerningly, the very notion of "first strike" becomes ambiguous if the environment has already been shaped, silently, but decisively.

In UK doctrine, the integration of cyber and kinetic effects is acknowledged, but often still bounded by domain and legality considerations. Adversaries appear to take a different approach, function over form, effect over domain. This does not suggest recklessness. Rather, it reflects a different calibration of strategic risk and reward. The effect is a growing asymmetry in readiness, speed, and cohesion across the non-kinetic spectrum.

2.6 Conclusion

Hybrid precision is not an emerging trend, it is an observed reality. Non-kinetic operations are now being used not only to degrade or disrupt, but to direct and enable kinetic action. The line between preparatory interference and operational effect is increasingly permeable. States such as Israel, India, and others are demonstrating what this integration looks like in practice. Proxy groups add further texture, complicating deterrence and amplifying friction.

For UK and allied planners, the implications are doctrinal and operational. Integration of cyber, narrative, and electronic warfare cannot remain aspirational. It must be structured, trained, and exercised as part of the routine rhythm of force employment, even in scenarios that fall short of open conflict. The capacity to operate in and through ambiguity, with clarity of purpose and tempo of action, will define strategic advantage in the decade ahead.

[4] June 2025 Israeli operations in Iran, including covert drone sabotage and airstrike sequencing. Open-source aggregation: Wikipedia.

[5] India's Operation Sindoor, multimodal retaliation including drone swarms, cyber, and information operations. Sources: Economic Times, Financial Times.

[6] Hacktivist-led DDoS spike, targeting U.S. infrastructure. Attribution to nationalist-aligned groups. Source: TechRadar.

Section 3: Narrative as Battlespace – The Doctrinal Divide

3.1 Introduction

In any strategic contest, control over perception can be as consequential as control over terrain. Yet in much of Western doctrine, the information environment continues to be treated as a supplementary concern, part of strategic communications or public affairs, but not a decisive domain of action in its own right.

Adversary doctrine takes a different view. Russia, China, and to varying degrees, Iran and other actors, treat the narrative space as a central theatre of operations. Influence is not a by-product; it is a primary objective. This divergence in conceptual approach is not merely academic. It is producing operational asymmetries with tangible effects in deterrence, decision tempo and societal resilience.

This section draws on NATO's internal analysis of cyber and influence operations during the 2024–25 window, and contrasts that assessment with observed Russian campaigns across Europe. The picture that emerges is not one of Western incapacity, but of doctrinal fragmentation, an absence of campaign-level integration in a space where adversaries operate with coherence, synchronisation and strategic patience.

3.2 NATO's Diagnosis – Fragmentation in the Face of Synchrony

In September 2024, NATO published DEEP Dive Vol. 1, an internal diagnostic on Allied cyber and influence posture【7】. While recognising technical progress across several member states, the report highlighted a critical structural weakness: the absence of unified narrative design across campaigns. Information operations were described as reactive, inconsistent, and often divorced from broader strategic intent. Cyber capabilities existed, but without narrative coordination, their effects remained ephemeral.

This is not a criticism of technical capability. Rather, it reflects the challenge of operating in an alliance structure where national mandates, legal constraints, and cultural norms differ markedly. In such an environment, narrative cannot easily be centralised, but it must still be synchronised.

NATO's findings show that while Russian activities remained persistent and directionally consistent, Allied counter-efforts were fragmented. In some instances, cyber responses were deployed without accompanying public messaging. In others, disinformation campaigns were addressed only after they had shaped perception among target audiences. The delay between action and counter-narrative often ceded the informational initiative to adversaries.

3.3 The Russian Approach – Distortion as Doctrine

1 — May 2024: Warsaw Arson

Coordinated attacks on retail outlets, attributed to "local extremists" but linked to Russian proxies.

2 — June 2024: Eiffel Tower Disinformation

Mock coffins placed near landmark, creating viral images suggesting French military casualties.

3 — December 2024: Undersea Cable Sabotage

Physical damage to communication infrastructure near UK and Baltic states, causing service disruptions.

By contrast, Russia has treated the information domain as a precondition to all other forms of engagement. The now well-documented hybrid campaign across Europe, spanning 2022 to 2025, demonstrates a sustained commitment to narrative operations【2】. Events such as the May 2024 Warsaw arson, the June 2024 Eiffel Tower disinformation stunt, and the repeated sabotage of undersea cables are not merely tactical disruptions. They are narrative interventions, designed to signal, distort, and destabilise.

The strategic value lies not in the incident itself, but in its interpretation. Each act is seeded into the media environment with plausible deniability, then amplified through aligned or opportunistic voices. The intended effect is disorientation: to erode the distinction between fact and fabrication, state and proxy, attack and accident.

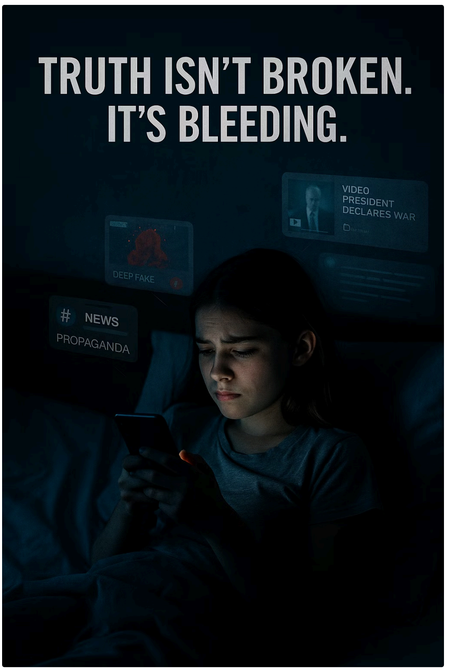
This is consistent with published Russian military thought, including General Gerasimov's earlier articulation of "information confrontation" as a foundational component of modern conflict. In this framework, victory is not defined solely by territorial gain or military success, but by the adversary's internal disintegration, socially, cognitively, and politically.

Western responses often struggle to contend with this framing. Without a clear attribution trail or physical damage, the instinct is to de-escalate or ignore. But over time, these unchallenged incursions accumulate, undermining the credibility of institutions, the trustworthiness of media, and the responsiveness of policy.

3.4 Weaponised Ambiguity – The Challenge for Open Societies

The difficulty in countering adversarial narrative operations is not simply technological, it is structural. Open societies are designed to tolerate disagreement, enable free expression, and resist centralised control over information. These are strengths in democratic governance, but they are friction points in contested information space.

Adversaries exploit this openness by inserting uncertainty into already crowded information environments. In such settings, ambiguity is not a bug, it is a feature. The objective is not to persuade, but to overwhelm. As clarity dissolves, confidence in decision-making weakens. This creates space for further intrusion, digital, economic, or otherwise, under the cover of noise. For Western states, the instinct has been to respond with transparency and fact-based rebuttal. While ethically sound, this approach is often too slow to reframe perception once seeded. Narrative dominance is not secured by facts alone. It is maintained by tempo, tone, and trust, each of which must be cultivated ahead of crisis, not during it.



NATO's findings acknowledge this. Without coordinated narrative pre-positioning, even the most sophisticated cyber or kinetic actions can be perceived as unprovoked or disproportionate, undermining legitimacy in the very audiences those operations are meant to protect.

3.5 Doctrinal Implications – From Communication to Campaigning

Adversary Approach

For Russia and, increasingly, China, narrative is a domain to be contested with the same seriousness as air or land. Information operations are integrated into campaign planning from the outset.

Western Approach

For many Western actors, narrative remains tied to reputational management, public affairs, or institutional messaging, often as an afterthought to operational planning.

Operational Asymmetry

Adversaries prepare the narrative environment long before events unfold. They signal intent obliquely, frame outcomes in advance, and shape the interpretive lens through which actions will be viewed.

Required Evolution

Narrative operations must be elevated within Western defence and security frameworks, with intentional design, doctrinal integration, and operational authority.

The divergence in doctrine between NATO and its adversaries is not rooted in capability but in conceptual alignment. This gap creates operational asymmetries. Adversaries prepare the narrative environment long before events unfold. They signal intent obliquely, frame outcomes in advance, and shape the interpretive lens through which their actions and ours will be viewed.

To address this, narrative operations must be elevated within Western defence and security frameworks. This does not mean adopting the tools or tactics of authoritarian regimes. It means recognising that strategic effect in the information domain requires intentional design, doctrinal integration, and operational authority.

Campaigns that begin in cyberspace or covert space will inevitably be judged in public space. Without narrative coherence, deterrence risks being misunderstood, and resolve misread. The consequences of such misalignment are visible across multiple recent theatres, where actions taken for defence are interpreted as escalation, and silence mistaken for weakness.

3.6 Conclusion

Narrative is not the consequence of conflict. It is its context. In modern grey zone operations, adversaries use narrative not as decoration, but as a means of shaping the conditions under which all other domains operate. The battlefield of perception is structured, persistent, and increasingly decisive.

For Western doctrine to remain effective, it must absorb this reality, not through mimicry, but through adaptation. Strategic communication must evolve into narrative campaigning. Cyber operations must be embedded within interpretive frameworks. Decision-makers must be equipped not only with facts, but with the authority to act within the ambiguity adversaries exploit.

In the invisible conflict, the fight for narrative clarity is not optional. It is foundational.

References (for Section 3):

[2] Russian hybrid warfare in Europe, May 2024 – June 2025 operations including arson, sabotage, and narrative stunts. Sources: Wikipedia; analysis: Geopolitical Monitor.

[7] NATO DEEP Dive Vol. 1, September 2024. Analysis of NATO-aligned cyber and narrative campaign coherence. Document: deepportal.hq.nato.int

Section 4: Resilience as Deterrence – Beyond Technical Defence

4.1 Introduction

Resilience has long been understood as a defensive posture, a society or system's capacity to absorb shocks and return to functional baseline. But in the context of silent strategic warfare, this framing is no longer sufficient. When adversaries employ continuous, coordinated, and deniable forms of disruption across cyber, economic, and narrative domains, resilience becomes more than a matter of recovery. It becomes a form of deterrence in its own right, signalling preparedness, denying strategic reward, and preserving freedom of action under pressure.

This section argues for a recalibration of resilience as a doctrinal tool. It draws on recent developments in UK policy, as well as operational lessons from adversary behaviour. In doing so, it offers a strategic framing in which resilience is not merely the shield after impact, but part of the posture that shapes adversary calculus before action is taken.

4.2 The UK Posture Shift – Resilience as Active Discipline

In May 2025, the UK Defence Secretary, John Healey, announced the creation of an integrated cyber, electronic warfare, and AI-enabled operations command, supported by a £1 billion investment into what was termed a "digital targeting web"【8】. The move coincided with public commitment to expanding the UK's capacity for offensive cyber operations, positioning cyber not simply as a defensive perimeter, but as a tool of pre-emptive effect.

This announcement should be understood not merely as a policy update, but as a shift in posture. For much of the previous decade, the UK, alongside most NATO members, framed cyber defence through the lens of critical infrastructure protection and reactive forensics. What is now emerging is a broader doctrine in which resilience includes the capacity to counter-shape the environment, to detect early, act pre-emptively, and operate with continuity even under hostile conditions.

Resilience, in this model, is not about eliminating vulnerability. It is about creating conditions in which adversary action is frustrated by design, technically, procedurally, and psychologically. The value lies not only in surviving attack, but in rendering certain forms of attack strategically futile.

4.3 Strategic Function of Resilience in Silent Warfare

Resilience in the context of silent warfare is not a singular capability. It is a system of systems, comprising detection, coordination, authority, and trust. Each of these components plays a role in denying adversaries the outcomes they seek from ambiguous, non-attributable action.

Take, for example, Iran's disruption of maritime communications in March 2025. Through signal jamming and interference with satellite communications, Iran affected more than 100 ships and offshore energy platforms【3】. The operation did not breach international law in a formal sense, nor did it provoke immediate retaliation. Yet its impact on economic throughput and maritime logistics was measurable.

Had resilience in this context been framed purely as system redundancy or patch management, the disruption would still have achieved its intended effect. What is required is a layered response capability: maritime operators aware of hostile EW activity, communication pathways that prioritise continuity under denial, and sovereign authority to respond proportionately in the face of ambiguous attack.

This points to a broader insight: resilience in the silent domain is a signalling mechanism. It communicates to adversaries not just that systems can recover, but that attacks will fail to achieve political or operational effect. It is this perception, of readiness, frictionlessness, and continuity, that deters.

4.4 Adversary Observations – Targeting the Seams

Adversary doctrine increasingly exploits the seams of Western governance. Where functions are distributed across public, private, and regulatory actors, attackers find opportunities to impose cost without breaching sovereign red lines. This is a defining feature of Russian grey zone operations, where undersea cable sabotage, proxy-led arson, and influence operations target infrastructure and social cohesion simultaneously【2】.

The strategic logic is not to destroy capacity outright, but to erode confidence in continuity. By injecting friction into transport, communications, or energy systems, even temporarily, adversaries hope to demonstrate systemic fragility. This is not incidental. It is the operationalisation of silent warfare through economic and infrastructural vectors.

From the attacker's perspective, fragmented responses validate this approach. When defence is siloed, cyber in one department, resilience in another, legal authority in a third, the result is a delayed or diluted countermeasure. The absence of coordinated resilience creates space for repeated intrusion without escalation. The message received is not simply that systems were breached, but that they were breach-able.

4.5 Civil Domain as a Strategic Theatre

Resilience also extends beyond government and defence. Silent warfare operates through and against civilian systems, logistics chains, hospitals, energy providers, financial intermediaries. Many of these entities are governed not by deterrence logic, but by commercial incentive or regulatory compliance.

800%

DDoS Attack Increase

Spike in distributed denial of service attacks against U.S. financial and defence-linked sectors in June 2025

100+

Maritime Platforms

Number of vessels and offshore energy platforms affected by Iranian signal jamming in March 2025

£1B

UK Investment

Funding allocated to the UK's "digital targeting web" for integrated cyber, EW, and AI operations

This makes them ideal pressure points in a silent conflict. When hacktivist groups aligned with state interests targeted U.S. financial and defence-linked sectors with an 800% spike in DDoS attacks in June 2025, their objective was not destruction but disruption【6】. They aimed to impose delay, generate uncertainty, and signal vulnerability at scale. These forms of disruption do not require advanced capabilities, only coordination, opportunity, and a target set spread across soft infrastructure.

The lesson is clear: resilience cannot be the sole responsibility of national security institutions. It must be designed as a distributed discipline, with delegated authority, rehearsed continuity procedures, and shared visibility across sectors. This includes public education, regulatory mandates, and operational frameworks that allow civilian operators to function confidently under stress.

4.6 Deterrence by Continuity

In conventional deterrence theory, the emphasis is often on punitive response, making the cost of attack outweigh any potential gain. But in the grey zone, where attribution is complex and timelines are compressed, the most effective form of deterrence may be denial of effect.

If adversaries understand that infrastructure will continue to function, that narratives will remain coherent, and that institutions will respond without delay or confusion, the logic of silent attack becomes less compelling. Deterrence is achieved not through threat, but through clarity of resilience. This is not a passive posture. It is an operational discipline with active requirements, monitoring, rehearsals, scenario modelling, and real-time decision-making across domains.

This recalibration aligns with lessons from adversary practice. China's doctrinal emphasis on "informatized warfare" includes the ability to shape and exploit system-level dependencies. Russia's persistent infrastructure testing demonstrates a belief that societal friction can be weaponised. Iran's maritime disruption illustrates that ambiguity can still achieve effect when resilience is partial.

For Western democracies, then, the challenge is not to match authoritarian doctrine but to adapt our own. Resilience must be elevated to a strategic capability, visible, credible and pre-authorised.

4.7 Conclusion

Resilience in the age of silent strategic warfare is not merely a safeguard. It is a signal, of readiness, of continuity, and of distributed deterrence. It must operate in real time, not as a post-incident recovery plan. It must extend beyond technical layers to include public trust, institutional tempo, and decision authority under conditions of ambiguity.

As adversaries refine their capacity to exploit seams, disrupt infrastructure, and shape perception, the West's ability to endure, to persist without disorder, will increasingly define the balance of strategic advantage. Resilience, properly understood, is not what happens after the crisis. It is what prevents the crisis from achieving its aim.

References (for Section 4):

[2] Russian hybrid warfare in Europe, incidents including infrastructure sabotage and social destabilisation. Timeline: Wikipedia; analysis: Geopolitical Monitor.

[3] Cyberwarfare and Iran, March 2025 jamming of maritime communications. Summary: Wikipedia.

[6] Hacktivist DDoS wave, June 2025 attacks on U.S. finance and defence-aligned infrastructure. Source: TechRadar.

[8] UK cyber and AI targeting doctrine, May 2025 policy announcement. Coverage: The Times, Financial Times.

Section 5: The Grey Zone is Not a Gap – It is the Ground

5.1 Introduction

The term "grey zone" has become a fixture of strategic discourse, typically used to describe the ambiguous space between peace and war. Yet its continued framing as an interim condition, a phase to be crossed or resolved, risks misunderstanding its strategic character. For many adversaries, the grey zone is not transitional. It is intentional. It is the primary terrain upon which national advantage is pursued, institutions are tested, and deterrence is shaped.

This section argues that the grey zone must be reframed, not as a deficiency in traditional doctrine, but as a distinct operating environment with its own rules, pressures, and forms of escalation. Silent warfare is not a rehearsal for something else. It is the contest itself. To treat it otherwise is to concede initiative.

5.2 Strategic Continuity Without Declaration

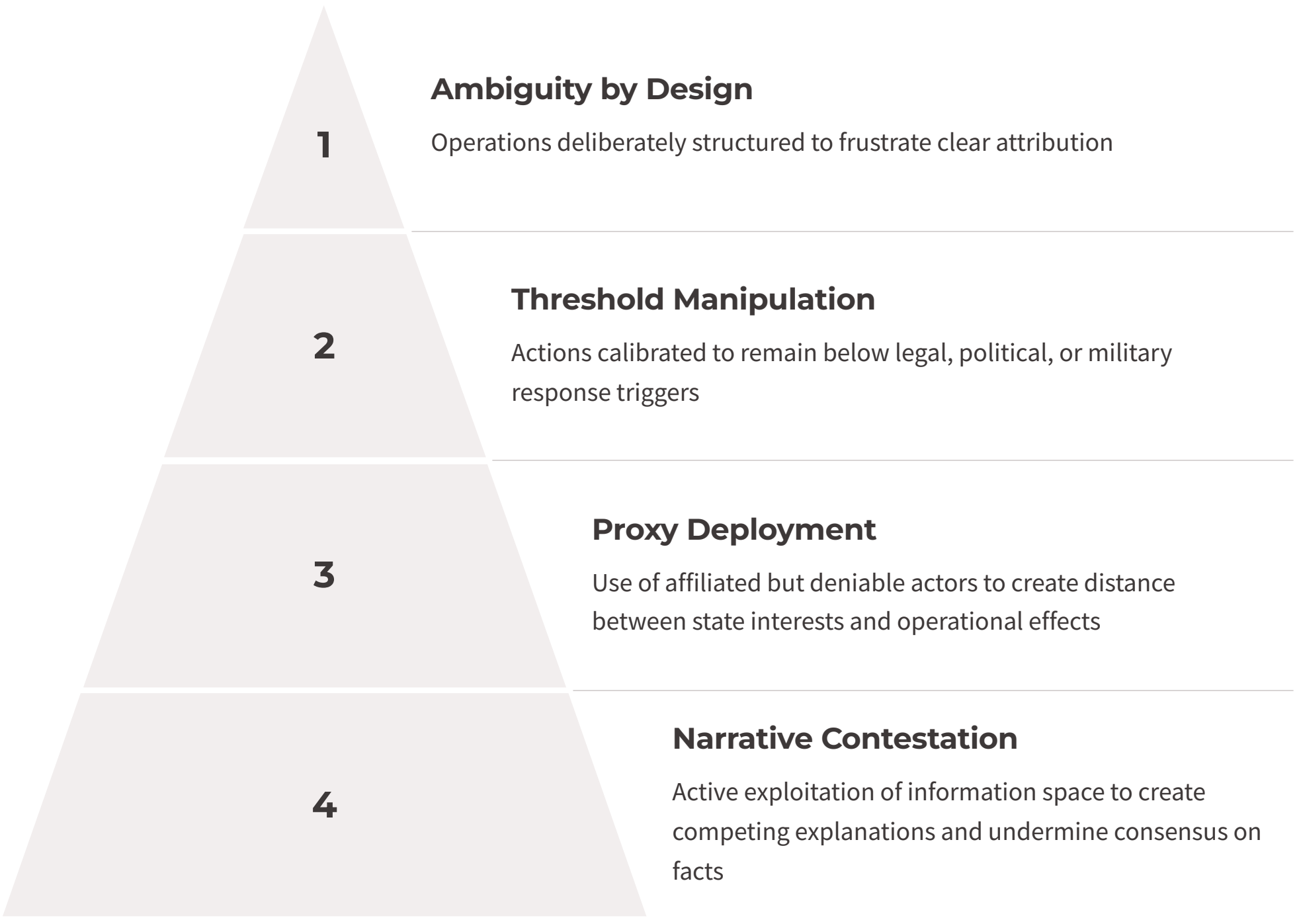
One of the defining characteristics of silent strategic warfare is temporal continuity. Unlike conventional military operations, which are bounded by declarations, deployments, or discrete engagements, grey zone activity unfolds across time with no clear beginning or end.

Russia's hybrid campaign in Europe, for example, has not followed a linear path. It comprises infrastructure sabotage, disinformation stunts, and proxy-led arson, conducted intermittently but with thematic coherence【2】. Each incident is individually deniable, yet collectively coherent, undermining cohesion, probing defences, and creating a sustained climate of uncertainty. It is this continuity, rather than intensity, that delivers strategic effect.

Similarly, China's creation of the PLA Cyberspace Force reflects a long-term investment in sustained shaping operations【1】. Its remit includes offensive cyber action and psychological influence, with an emphasis on persistent presence in adversary digital and cognitive terrain. The goal is not to trigger a crisis, but to shape strategic conditions without entering one.

These examples point to a doctrinal truth: adversaries are increasingly operating without closure. They pursue advantage through presence, ambiguity, and pressure, conditions designed not to end conflict, but to extend influence indefinitely.

5.3 Shaping Without Attribution



Another feature of grey zone activity is its avoidance of clear attribution. Operations are designed to frustrate response frameworks by operating below the thresholds of legality, attribution, or consensus. The absence of smoking guns is not incidental, it is strategic design.

Iran's maritime disruption in March 2025 is illustrative. By jamming communications and satellite links across more than 100 vessels and platforms, Iranian-linked actors imposed economic cost and strategic signalling without breaching laws of armed conflict【3】. The ambiguity of origin allowed space for narrative manoeuvre, while the effect was absorbed into commercial risk environments rather than military deterrence structures.

The June 2025 DDoS wave, attributed to nationalist-aligned hacktivist groups, further demonstrates this tactic【6】. These groups operate without uniform or flag, yet consistently align with the interests of known state actors. They offer plausible deniability while delivering coordinated friction. Attribution becomes contested, response is delayed, and the initiative is retained.

This presents a dilemma for Western institutions, which are structured around clear lines of responsibility and proportionality. In the grey zone, adversaries are not avoiding escalation, they are avoiding accountability. This distinction is central to understanding their intent.

5.4 Operating Without Declared Hostility

The grey zone also permits operations that feel hostile without being declared so. This enables states to act with assertiveness while denying the premise of conflict. It is a posture that allows for action without commitment, pressure without mobilisation, and coercion without crossing into formal warfare.

This logic is not unique to any one actor. It is visible in Israel's covert sabotage preceding kinetic action【4】, in India's integrated drone–cyber–narrative operations during Operation Sindoor【5】, and in the systemic testing of infrastructure across NATO's periphery. Each case demonstrates the capacity of states to project effect without opening formal hostilities.

In strategic terms, this is a challenge to the utility of threshold-based deterrence. If the triggers for response are defined in ways adversaries can sidestep, then deterrence is bypassed without being breached. The rules still stand, but adversaries have learned to walk between them.

For NATO and its allies, this requires a reappraisal of posture. Rather than relying solely on deterrence by punishment, there is an increasing need for deterrence by friction, making grey zone activity costly, slow, or strategically unrewarding, even if it does not cross into the conventional battlespace.

5.5 Governance Without Closure

Finally, the grey zone presents challenges for governance. Western institutions are not designed for permanent contestation. Decision-making processes rely on clarity, escalation frameworks depend on defined breaches, and public trust presumes a level of narrative coherence that is difficult to sustain under continuous silent pressure.

Yet the evidence suggests that silent conflict is now a persistent condition. It spans cyber, economic, and narrative domains. It is prosecuted by state and proxy alike. It requires no formal entry point and has no natural end state.

Standing Authorisation

Establish frameworks for response under ambiguity, rather than relying on ad hoc escalation processes that delay effective countermeasures.

Civilian Integration

Incorporate critical civilian infrastructure into strategic deterrence planning, not just as systems to be protected but as elements of national resilience posture.

Narrative Resilience

Develop narrative coherence as a core strategic competence, not merely as a public affairs function or crisis communication tool.

Accelerated Decision Cycles

Create faster, legally bounded decision frameworks that enable pre-emptive action within clear ethical and operational constraints.

As a result, Western governance frameworks must adapt to this environment. This is not an argument for militarisation of society. It is an argument for coherence, across public, private, and sovereign actors, in recognising that strategic competition is already under way, even if war has not been declared.

5.6 Conclusion

The grey zone is not a conceptual gap between peace and war. It is a doctrinal space, deliberately occupied, and increasingly decisive. Adversaries are operating with clarity of intent and coherence of method. They are shaping strategic outcomes without seeking decisive battles. Their objective is not domination through confrontation, but advantage through persistence.

For the UK and its allies, the task is not to redefine war, but to recognise that warlike effects are now being pursued by other means and to develop a posture that meets this challenge with composure, capability, and sovereign control.

Strategic competition is not waiting for a trigger. It is unfolding now, without closure, without declaration, and without obvious end. The grey zone is not what comes before. It is where we are.

References (for Section 5):

[1] People's Liberation Army Cyberspace Force, established April 2024. Overview: Wikipedia; corroborated by Jamestown Foundation briefings.

[2] Russian hybrid warfare in Europe, May 2024 – June 2025. Incidents: Wikipedia; analysis: Geopolitical Monitor.

[3] Cyberwarfare and Iran, LabDookhtegan maritime disruption, March 2025. Overview: Wikipedia.

[4] Israeli covert operations in Iran, June 2025. Reported coordination between drone sabotage and precision airstrikes. Summary: Wikipedia.

[5] India's Operation Sindoor, May 2025. Drone–cyber–narrative integration. Sources: Economic Times; Financial Times.

[6] Hacktivist-led DDoS wave, June 2025. Source: TechRadar.

References

1. People's Liberation Army Cyberspace Force (2024) "People's Liberation Army Cyberspace Force", Wikipedia. Accessed June 2025. https://en.wikipedia.org/wiki/People%27s_Liberation_Army_Cyberspace_Force
2. Russian Hybrid Warfare in Europe (2022–2025) "Russian hybrid warfare in Europe (2022–present)", Wikipedia. Accessed June 2025. https://en.wikipedia.org/wiki/Russian_hybrid_warfare_in_Europe_%282022%E2%80%93present%29 Geopolitical Monitor. "Russia's Gray Zone Warfare Campaign in Europe", December 2024. https://www.geopoliticalmonitor.com/russias-gray-zone-warfare-campaign-in-europe/
3. Cyberwarfare and Iran (March 2025) "Cyberwarfare and Iran", Wikipedia. Accessed June 2025. https://en.wikipedia.org/wiki/Cyberwarfare_and_Iran
4. June 2025 Israeli Operations in Iran "June 2025 Mossad operations in Iran", Wikipedia. Accessed June 2025. https://en.wikipedia.org/wiki/June_2025_Mossad_operations_in_Iran
5. India's Operation Sindoor (May 2025) Nayyar, K. "Airspace to Cyberspace: How India Fought Swarms of Drones & Misinformation During Conflict", The Economic Times, 14 May 2025. https://economictimes.indiatimes.com/news/defence/airspace-to-cyberspace-how-india-fought-swarms-of-drones-wave-of-misinformation-during-conflict/articleshow/121165746.cms Stacey, K. "India Executes Cross-Domain Retaliation Operation Following Terrorist Attack", Financial Times, 15 May 2025. https://www.ft.com/content/5a3abd52-3b26-44b7-ab94-7a76fbb485a6
6. Hacktivist-Led DDoS Campaign (June 2025) Muncaster, P. "Mr. Hamza, Mysterious Team Bangladesh, and Keynous+ Led a Massive Surge in DDoS on US Businesses", TechRadar Pro, 28 June 2025. https://www.techradar.com/pro/security/mr-hamza-mysterious-team-bangladesh-andkeynous-led-a-massive-surge-in-ddos-on-us-businesses-following-an-attack-on-iran
7. NATO DEEP Dive Vol. 1 (September 2024) NATO DEEP eAcademy. DEEP Dive Volume 1: Allied Integration in the Cognitive and Cyber Domains, September 2024. https://deepportal.hq.nato.int/eacademy/wp-content/uploads/2024/09/DEEP-DIVE-Vol.1.pdf
8. UK Cyber Doctrine & Digital Targeting Initiative (May 2025) Beale, J. "Britain to Increase Cyberattacks on Russia and China", The Times, 28 May 2025. https://www.thetimes.co.uk/article/britain-increase-cyberattacks-russia-china-zg5jrn3hv O'Connor, S. "UK Military to Build AI-Powered Digital Targeting Web", Financial Times, 28 May 2025. https://www.ft.com/content/1f7c7261-b379-4d03-9809-2067a8fe9c4c