



SAGE INTERNATIONAL AUSTRALIA

STRATEGIC INTELLIGENCE BRIEF | NO. 004

THRESHOLD CONDITIONING

Winning Without Crossing the Threshold

Dr John Bruni | 10 August 2026 | Adelaide, Australia

NATO's greatest vulnerability may be a campaign designed never to cross the Article 5 threshold.

CHALLENGE THE ASSUMPTION | TEST THE SYSTEM | IDENTIFY THE CONSEQUENCE

sageinternational.com.au

Suggested Citation

Bruni, J. (2026). Threshold Conditioning — Winning Without Crossing the Threshold (SAGE International Strategic Intelligence Brief No. 004). Adelaide: SAGE International Australia

Executive Summary

This brief assesses the evolving nature of hybrid threats posed by the Russian Federation to NATO, with particular emphasis on the concept of ‘threshold conditioning.’ Repeated low-level hostile actions, if unaddressed collectively, risk normalising behaviour that erodes the credibility of Western deterrence. The brief argues that NATO’s strategic approach must shift from incident-by-incident response to cumulative deterrence, leveraging Article 4 and enhancing resilience measures. The implications extend beyond Europe, signalling broader challenges for Western alliances in the Indo-Pacific context. High confidence is assigned to the assessment that Russia will persist in hybrid activities designed to test and weaken Alliance cohesion, while the likelihood of immediate large-scale conventional attack remains low.

Threshold Conditioning

The danger presented by Russian hybrid activity is not simply that individual attacks may prove difficult to attribute or respond to. There is a second and potentially more consequential effect. Repeated provocations can change what governments and populations regard as normal.

This might be described as ‘threshold conditioning.’

Consider the political psychology involved. The first unexplained explosion at a European defence facility attracts considerable attention. The fifth becomes part of the security environment. The first major GPS disruption affecting civilian aviation generates alarm. Persistent interference becomes an operational problem to be managed. The first Russian drone entering NATO airspace appears potentially escalatory. Repeated incursions risk becoming another feature of the confrontation between Russia and the West.

Nothing in NATO’s treaties has changed. But expectations have. The danger is therefore that repeated hostile behaviour gradually increases the political threshold at which Western governments believe retaliation is justified.

This creates an important asymmetry.

Russia can repeatedly experiment with the lower boundary of Western tolerance while NATO governments must continually decide whether each incident is sufficiently serious to justify collective action. Every incident therefore generates information.

Moscow observes which actions produce condemnation, which produce sanctions, which lead to military responses and which disappear from public attention.

Over time, this process can reveal the practical rather than declared boundaries of Western deterrence.

The result could be deterrence erosion through successful non-response. This does not mean NATO must retaliate militarily against every hostile act. Indeed, doing so would create precisely the escalation instability that Moscow might seek to exploit. The problem instead lies in treating a coordinated campaign as a collection of unrelated incidents.

An adversary employing hybrid coercion benefits from fragmentation. A cyberattack is investigated by cybersecurity agencies. Sabotage becomes a police matter. Disinformation is addressed by

communications specialists. Infrastructure damage becomes an engineering problem. Border incidents become matters for national governments. Viewed individually, each may remain manageable. Viewed collectively, however, they may reveal strategic intent.

The distinction is fundamental.

KEY JUDGEMENTS

- Russia's most realistic escalation strategy against NATO is likely to emphasise coercion rather than conquest. Its objective would be to weaken confidence in collective defence without triggering a conventional conflict Russia cannot confidently control.
- The principal vulnerability is political rather than military. NATO possesses overwhelming aggregate military capability, but deterrence ultimately depends upon the willingness of 32 governments to interpret hostile behaviour as requiring collective action.
- Threshold conditioning represents an underappreciated danger. Repeated low-level hostile actions can gradually normalise behaviour that previously would have generated considerably greater alarm.
- Every unanswered provocation can provide information about Western tolerance. Moscow can learn from NATO responses and adapt subsequent activity accordingly.
- Hybrid campaigns should therefore be assessed cumulatively. Tactical ambiguity should not be permitted to conceal strategic intent.
- Article 4 could become a more important instrument of deterrence. Collective consultation should lead to visible and increasingly consequential responses when patterns of hostile activity emerge.
- Resilience is a form of deterrence. Reducing the political and economic effects of disruption reduces the strategic value of attacking Western societies.
- NATO should retain ambiguity regarding its response. Cumulative deterrence should not create a checklist of actions Russia can safely conduct beneath predetermined thresholds.
- The objective should be to reverse the burden of uncertainty. Moscow should be uncertain about when accumulated hostile behaviour will produce collective consequences.

Cumulative Deterrence

Traditional deterrence tends to concentrate on thresholds. An adversary is warned that if it undertakes a sufficiently serious action, consequences will follow. NATO's Article 5 provides perhaps the world's most powerful example: an armed attack upon one member is considered an attack upon all.

Grey-zone coercion attempts to exploit the territory beneath that threshold.

The appropriate response may therefore require a complementary concept:

Cumulative Deterrence

Under cumulative deterrence, hostile actions would not necessarily be assessed solely as individual incidents. NATO would also assess whether apparently separate activities collectively constitute an attributable campaign intended to intimidate, destabilise or coerce one or more Alliance members.

The principle would be straightforward:

An adversary should not be able to avoid collective consequences merely by dividing a strategic attack into sufficiently small individual components.

One cyberattack might not constitute an armed attack.

One act of sabotage might not.

One border violation might not.

One campaign of political interference might not.

But a sustained combination of such activities could represent something strategically different from the individual incidents from which it is composed.

Intent emerges from pattern.

This would not require rewriting Article 5, nor should NATO automatically classify cumulative hybrid activity as an armed attack.

Instead, cumulative deterrence would create a structured range of collective responses below Article 5. The objective would be to remove one of the central assumptions underpinning grey-zone coercion: that remaining below the threshold of war also means remaining below the threshold of meaningful collective response.

Making Article 4 Matter

Article 4 may therefore become increasingly important to NATO's future deterrence architecture.

Article 5 understandably dominates public discussion because it embodies collective defence. But Article 4 permits any member to request consultations whenever its territorial integrity, political independence or security is threatened.

Rather than regarding Article 4 principally as a diplomatic consultation mechanism—or as a waiting room before Article 5—NATO could increasingly use it as an instrument of collective grey-zone deterrence. A recognised campaign of hostile activity could automatically trigger intensified intelligence sharing, coordinated attribution, increased infrastructure protection, cyber assistance, military surveillance and predetermined diplomatic or economic measures.

The significance would be political.

Russia would know that remaining beneath Article 5 no longer guaranteed that NATO's response would remain primarily national.

This would close part of the gap that grey-zone coercion seeks to exploit.

Practical Countermeasures

Cumulative deterrence would require institutional mechanisms capable of translating the concept into credible action.

1. Campaign Attribution

NATO should increasingly assess hostile activity as campaigns rather than isolated events.

Cyber incidents, sabotage, electronic interference, political influence operations, airspace violations and attacks upon critical infrastructure should be integrated into a common strategic picture.

The question would no longer simply be:

Who conducted this incident?

It would also become:

Is this incident part of an identifiable campaign?

NATO already possesses intelligence and hybrid-analysis structures capable of supporting such an approach. The next step would be making campaign attribution an explicit component of deterrence.

2. Graduated Collective Consequences

The Alliance requires meaningful options between condemnation and Article 5.

An attributable hostile campaign could trigger progressively stronger collective responses according to its persistence and severity.

These could include coordinated diplomatic measures, financial restrictions, strengthened cyber defence, increased counter-intelligence cooperation, enhanced infrastructure protection, additional surveillance and temporary increases in NATO military presence.

The precise response should remain unpredictable.

Deterrence benefits when an adversary understands that costs will follow hostile behaviour without knowing precisely where, when or how those costs will be imposed.

3. Resilience as Deterrence by Denial

Hybrid coercion succeeds when relatively inexpensive actions produce disproportionately large political consequences.

Resilience changes that calculation.

Redundant communications, hardened infrastructure, rapid repair capacity, cybersecurity, continuity-of-government arrangements, alternative energy supplies and effective civil-defence mechanisms reduce the potential strategic return from sabotage or disruption.

This turns national resilience into something more than emergency preparedness.

It becomes deterrence by denial.

If Russian planners conclude that attacking infrastructure will produce temporary inconvenience rather than political crisis, the attractiveness of the attack diminishes.

4. Rapid Collective Attribution

Democratic governments are often disadvantaged by the time required to investigate incidents, establish responsibility and develop political consensus.

Hybrid operations exploit that delay.

NATO should therefore continue improving mechanisms through which members can rapidly pool intelligence and issue collective assessments where evidence permits.

Perfect certainty should not become the enemy of strategic judgement.

Attribution must remain evidence-based, but governments should recognise that adversaries deliberately exploit the evidentiary standards of democratic societies.

5. Strategic Communication

Western governments should explain the campaign rather than merely announce the incident.

This is critical.

If citizens hear about a railway fire on Monday, a cyberattack three weeks later and GPS disruption the following month, they may perceive three unrelated events.

If credible evidence indicates they form part of a coordinated coercive campaign, governments should explain that pattern publicly.

Doing so reduces the psychological advantage created by ambiguity and makes subsequent countermeasures easier to justify democratically.

6. Exercises for Political Decision-Makers

NATO exercises extensively for military contingencies.

It should equally stress-test the political machinery of collective defence against ambiguous scenarios.

How quickly can governments reach agreement when attribution is incomplete?

What happens when several members interpret the same incident differently?

What if hybrid attacks occur simultaneously across several states?

What happens when Russia denies responsibility while threatening escalation if NATO responds?

These are ultimately political rather than tactical problems. They should therefore be exercised at the political level before a real crisis occurs.

From Deterrence by Punishment to Deterrence of Process

The deeper implication is that Western deterrence may need to evolve.

During the Cold War, deterrence largely concerned identifiable thresholds: territorial invasion, strategic attack and ultimately nuclear escalation.

Contemporary authoritarian states possess far more opportunities to operate inside Western societies without crossing those traditional thresholds. Digital infrastructure, global financial systems, social media, supply chains, energy networks and open political systems provide both enormous economic benefits and potential strategic vulnerabilities.

Russia does not necessarily need to destroy these systems. It can attempt to manipulate their interdependence. The objective of cumulative deterrence would therefore be to deny Moscow the ability to determine the tempo of escalation through a sequence of individually ambiguous actions.

NATO would effectively communicate:

We will judge hostile behaviour not simply by individual incidents, but by the strategic pattern those incidents collectively create.

This restores uncertainty to the aggressor.

Moscow would no longer be able to assume that staying immediately beneath a perceived Article 5 threshold protects it from collective consequences. The uncertainty upon which hybrid coercion depends would begin operating in both directions.

Assessment

Russia's most plausible escalatory strategy against NATO is unlikely to resemble the Soviet scenarios that dominated Cold War planning. The threat of large-scale conventional war remains important, particularly as Russia rebuilds forces depleted by the Ukraine conflict. But NATO's aggregate conventional and nuclear strength makes deliberate general war extraordinarily dangerous for Moscow.

The more attractive option may therefore be political warfare conducted through asymmetric means.

The objective would not necessarily be territorial conquest.

It would be deterrence erosion.

Cyber operations, sabotage, information warfare, infrastructure disruption, electronic interference and calibrated military provocations could be employed to determine how much pressure individual NATO states will absorb before the Alliance responds collectively.

Repeated carefully enough, these actions could produce threshold conditioning: behaviour once considered intolerable gradually becomes incorporated into Europe's normal security environment. The ultimate danger is not that Article 5 disappears. It is that governments and populations gradually become uncertain about the circumstances in which it remains politically usable.

Cumulative deterrence offers one possible response.

Instead of allowing an adversary to fragment strategic coercion into individually manageable incidents, NATO would increasingly judge behaviour according to the cumulative pattern it creates. The Alliance would retain Article 5 for the gravest circumstances while developing stronger collective consequences beneath it. The strategic message would be simple: Remaining below the threshold of war does not mean remaining below the threshold of collective defence.

Key Policy Recommendations:

- Institutionalise cumulative deterrence by integrating incident reporting and attribution across NATO members.
- Operationalise Article 4 as a trigger for collective intelligence-sharing, attribution, and graduated response options below Article 5.
- Invest in resilience measures—cyber, infrastructure, civil preparedness—as core deterrence-by-denial tools.
- Conduct regular exercises at the political level to test Alliance decision-making under ambiguous and hybrid attack scenarios.
- Ensure strategic communications highlight the cumulative nature of hybrid campaigns to both domestic and international audiences.

These measures are assessed as necessary to maintain credible deterrence amid evolving hybrid threats. (High Confidence)

Confidence Assessment (as of August 2026)

High Confidence

Russia will continue employing cyber, information, intelligence, economic and other hybrid instruments against NATO members. NATO itself assesses that Russian hybrid activity has increased in scale and intensity and is intended to destabilise Allied societies and weaken support for Ukraine.

Moderate-High Confidence

Moscow will continue testing Western political tolerance while attempting to avoid an uncontrollable direct military confrontation with NATO.

Moderate Confidence

Repeated hostile activity can contribute to threshold conditioning if individual incidents become normalised and governments fail to communicate their cumulative strategic significance.

Moderate Confidence

A more systematic NATO approach combining campaign attribution, resilience and graduated collective consequences could reduce the attractiveness of grey-zone coercion, although no system can eliminate the problems of attribution and escalation management.

Low Confidence

Russia will deliberately initiate a major conventional attack against NATO in the immediate term. Capability assessments concerning the later 2020s should not be treated as proof of political intent.

Addendum — The AI Attribution Problem

The preceding assessment largely assumes a traditional model of strategic competition: a human adversary makes a political decision, directs hostile activity and calibrates that activity to remain beneath an opponent's threshold for escalation.

Artificial intelligence may complicate this model considerably.

Grey-zone competition already depends upon ambiguity. Cyber operations, disinformation, sabotage, drone activity and influence operations can make attribution difficult and delay political decision-making. AI potentially adds another layer by dramatically increasing the speed, scale and adaptability with which such activity can be generated and coordinated.

An adversary employing AI-enabled systems could potentially generate large numbers of apparently independent actions: synthetic personas, false narratives, cyber probes, deepfakes, automated influence operations and other forms of digital disruption. What appears to be a series of unrelated human-directed incidents may instead constitute a machine-amplified campaign operating at a tempo considerably faster than traditional government decision-making.

This creates what SAGE describes as the AI Attribution Problem.

Traditional deterrence assumes that governments can answer several questions before deciding upon a response:

Who conducted the action?

What was their intention?

Who authorised it?

What response is proportionate?

AI-enabled grey-zone activity introduces another question:

To what extent is a human actor actually controlling the campaign?

This distinction matters.

There is a considerable difference between human-directed activity, AI-assisted human activity, and potentially semi-autonomous or autonomous AI activity operating within parameters established by a human actor.

In each case, political responsibility may ultimately remain with the state or organisation deploying the system. But determining immediate intent becomes considerably more complicated.

An AI-enabled campaign might identify vulnerabilities, generate narratives, test responses and modify subsequent activity considerably faster than governments can establish attribution and coordinate countermeasures.

The danger therefore operates in two directions.

Respond too slowly, and an AI-enabled campaign may become self-reinforcing—exploiting political divisions, generating new narratives and adapting to defensive measures before governments have agreed upon what is occurring.

Respond too quickly, however, and governments risk misattribution. An incorrectly attributed cyberattack, deepfake, infrastructure disruption or information operation during an international crisis could itself become an escalation mechanism.

The problem is therefore not simply one of artificial intelligence.

It is one of decision time.

From Cumulative Deterrence to Cumulative Attribution

This has important implications for the concept of Cumulative Deterrence developed in this brief.

Cumulative deterrence depends upon identifying patterns across apparently separate hostile activities. AI could simultaneously make those patterns both larger and harder to interpret.

Volume cannot automatically be equated with strategic intent.

A thousand AI-generated incidents do not necessarily represent a thousand political decisions.

Conversely, what appears to be thousands of independent incidents could originate from a single adversarial campaign.

NATO therefore requires not simply faster attribution but cumulative attribution: the ability to identify relationships among incidents, distinguish machine-generated amplification from independent human activity, and determine which actor ultimately benefits from the resulting disruption.

This suggests three increasingly important questions for strategic intelligence:

Who is doing this? Is a human directing it, or is AI generating or amplifying it? Who benefits?

The third question may become particularly important when technical attribution remains uncertain.

An AI-Enabled Attribution Architecture

The practical implication is that Western governments may require an AI-enabled attribution and verification architecture capable of operating at something approaching machine speed while retaining human authority over consequential political decisions.

AI could assist analysts by identifying anomalous activity, correlating apparently unrelated incidents, detecting synthetic information, tracing digital infrastructure and identifying patterns too large for human

analysts to process in real time.

But AI should assist attribution rather than determine retaliation.

The distinction is fundamental.

Machines may increasingly identify the pattern. Humans must continue deciding what the pattern means.

This creates a requirement for what might be described as human-speed sovereignty within machine-speed competition: preserving meaningful human political judgement while ensuring that the information required for that judgement arrives quickly enough to remain strategically relevant.

The AI revolution therefore potentially strengthens rather than weakens the argument for Cumulative Deterrence.

If grey-zone warfare seeks to fragment hostile activity into ambiguous individual incidents, AI could industrialise that fragmentation.

The defensive response must consequently become better at reconstructing the whole.

The strategic contest may increasingly become a race between machine-generated ambiguity and machine-assisted attribution.

And in that contest, the decisive advantage may not belong to the actor possessing the most sophisticated artificial intelligence.

It may belong to the political system capable of determining what is happening, who is responsible and what it means—before the window for effective human action closes.

Strategic Outlook: Beyond Russia—Implications for Western Alliance Structures

There is a final question. The vulnerabilities examined in this brief are not uniquely European. NATO represents the world's most institutionalised military alliance, but the broader Western strategic system extends considerably further.

Across the Indo-Pacific, the United States maintains bilateral alliances with Japan, South Korea, Australia and the Philippines, while Taiwan occupies a strategically important but deliberately ambiguous position within the regional security architecture. Australia and New Zealand maintain their own longstanding defence relationship, while increasingly dense networks of trilateral and minilateral cooperation connect many of these states.

The People's Republic of China also possesses considerably greater economic leverage over many regional countries than Russia possesses over contemporary Europe.

This raises an uncomfortable possibility.

If Russia can seek to undermine NATO by separating military capability from the political willingness to use it, could China apply a similar strategic principle in the Indo-Pacific? The instruments would not necessarily be identical.

Economic coercion, maritime pressure, cyber operations, political influence, information manipulation, incremental changes to established patterns of military activity and carefully calibrated challenges to regional security commitments could potentially serve a comparable purpose.

The institutional target would also differ.

There is no Indo-Pacific Article 5. Instead, the central strategic question would concern the credibility of the network itself: At what point does pressure against one American ally or partner become a problem requiring action by the others?

And perhaps more importantly:

Could Beijing gradually change that threshold without ever creating the single crisis that forces the regional security system to respond? If so, the challenge confronting NATO may represent only one manifestation of a much broader transformation in strategic competition. The emerging contest may not simply concern territory, military power or even deterrence in its traditional sense. It may concern something more fundamental: the credibility of the institutions and relationships through which Western military power becomes collective political action.

That question will be examined in the next SAGE Intelligence Brief.

Disclaimer

SAGE Strategic Intelligence Briefs are produced independently and are intended to support informed discussion of geopolitical, defence, security and economic developments. Assessments reflect information available at the time of publication and may change as new information emerges.

About SAGE International Australia

SAGE International Australia is an independent strategic research and analysis organisation specialising in geopolitics, defence, national security, economic resilience and strategic foresight.

Through objective, evidence-based and non-partisan analysis, SAGE helps decision-makers understand risk, identify opportunity and prepare for future challenges.

For more information, visit:

www.sageinternational.com.au