JOURNAL OF INTERNATIONAL RELATIONS AND GLOBAL AFFAIRS
Vol. 51, No. 3 (2026) | pp. 214–229 | DOI: 10.5555/jirga.2026.51.3.214

RESEARCH ARTICLES · GLOBAL SECURITY AND CONFLICT STUDIES

# Deterrence in the Grey Zone

*Rethinking Escalation Thresholds in Contested Cyber-Physical Domains*

Naomi Reyes-Fischer and Tobias Lindqvist
Department of Security Studies, Fenton University · Nordic Security Institute

**ABSTRACT**

Traditional deterrence theory, developed primarily around nuclear and conventional military threats, struggles to account for the ambiguous, incremental, and often deniable nature of grey-zone competition between state and state-aligned actors. This article develops a revised framework for understanding escalation thresholds in cyber-physical conflict, arguing that the binary logic of classical deterrence — premised on clear signaling and identifiable red lines — breaks down when actions occur below the threshold of armed conflict and attribution remains contested. Drawing on case studies of infrastructure disruption incidents between 2019 and 2024, the article identifies three mechanisms through which grey-zone actors calibrate risk: plausible deniability, incremental probing, and proxy delegation. It argues that effective deterrence in this domain requires shifting from threshold-based signaling toward resilience-based deterrence, in which the credible capacity to absorb and recover from disruption becomes a more stable deterrent than retaliatory threat alone. The article concludes by outlining implications for alliance coordination and international norm-building in cyberspace.

**Keywords:** deterrence theory; grey-zone conflict; cybersecurity; escalation dynamics; critical infrastructure

## 1. Introduction

Deterrence theory has long rested on a set of assumptions inherited from the nuclear age: that adversaries are identifiable, that threats can be communicated with clarity, and that the costs of crossing a defined threshold are calculable in advance. These assumptions travelled reasonably well into the domain of conventional military deterrence, where force postures, alliance commitments, and territorial boundaries provided reference points against which credibility could be assessed. They travel far less well into the contested space of grey-zone competition, where state and state-aligned actors pursue strategic objectives through means that are deliberately calibrated to remain below the threshold that would trigger a forceful response.

This article is concerned with a specific and increasingly consequential instance of this problem: the disruption of critical infrastructure through cyber-physical means. Unlike overt military aggression, such disruption is frequently difficult to attribute with confidence, is often carried out through intermediaries or proxies, and unfolds incrementally rather than as a single, threshold-crossing event. Under these conditions, the central pillars of classical deterrence — clear signaling, credible retaliation, and threshold definition — lose much of their functional value.

## 2. The Limits of Threshold-Based Deterrence

Threshold-based deterrence assumes that a defender can specify, ex ante, a line whose crossing will trigger a proportionate and credible response, and that a challenger will rationally avoid crossing it once the costs are made sufficiently clear. This logic depends on three conditions that are frequently absent in cyber-physical grey-zone conflict: reliable attribution, unambiguous signaling, and a shared understanding between adversaries of where the threshold lies. Grey-zone actors have strong incentives to violate all three conditions simultaneously, since ambiguity is not an unfortunate byproduct of their operations but a primary strategic asset.

Our analysis of infrastructure disruption incidents occurring between 2019 and 2024 — spanning energy grid intrusions, water treatment system interference, and logistics network disruptions across several regions — suggests that this ambiguity is exploited through three recurring mechanisms.

## 3. Three Mechanisms of Risk Calibration

*Plausible deniability.* Actors structure operations so that technical attribution, even where achieved with reasonable confidence by defenders, can be publicly and diplomatically contested. This does not require actual anonymity, but rather sufficient ambiguity that a forceful response by the target state risks appearing disproportionate or unjustified to third-party audiences.

*Incremental probing.* Rather than executing a single decisive action, grey-zone actors frequently conduct a sequence of smaller operations, each individually calibrated to fall below any plausible retaliation

threshold, while cumulatively achieving strategic effects comparable to a more overt action. This incrementalism exploits the fact that deterrence frameworks are typically built around discrete, identifiable events rather than cumulative patterns.

*Proxy delegation.* Operations are frequently delegated, formally or informally, to non-state or quasi-state intermediaries, allowing sponsoring states to maintain a layer of separation that complicates both attribution and the political calculus of retaliation.

## 4. Toward Resilience-Based Deterrence

If threshold-based signaling is structurally ill-suited to this environment, an alternative approach is needed. We propose a shift in emphasis from deterrence-by-punishment, which depends on the credible threat of retaliation once a threshold is crossed, toward deterrence-by-resilience, which depends on the credible demonstration that disruption will fail to achieve its intended strategic effect because the target system can absorb, adapt, and recover quickly. Resilience-based deterrence does not require confident attribution or a clearly defined threshold; it operates instead by devaluing the expected payoff of disruption itself, regardless of who carries it out or how incrementally it is pursued.

This reorientation has practical implications for infrastructure investment, redundancy planning, and the pooling of recovery capacity across allied states, treating resilience not merely as a defensive contingency but as an active component of strategic signaling.

## 5. Conclusion

Grey-zone competition in cyber-physical domains exposes structural weaknesses in classical deterrence theory that cannot be resolved simply by improving attribution technology or clarifying declaratory thresholds. A more durable approach recognizes that ambiguity is a permanent feature of this competitive space rather than a temporary obstacle, and builds deterrent credibility around the demonstrated capacity to withstand and recover from disruption. Future research should examine how resilience-based signaling can be credibly communicated to adversaries without undermining the operational security of the systems it is meant to protect, and how allied states might coordinate recovery capacity as a form of collective deterrence.

## References


Jervis, R. (1979). Deterrence theory revisited. *World Politics*, 31(2), 289–324.

Lindsay, J. R. (2015). Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, 1(1), 53–67.

Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict*. U.S. Army War College Press.

Valeriano, B., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.