



Ricardo Rodrigues Caiado Researcher and PhD in Law and Security.

INTELLIGENCE, HYBRID THREATS AND EUROPEAN SECURITY

21 September 2026

Hybrid competition changes the conditions under which European security is organised. Intelligence cannot guarantee prevention, and its strategic value depends on institutional connectivity. For Europe, the challenge is to strengthen connections among national authorities, EU mechanisms, NATO capabilities and infrastructure operators while maintaining legal and democratic safeguards.

The contemporary international order is increasingly characterised by strategic competition conducted through combinations of military, cyber, informational, economic and societal instruments. Hybrid threats exploit vulnerabilities while preserving ambiguity, complicating attribution and challenging the traditional distinction between peace, crisis and conflict.

Critical infrastructure is particularly exposed because energy, transport, telecommunications, finance, health and digital services depend on interconnected systems. A disruption can therefore propagate across organisational and sectoral boundaries. In this environment, intelligence and early warning acquire a preventive function: they can reduce relevant uncertainty, identify vulnerabilities, recognise patterns and create opportunities for timely decision.

The central argument is that intelligence becomes strategically consequential when it is connected to institutional mechanisms capable of transforming information into warning, warning into decision, decision into protection and protection into resilience. The article proposes the Preventive Intelligence and Early Warning Framework (PIEW) as an analytical synthesis linking detection, fusion and interpretation, anticipation, decision activation, infrastructure protection and learning. The framework is conceptual rather than predictive and requires empirical validation.

Hybrid competition and strategic vulnerability

Hybrid competition does not necessarily involve a single identifiable method or threshold. Cyber operations, sabotage, information manipulation, economic coercion, covert political activity and exploitation of social or technological vulnerabilities can be combined in ways that create cumulative effects. Farrell

and Newman (2019) help explain why dependencies embedded in interconnected networks can become sources of leverage.

For critical infrastructure, the challenge is amplified by interdependence. A local incident may affect suppliers, communications, energy, logistics or digital services elsewhere. Security analysis therefore needs to move from isolated incidents towards system-level vulnerabilities and possible cascading effects.

Ambiguity is a further difficulty. Detection of an anomaly does not establish hostile intent; identification of a hostile pattern does not automatically establish legal attribution. Intelligence must consequently operate under uncertainty and provide decision-makers with assessments that distinguish evidence, confidence and alternative explanations.

Intelligence, early warning and strategic decision

Classical intelligence literature emphasises the transformation of information into knowledge relevant to policy and decision (Herman, 1996; Kent, 1966; Lowenthal, 2022). In a hybrid environment, the preventive value of intelligence depends

increasingly on the ability to integrate information across domains and institutions.

Early warning should not be understood as deterministic prediction. Its purpose is to create usable decision time by identifying changes, vulnerabilities or patterns early enough for protective measures to be considered. This requires attention to both threat indicators and the conditions that make infrastructure exploitable.

Recent research on hybrid threats and intelligence communities similarly emphasises the need to adapt intelligence practices to an environment in which threats are multidomain, persistent and difficult to attribute (Nilsson, Weissmann, & Palmertz, 2025). The implication is that warning systems should connect collection, interpretation and decision rather than treating them as separate activities.

From Warning to Resilience

A preventive system can be represented as a continuous cycle:

detection → fusion and interpretation → early warning and anticipation → decision activation → infrastructure protection and resilience → learning and adaptation → detection.

FIGURE 1. PREVENTIVE INTELLIGENCE AND EARLY WARNING (PIEW) FRAMEWORK

Note: The PIEW Framework is an author-developed analytical synthesis. It is not presented as a NATO or EU framework, a legal test or an empirically validated predictive model. Its value is to make explicit the institutional chain required for intelligence to become preventive capacity.

Function	Purpose	Output
1. Detection	Identify anomalies, indicators, vulnerabilities and relevant changes	Initial signal
2. Fusion and interpretation	Correlate information across domains and assess alternative explanations	Assessed pattern
3. Early warning and anticipation	Estimate plausible trajectories and create decision time	Warning
4. Decision activation	Connect warning to competent authorities and usable options	Protective decision
5. Protection and resilience	Reduce exposure, maintain continuity and limit cascading effects	Reduced vulnerability
6. Learning and adaptation	Evaluate outcomes and update indicators, procedures and assumptions	Improved prevention

Detection without interpretation generates noise. Interpretation without warning may arrive too late. Warning without decision authority creates inaction. Decision without protective capability does not necessarily reduce vulnerability. Learning is required because hybrid campaigns adapt to defensive measures and because infrastructure vulnerabilities change over time.

Warning levels and decision time

Three analytical warning levels can help connect assessment with graduated attention.

Level I – Situational Warning applies when an anomaly, vulnerability or relevant change is detected but evidence is insufficient to establish a coherent hostile pattern.

Level II – Operational Warning applies when multiple indicators suggest an emerging campaign, exploitation attempt or coordinated activity.

Level III – Strategic Warning applies when there is a credible trajectory towards significant disruption or systemic national or transnational consequences.

These categories are analytical rather than legal thresholds. Their purpose is to avoid treating every anomaly as an imminent attack while ensuring that accumulating indicators can trigger progressively higher levels of preparation.

The key variable is decision time: the interval between recognition of a meaningful threat and the point at which protective measures can no longer materially change the outcome. Intelligence can increase preventive opportunity by shortening the time between detection and decision or by identifying protective options before disruption occurs.

Intelligence and critical infrastructure

Preventive intelligence should integrate threat intelligence with vulnerability intelligence. Assessment should consider exposure, exploitability, propagation and consequence. Cross-domain fusion is important because hybrid activity rarely respects organisational boundaries.

Cyber intelligence can provide visibility into technical threats and vulnerabilities, while open-source intelligence can contribute information on public narratives, procurement activity, technical disclo-

sures, infrastructure changes and other indicators. Neither source is sufficient alone. Their value increases when combined with law-enforcement, diplomatic, economic, geospatial and infrastructure information.

Public-private cooperation is equally important. Many critical infrastructures are privately owned or operated, while public authorities may possess strategic intelligence that operators need for protection. Operators, in turn, hold technical and operational information that may be unavailable to government. Effective prevention therefore depends on trusted information-sharing mechanisms, clear responsibilities and appropriate safeguards.

Intelligence can reduce relevant uncertainty, identify vulnerabilities, recognise patterns and create decision opportunities, but it cannot guarantee prevention.

Intelligence should also map infrastructure dependencies and possible cascading effects. The distinction between a localised technical incident and an event capable of propagating across sectors can determine the appropriate level of response. The ultimate objective is not intelligence collection as an end in itself, but reduction of vulnerability through continuity planning, redundancy, protective investment and recovery capacity.

NATO, the European Union and European security

The North Atlantic Treaty Organization (NATO) and the European Union (EU) approach hybrid threats from different but complementary institutional positions. NATO contributes through collective defence, intelligence, preparedness, deterrence and resilience. The EU combines situational awareness with regulatory, economic, diplomatic and internal-security instruments.

The EU's NIS2 and Critical Entities Resilience (CER) frameworksⁱ address complementary dimensions of systemic risk: cybersecurity and the resilience of critical entities. NATO's resilience requirements similarly emphasise preparedness, con-

tinuity, redundancy and the management of strategic dependencies. These developments point towards a broader European security architecture in which intelligence, infrastructure protection and resilience are increasingly connected.

The emerging architecture should not be understood as a single centralised warning system. Its effectiveness depends on interoperability among national authorities, EU institutions, NATO structures, infrastructure operators and other relevant actors. Complementarity is therefore more important than institutional duplication.

Whole-of-society resilience is particularly significant because the security of critical infrastructure depends on public authorities, regulators, operators, technology providers, law enforcement, emergency services and technical communities. Intelligence must circulate across these communities in forms that are actionable while respecting legal and democratic constraints.

Legal and democratic constraints

Preventive intelligence operates within legal and democratic governance. The need to act under uncertainty does not remove requirements concerning legality, necessity, proportionality, data protection, privacy, accountability and oversight.

Three distinctions are essential. Detection is not attribution. Attribution is not legal responsibility. Intelligence assessment is not authorisation. These distinctions help prevent analytical uncertainty from being converted into unjustified operational or political conclusions.

Artificial intelligence and automated analytics can support correlation, anomaly detection and processing of large datasets, but they do not eliminate the need for human validation, contextual assessment and scrutiny of bias and false positives. The preventive chain should therefore combine technological assistance with accountable human judgement.

The PIEW framework: Limits and research agenda

The PIEW Framework remains conceptual. Its principal limitations include differences among national and institutional warning cultures, variable data quality, attribution uncertainty, uneven public-private information sharing and the difficulty of measuring prevention when the relevant



outcome is an incident that did not occur. Future empirical research could test whether shorter detection-to-decision intervals are associated with improved protective outcomes; whether cross-domain fusion improves recognition of hybrid campaigns; which information-sharing arrangements most effectively support critical-infrastructure operators; and how warning thresholds can be calibrated without generating excessive false alarms. The framework nevertheless provides a useful analytical lens because it treats intelligence as part of an infrastructure of prevention rather than as an isolated collection function.

Conclusion

Hybrid competition changes the conditions under which European security is organised. Threats may combine cyber, informational, economic and physical instruments while exploiting technological and infrastructural dependencies. Critical infrastructure is therefore both an object of protection and a potential source of cascading vulnerability.

Intelligence can reduce relevant uncertainty, identify vulnerabilities, recognise patterns and create decision opportunities, but it cannot guarantee prevention. Its strategic value depends on institutional connectivity: information must become warning, warning must reach decision-makers, decisions must activate protective measures, and outcomes must generate learning.

The PIEW framework captures this preventive cycle through six functions: detection; fusion and interpretation; early warning and anticipation; decision activation; protection and resilience; and learning and adaptation. Its purpose is not to prescribe a single organisational model, but to clarify the conditions under which intelligence can contribute to infrastructure resilience.

For Europe, the challenge is consequently to strengthen connections among national intelligence and security structures, EU mechanisms, NATO capabilities and infrastructure operators while maintaining legal and democratic safeguards. In an emerging international order marked by persistent ambiguity and multidomain competition, the ability to convert knowledge into timely, lawful and coordinated action is itself a component of strategic security. ●

<https://doi.org/10.26619/2183-4822.2026.CJ.26>

Note

¹ The EU's NIS2 Directive and the Critical Entities Resilience (CER) Directive form a dual legislative framework designed to secure essential digital and physical infrastructure across the European Union: the NIS2 Directive focuses strictly on cybersecurity, network security, and digital risk management, while the CER Directive focuses on physical and operational resilience against natural disasters, sabotage, physical attacks, and insider threats.

References

- Council of the European Union. (2026, March 16). *Council adopts conclusions on advancing the EU's capacity to counter hybrid threats*. Council of the European Union.
- European Parliament & Council of the European Union. (2022a). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union*, L 333, 80-152.
- European Parliament & Council of the European Union. (2022b). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. *Official Journal of the European Union*, L 333, 164-198.
- Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42-79. https://doi.org/10.1162/isec_a_00351
- Herman, M. (1996). *Intelligence power in peace and war*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511521737>
- Kent, S. (1966). *Strategic intelligence for American world policy*. Princeton University Press.
- Lowenthal, M. (2022). *Intelligence: From secrets to policy* (9th ed.). CQ Press.
- NATO. (2026a). *Countering hybrid threats*. The North Atlantic Treaty Organization.
- NATO. (2026b). *Joint intelligence, surveillance and reconnaissance*. The North Atlantic Treaty Organization.
- NATO. (2026c). *2026 resilience baseline requirements*. The North Atlantic Treaty Organization.
- Nilsson, N., Weissmann, M., & Palmertz, B. (2026). Hybrid threats and the intelligence community: Priming for a volatile age. *International Journal of Intelligence and Counterintelligence*, 39(1), 109-131. <https://doi.org/10.1080/08850607.2024.2435265>
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.