Mattermost

Sovereignty Under Fire

What Resilience Laws and Real Incidents Reveal About Operational Control

Executive Brief

Across Europe and allied environments, recent incidents have revealed a consistent pattern: governance and coordination arrangements that appear sound in steady state often fail under operational stress.

When crises occur, three factors determine whether organisations respond effectively:

1. How quickly authority can be exercised
2. How cleanly decisions can be escalated
3. How completely the decision trail can be reconstructed afterwards

Collaboration environments sit at the centre of these outcomes. They are no longer workplace tools — they are operational infrastructure.

For senior defence and public-sector leaders, the evaluation of collaboration and operational systems is shifting. The question is no longer which platform offers the most capable feature set. It is whether the systems underpinning command, coordination, and continuity will hold under the conditions that actually matter — contested environments, cross-border incidents, and the compressed timelines that crises impose.

Collaboration environments are the infrastructure through which those questions are answered. Evaluating them on features alone is a category error. The risk is infrastructure level. The evaluation must be too.

This shift has not emerged from policy debate. It has been established by what breaks — and when — across live incidents and oversight reviews in Europe and allied environments. Regulation has followed, not led.

Sovereignty as an Operational Requirement

When a targeted attack on the Viasat KA-SAT network disrupted Ukrainian military communications in February 2022, the effects did not stay within military boundaries. Civilian broadband users across multiple European countries lost connectivity. Wind farm management systems went offline.

The incident exposed something that planning assumptions had not fully absorbed: digital dependencies span national borders, private operators, and alliance structures simultaneously — and their full extent becomes visible only when disruption occurs. What also became immediately visible, was how quickly the absence of clear authority and coordinated escalation paths compounds the damage.

That is the operational reality sovereignty policy is now designed to address. The European Parliament defines digital sovereignty as Europe's capacity to act autonomously in the digital domain while remaining open and connected — emphasising security, resilience, and continuity of critical functions rather than isolation from global technology partners. ENISA frames it in operational terms: digital strategic autonomy is the capability to design, deploy, and operate critical digital infrastructures under EU control, because geopolitical pressure and supply-chain disruption can remove that capability without warning.

The European Commission's Cloud Sovereignty Framework translates these concerns into enforceable conditions — control over data location, immunity from non-EU jurisdictional interference, continuity of operations, and the verified ability to switch providers. The framework links sovereignty directly to crisis management: institutions must sustain operational capability in the event of provider failure, legal conflict, or geopolitical stress. The European Organisation for Security reinforces the point: sourcing critical cybersecurity elements outside Europe risks jeopardising continuity of operational capabilities. Digital autonomy is not about withdrawal from alliances — it is about preserving the assured ability to act within them when conditions deteriorate.

Accountability Has Moved to Leadership

The pattern identified in incident after incident is consistent. Governance weaknesses that appear manageable under normal conditions become operationally consequential when tempo increases and decisions must be made quickly. How fast an organisation can mobilise, how coherently it can escalate, and how clearly it can account for its decisions afterwards are not outcomes that emerge from good intentions under pressure. They are products of choices made — or deferred — well in advance.

Regulatory frameworks have registered this reality by placing accountability where the risk actually sits. Under NIS2, cybersecurity risk management and incident response obligations fall directly on the management bodies of essential and important entities. Boards and senior executives must approve measures, oversee implementation, and bear personal liability for failures. Temporary prohibition from managerial functions is an available sanction for serious breach. These are not compliance formalities — they reflect a deliberate decision to locate accountability at the level where governance choices are made.

The incident reporting timelines embedded in NIS2 give that accountability operational force. An early warning within twenty-four hours. A full notification within seventy-two hours. A final report within one month. Those timelines are not administrative targets, they measure whether authority is clear, escalation works, and decisions can be reconstructed afterwards. Organisations that encounter their first serious incident without having resolved those questions in advance will find the timelines impossible to meet. The clock does not adjust for unresolved governance questions.

The Critical Entities Resilience framework extends the same logic into physical and operational continuity, requiring risk assessments and sustained delivery of critical services across a broad range of threats, including hybrid. ENISA's cyber stress-testing guidance makes the underlying distinction explicit: having controls in place and being able to sustain services under stress are not the same thing. Stress tests assess whether organisations can maintain critical services during and after significant incidents. Evaluators examine governance maturity and escalation coherence not the existence of documented frameworks. Competent authorities may issue binding instructions, which means boards must be able to evidence control over systems, providers, and data flows under conditions that may already be degraded.

The Governance Risk of Feature-Led Decisions

The governance risks introduced by feature-led decisions about collaboration infrastructure do not surface during procurement. They surface during incidents — when decision velocity drops, escalation stalls, and the audit trail needed to account for what happened does not exist.

Cross-border outages have required reporting through multiple national channels simultaneously, with genuine ambiguity over which authority held primary responsibility and how information should flow at EU level. Where that clarification takes time, situational awareness degrades for all actors at once. A single software update to a widely deployed security agent in 2024 produced cascading disruption across aviation, banking, health, and government systems across multiple countries. Coordinated recovery required visibility across interdependencies that organisations had not previously mapped. The accountability consequences were public and immediate.

These failures were not feature failures. They were infrastructure failures in the governance structures, authority lines, and coordination arrangements that determine how collaboration environments perform when operational conditions deteriorate. Selecting systems on the basis of interface capability and nominal security controls does not reveal those failure modes, it defers them.

The European Parliament's digital sovereignty analysis identifies the structural vulnerability: dependence on a small number of non-EU cloud and platform providers creates exposure to foreign jurisdictions, limits the ability to enforce EU standards, and introduces the risk that access conditions or lawful access regimes change in ways that constrain European decision-making at precisely the moment it is most needed. The Commission's Cloud Sovereignty Framework treats jurisdiction, auditability, and exit strategies as central risk dimensions — not considerations to be weighed after feature comparison.

ENISA's stress-testing guidance draws the same conclusion from a different direction: traditional audits and certifications, which focus on documented controls and service features, must be complemented by scenario-based tests that surface resilience gaps and interdependencies affecting continuity. ENISA's sectoral assessments of public administration identify concentration risk as a system-level concern: widely adopted collaboration infrastructure, if concentrated in a few providers, can create single points of failure at sector or EU level. The concern is not usability, it is control, concentration, and the coherence of coordinated recovery.

In EU crisis-management settings, ENISA is direct: large-scale incidents may require rapid decisions on restricting traffic, sharing sensitive information, or invoking crisis mechanisms. Those decisions depend on clear authority over infrastructure and data. Feature-led procurement does not automatically provide that authority, and incidents do not wait while it is established.

The governance risks introduced by feature-led decisions about collaboration infrastructure do not surface during procurement. **They surface during incidents.**

Coalition Operations as a Test of Real Conditions

Multi-jurisdiction and coalition operations are where governance and coordination assumptions encounter conditions they were not designed for — and where the time taken to establish authority, synchronise escalation, and produce a coherent operational picture determines whether a collective response is possible at all.

Operational experience from Ukraine illustrates what sustained adversarial pressure reveals. Maintaining command and communication arrangements under persistent cyber and electronic warfare required multiple pathways, adaptive switching, and local autonomy that conventional architectures had not assumed. Resilience depended not on the capabilities of individual systems in normal conditions, but on redundancy and the capacity to adapt when primary systems were unavailable. These conditions are now treated as planning baselines, not contingencies.

ENISA's work on EU incident response and cyber crisis management identifies the coordination challenge directly: cross-border incidents require shared situational awareness and coordinated decision-making by national and EU bodies, supported by exercises and procedures that test the capacity to act collectively under time pressure. ENISA's stress-testing framework extends this across national, regional, and EU-wide levels, explicitly assessing control and authority gaps across sectors and jurisdictions.

Analysis of NATO's digital backbone identifies a persistent gap between stated interoperability ambitions and the governance mechanisms, standardisation, and shared procedures required to deliver them under operational conditions. Interoperability is not a property of individual systems — it is a property of agreed authority structures and tested procedures. In multi-national settings, fragmented approaches and siloed development produce coordination friction precisely when coherent collective action is most required.

European policy analysis on strategic autonomy highlights that many critical digital technologies underpinning defence and security are dominated by non-EU actors, creating vulnerabilities in coalition operations where EU actors depend on external systems for situational awareness, command, and logistics.

The pattern that emerges is consistent. In multi-jurisdiction operations — whether EU crisis response or NATO digital backbone initiatives — the decisive factors are clarity of authority, shared governance mechanisms, and assured control over infrastructure and data. The maturity or usability of individual collaboration platform features is not among them.

Analysis of NATO's digital backbone identifies a persistent gap between stated interoperability ambitions and the governance mechanisms, standardisation, and shared procedures required to deliver them under operational conditions.

The Evaluation Criteria That Now Apply

For senior defence and public-sector leaders, these developments establish a clear direction. Sovereignty and control are no longer considerations to weigh against feature sets. They are prerequisite evaluation criteria for collaboration infrastructure in defence and regulated environments — established not by policy preference, but by what incidents have shown to matter.

Collaboration environments that underpin command, coordination, and continuity of essential functions must be evaluated as the infrastructure they are. That means assessing behaviour under contested and degraded conditions, clarity of authority and governance during incidents, auditability and forensic traceability, and the capacity to coordinate across jurisdictions and coalitions. It also means ensuring organisations retain operational control of the coordination layer itself — including where it runs, how it integrates with mission systems, and how decisions are captured and governed. It means evaluating what happens when primary systems are unavailable, when legal regimes intersect, and when the speed with which authority can be exercised and decisions reconstructed is the difference between containment and escalation. Feature-level assessment addresses none of this.

EU digital sovereignty is defined operationally: the ability to retain control, continuity, and authority under disruption. NIS2 and the Critical Entities Resilience framework shift accountability for operational resilience and incident response explicitly to senior leadership, requiring demonstrable control rather than assumed assurance. EU and NATO crisis-management frameworks confirm that coordination, authority, and shared governance — not tool usability — determine effectiveness under pressure.

The implication is direct. In sovereign and coalition environments, misclassifying collaboration infrastructure as a productivity tool carries operational consequences. Authority becomes ambiguous, escalation slows, and the ability to account for decisions after the fact disappears. Mean Time to Ready, Respond, and Recover is not a technical performance metric. It is a governance outcome, determined by how clearly authority is exercised, how quickly decisions escalate, and how completely the decision trail can be reconstructed.

Sources Referenced

- Directive (EU) 2022/2555 (NIS2 Directive), European Parliament and Council, 2022
- Directive (EU) 2022/2557 (Critical Entities Resilience Directive), European Parliament and Council, 2022
- Government Cyber Resilience, UK National Audit Office, 2025
- Handbook for Cyber Stress Tests, European Union Agency for Cybersecurity (ENISA), 2025
- Telecom Security Incidents 2024 – Annual Summary of Incident Reports, European Union Agency for Cybersecurity (ENISA), 2025
- Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted against Ukraine (KA-SAT satellite network), Council of the European Union, 2022
- AJP-6 Allied Joint Doctrine for Communications and Information Systems, NATO, 2025
- NATO Strategic Concept, NATO, 2022
- UAE Information Assurance Regulation (Version 1.1), Telecommunications and Digital Government Regulatory Authority, United Arab Emirates, 2020
- National Information Assurance Framework (NIAF), Government of the United Arab Emirates, 2014
- Essential Cybersecurity Controls (ECC – 2024 – EN), National Cybersecurity Authority, Kingdom of Saudi Arabia, 2024