

Verified Interoperability: Information Integrity and Cyber Resilience in NATO Federated Tactical Networks

Efthymia Koliokosta

efigrx@yahoo.com

University of the Aegean: Panepistemio Aigaiou <https://orcid.org/0000-0001-5439-5536>

Research Article

Keywords: information integrity, cyber resilience, interoperability, C4ISR, Federated Mission Networking, data provenance

Posted Date: September 23rd, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11118648/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Abstract

Digital interoperability is central to contemporary military effectiveness, enabling federated C4ISR systems, tactical data links and distributed sensors to support shared situational awareness across platforms, services and national boundaries. Yet increased connectivity also creates dependence on the integrity, provenance, timeliness and trustworthiness of exchanged information, particularly in multinational alliances where interoperability coexists with national sovereignty and differentiated disclosure policies. This article develops the Information Integrity and Resilience Assessment Model (IIRAM), a structured framework for evaluating information-integrity risk using non-classified, system-independent variables. IIRAM integrates five risk categories—communication degradation, data inconsistency, endpoint uncertainty, source unreliability and governance failure—with six resilience dimensions covering identity assurance, data provenance, multisource corroboration, redundancy, trust-domain governance, and detection, recovery and adaptation. A synthetic application and sensitivity analysis demonstrate operationalisation and weighting robustness. The Greece–Türkiye case is used to illustrate “interoperability without unconditional trust”. The article advances the concept of verified interoperability and proposes a Trusted Operational Picture, shifting emphasis from information sharing alone to the assessable reliability of information supporting mission-critical decisions

1. Introduction

Contemporary military capability increasingly depends on information generated outside the individual platform undertaking an operational task, a trend associated with networked and system-of-systems approaches to defence capability (Liwång et al. 2023). Aircraft, ships, land formations, command centres, space-based assets and distributed sensors can contribute information to wider command-and-control architectures, allowing decision-makers to build operational awareness from multiple sources (Looney 2001; NCIA 2025). Within NATO practice, these interconnected functions are commonly described through C4ISR—Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance— which integrates data-gathering platforms, communications and information-processing technologies in support of political and military situational awareness and decision-making (NCIA 2025). The effectiveness of an individual platform therefore increasingly depends on the quality, interoperability and resilience of the wider C4ISR information ecosystem within which it operates (Liwång et al. 2023; NATO ACT 2025).

NATO's digital transformation reflects this shift. The Alliance's Digital Transformation Implementation Strategy links digital transformation to multi-domain operations, interoperability, situational awareness and data-driven decision-making (NATO 2024). The Alliance's Data Strategy subsequently treats data as an enduring strategic asset and emphasises interoperability, security, curation and trust as foundations for decision-making and military effectiveness (NATO 2025a). The Data Quality Framework formalises dimensions including accuracy, completeness, consistency, timeliness, validity and granularity while emphasising provenance and lineage as determinants of information quality (NATO 2025b). The Alliance Digital Strategy further connects digital transformation with secure-by-design systems, Zero Trust,

resilient mission-critical services and diversified communications arrangements based on the PACE principle (NATO 2026a). This policy trajectory is consistent with wider analyses of NATO's institutional adaptation to cyber and emerging operational domains (Burton 2015; Gottemoeller et al. 2022; Shea 2025).

Networked operations provide substantial benefits, but also generate information dependence. Multi-source fusion and common operational pictures can improve situational awareness by combining observations that no single platform necessarily possesses independently (Looney 2001; Steen-Tveit and Munkvold 2021). A communications network may nevertheless remain technically available, while the information distributed through it becomes delayed, inconsistent, incomplete or unreliable (Feng et al. 2021; NATO 2025b). Conversely, a technically degraded network may remain operationally useful when alternative pathways, independent sources and effective verification mechanisms preserve sufficient information confidence (Goldman, McQuaid and Picciotto 2011; Ross et al. 2021). Cybersecurity in C4ISR environments should therefore be considered not merely as protection of networks, but also as protection of the information quality and decision processes that those networks support (Ross et al. 2021; NATO 2026a).

The problem becomes more complex in multinational alliances. Interoperability requires systems belonging to different states to exchange information, while sovereignty requires states to preserve control over national information, capabilities and disclosure decisions (Brannsten et al. 2015; Paananen 2026). NATO's Federated Mission Networking (FMN) framework addresses this through federation rather than complete centralisation: national and NATO capabilities can be connected through common standards, services and governance while participating entities retain control of their own systems (Brannsten et al. 2015; NATO ACT 2026). NATO's Data Strategy similarly combines Alliance-wide sharing with data-centric security and originator-defined controls (NATO 2025a).

This article introduces the concept of interoperability without unconditional trust. The phrase does not imply political distrust among Allies; rather, it distinguishes institutional cooperation from the technical assumption that every user, device, service or data object should be trusted automatically. NATO's current data policy explicitly limits sharing to authorised users and systems and preserves originator-defined controls (NATO 2025a), while Zero Trust architecture rejects implicit trust based solely on network location, affiliation or ownership (Rose et al. 2020). Secure multinational information exchange therefore depends on bounded permissions, authenticated identities, mission-specific authorisations, provenance and controlled information release (Rose et al. 2020; NATO 2025a). This interpretation is also compatible with research showing that NATO can integrate military cyber effects while states retain sensitive information about the underlying capabilities that generate those effects (Jensen 2022).

The article addresses three research questions. First, how can information-integrity risk in federated military networks be assessed without requiring classified technical vulnerability data? Second, which technical and organisational resilience dimensions most directly influence the ability of a networked force to maintain trustworthy situational information? Third, how does the coexistence of interoperability

and nationally retained information control affect the conceptualisation of trust within a military alliance?

To answer these questions, the study develops the Information Integrity and Resilience Assessment Model (IIRAM), applies it to a synthetic information environment, and uses Greece and Türkiye as an institutional case through which to interpret bounded trust in an alliance setting. The case is not a war-game and does not assess national combat effectiveness, classified network configurations or exploitable vulnerabilities. The analysis relies exclusively on open, non-classified material.

2. Interoperability, federation and the information problem

Interoperability is often treated as a technical question of compatibility, but contemporary defence scholarship increasingly presents it as a multidimensional organisational problem (Paananen 2026). Paananen (2026), for example, conceptualises interoperability as an intertwined phenomenon spanning military, political, operational and institutional levels, while Liwång et al. (2023) argue that defence capability development requires systemic treatment of interactions between technological and social components. These perspectives are particularly relevant to C4ISR and tactical networking because the capability produced by a data link depends not only on radios and message standards but also on sensors, software, operators, doctrine, authentication mechanisms, data rules and command relationships (Sorroche 2012; Brannsten et al. 2015). NATO's interoperability exercises likewise treat digital interoperability as a prerequisite for effective multi-domain C4ISR capabilities rather than as a narrow communications objective (NATO ACT 2025).

Tactical data links are designed to exchange structured tactical information among participating units and to support compatibility and interoperability across command-and-control and communications systems (Sorroche 2012; US Department of Defense 2024). Link 16, for example, is standardised specifically to enable interoperable information exchange among US and coalition forces in joint tactical operations (US Department of Defense 2024). As C4ISR enablers, tactical data links connect surveillance and platform information with wider command-and-control processes, allowing observations from distributed nodes to contribute to a common or shared picture (Sorroche 2012; Looney 2001). This aggregation can improve situational awareness and reduce exclusive dependence on the organic sensors of a single platform (Looney 2001; Steen-Tveit and Munkvold 2021). Distributed architectures, however, also create data-management and consistency problems. Feng et al. (2021) identify data inconsistency among tactical data-link entities as a substantive challenge, while Huang, Li and Zhang (2024) frame reliable tactical data-link performance as a resilience problem under communications adversity.

FMN extends the interoperability problem beyond a single tactical link and toward the federation of wider C4ISR services. Brannsten et al. (2015) describe the challenges of extending service-oriented interoperability, messaging, collaboration, discovery and security services into the tactical domain. NATO's current FMN framework similarly combines people, processes and technology to support

command and control and decision-making through improved information sharing across national and organisational boundaries (NATO ACT 2026). Federation is significant because it does not abolish national boundaries; instead, it governs interaction between independently controlled capabilities (Brannsten et al. 2015; NATO ACT 2026).

Three distinctions follow from the federated model. Technical compatibility does not equal information entitlement, because interoperable standards define how exchange can occur rather than who is authorised to receive every data object (US Department of Defense 2024; NATO 2025a). Alliance membership does not equal unrestricted network access, because NATO's data principles explicitly distinguish discoverability, accessibility, sharing and security for authorised users and systems (NATO 2025a). Interoperability therefore does not equal unconditional trust. A shared technical standard establishes the possibility of exchange under appropriate conditions, while governance determines whether exchange occurs, what information is released and how trust is established for a given mission (Brannsten et al. 2015; NATO ACT 2026).

2.1 Information integrity beyond confidentiality and availability

Information security is commonly concerned with preserving confidentiality, integrity and availability, while contemporary cybersecurity frameworks additionally emphasise governance, identification, protection, detection, response and recovery as interconnected risk-management outcomes (Pascoe, Quinn and Scarfone 2024). In operational C4ISR environments, integrity has a particularly direct relationship with decision-making because an encrypted and available message can still contain inaccurate, stale or internally inconsistent information (NATO 2025b). A user may also be legitimately authenticated while relying on an information source whose quality or reliability has degraded (NATO 2025b; Ross et al. 2021). For mission assurance, the question is therefore not only whether information is protected and available, but whether it remains sufficiently trustworthy for the decision it is intended to support (Goldman, McQuaid and Picciotto 2011; Ross et al. 2021).

For this reason, information integrity should be analysed at the level of the decision environment rather than exclusively at the level of individual packets, databases or communication channels. Research on common operational pictures shows that decision support depends on the quality of the fused representation presented to commanders, not merely on the successful transport of individual data elements (Looney 2001; Steen-Tveit and Munkvold 2021). NATO's Data Quality Framework supports this broader interpretation by evaluating whether data are accurate, complete, consistent, timely, valid and sufficiently granular for their intended use (NATO 2025b).

Provenance and lineage become particularly important as data-centric C4ISR architectures introduce additional processing stages. NATO defines provenance in terms of data origin, historical context and authenticity, while lineage concerns how data move and change across systems and processes (NATO 2025b). A simplified chain may run from sensor to local processor, data service, fusion process,

analytical system, command interface and finally a human decision-maker; information can be transformed at each stage (Looney 2001; NATO 2025b). Knowing that information arrived through an authorised network therefore does not by itself establish that it remains sufficiently accurate, current or reliable for a particular decision (NATO 2025a, 2025b).

2.2 Zero Trust, resilience and mission assurance

Zero Trust provides a useful conceptual foundation for federated military and C4ISR information systems. NIST SP 800 – 207 rejects the assumption that trust should be granted solely because a user or device occupies a particular network location, belongs to a particular organisation or is owned by a trusted enterprise (Rose et al. 2020). Authentication and authorisation are instead associated with specific subjects, devices and resources and are evaluated before access is established (Rose et al. 2020). NATO's 2026 Alliance Digital Strategy incorporates comparable principles of continuous verification, least privilege and secure handling of data, users and systems as part of mission assurance and digital resilience (NATO 2026a).

Zero Trust should not be confused with zero political trust. Strategic and institutional trust can coexist with continuous technical verification because the two concepts operate at different analytical levels (Rose et al. 2020; Paananen 2026). Political and institutional trust enables cooperation, while technical verification limits the consequences of misplaced or overly broad implicit trust. In this sense, reducing implicit technical trust may permit greater explicit information sharing because access decisions can be tied to specific identities, resources and purposes rather than inferred from general network membership (Rose et al. 2020; NATO 2025a).

Cyber resilience adds a second conceptual layer. Prevention seeks to reduce the likelihood of adverse events, whereas resilience assumes that disruption, degradation or compromise may nevertheless occur and focuses on maintaining mission-relevant functions under those conditions (Goldman, McQuaid and Picciotto 2011; Ross et al. 2021). NIST SP 800 – 160 Vol. 2 frames cyber resilience around the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises (Ross et al. 2021). Earlier mission-assurance work similarly argues that critical systems must continue essential functions even when defensive measures fail or components are compromised (Goldman, McQuaid and Picciotto 2011). NATO's 2026 digital strategy operationalises the same logic through resilient mission-critical services, diversified technical solutions and PACE-based continuity (NATO 2026a).

For tactical C4ISR environments, the resulting question is not simply whether disruption can be prevented. It is whether the organisation can continue to construct a sufficiently reliable operational picture when one or more communications paths, sources, endpoints or organisational relationships become uncertain (Goldman, McQuaid and Picciotto 2011; Ross et al. 2021). This shifts assessment from component survival alone toward mission-level information assurance and decision support.

3. Methodology

The study adopts a theory-building and framework-development design. IIRAM is not presented as a statistically calibrated probability model. It is a structured, transparent and reproducible assessment framework intended for comparative analysis and later empirical validation. The framework deliberately uses variables that can be evaluated without disclosure of classified system characteristics.

Development followed four stages. First, constructs related to information integrity, resilience, verification and federation were identified from authoritative NATO and NIST frameworks and from peer-reviewed literature on defence interoperability, C4ISR, cyber resilience, tactical data links and systems capability (Brannsten et al. 2015; Rose et al. 2020; Ross et al. 2021; Liwång et al. 2023; NATO 2025a, 2025b). Second, overlapping concepts were consolidated into risk and resilience dimensions suitable for federated military information environments. Third, ordinal scoring rules were developed so that the constructs could be applied consistently without implying false probabilistic precision. Fourth, a synthetic case and alternative weighting structures were used to examine the internal behaviour and sensitivity of the model. The resulting design follows a theory-building logic in which established constructs are recombined for a specific analytical problem rather than presented as a statistically validated predictive instrument.

The construct mapping provides external theoretical anchoring. Identity and Access Assurance draws primarily on Zero Trust, continuous verification and least-privilege principles (Rose et al. 2020; NATO 2026a). Data Provenance and Integrity draws on NATO's data-quality, provenance and lineage concepts (NATO 2025a, 2025b). Multisource Corroboration reflects information-fusion and consistency concerns identified in common-operational-picture and tactical data-link research (Looney 2001; Feng et al. 2021). Communications and Service Redundancy draws on cyber-resilience, mission-assurance and continuity principles (Goldman, McQuaid and Picciotto 2011; Ross et al. 2021; NATO 2026a). Trust-Domain Governance reflects FMN's federated structure, controlled information sharing and nationally retained authority (Brannsten et al. 2015; NATO 2025a; NATO ACT 2026). Detection, Recovery and Adaptation derives directly from contemporary cyber-resilience engineering (Ross et al. 2021).

The methodology has two deliberate boundaries. It does not identify weaknesses in particular national systems, and it does not model techniques for bypassing authentication, cryptography or tactical-network safeguards. The unit of analysis is therefore information resilience at the architectural and governance level rather than exploitability at the component level.

4. The Information Integrity and Resilience Assessment Model (IIRAM)

IIRAM separates two analytical components: Initial Information Risk, describing conditions capable of degrading the reliability of an operational information environment, and Resilience Capacity, describing the ability of the socio-technical C4ISR system to continue producing trustworthy information despite those conditions. This distinction reflects the mission-assurance literature's separation between exposure to adverse cyber conditions and the capacity to sustain essential functions despite disruption

(Goldman, McQuaid and Picciotto 2011; Ross et al. 2021). The combination produces a residual information-integrity indicator suitable for comparing notional architectures, governance arrangements or capability-development options without evaluating classified vulnerabilities.

Five risk categories are used: communication degradation, data inconsistency or corruption, endpoint or processing uncertainty, source unreliability and governance or trust failure (Table 1). These categories are deliberately cause-neutral because degraded information can result from hostile activity, equipment failure, software defects, configuration errors, data incompatibility, human error or policy misalignment (Feng et al. 2021; Ross et al. 2021; NATO 2025b). Decision-makers may initially observe the operational effect before they can establish the underlying cause; IIRAM therefore prioritises the reliability of the resulting information environment rather than attributing every anomaly to malicious cyber activity.

For each risk category i , the initial risk score is calculated as

$$IR_i = L_i \times V_i \times M_i \quad (1)$$

where L represents likelihood or exposure, V represents vulnerability or dependence and M represents potential mission consequence (Koliokosta, 2025). Each component is scored on a five-point ordinal scale (Table 2). The maximum individual risk score is therefore 125.

For n risk categories, Normalised Initial Risk is

$$NIR = \sum IR_i / (125n) \quad (2)$$

producing a value between 0 and 1.

The ordinal interpretation is intentionally conservative. A score of 4 is not assumed to represent precisely twice the probability or consequence of a score of 2. The scale is a prioritisation device, not a probabilistic estimator. This distinction is essential because otherwise a simple risk matrix could create an appearance of mathematical precision unsupported by empirical data.

Table 1
IIRAM information-risk categories and analytical questions.

Code	Risk category	Analytical question
R1	Communication degradation	Can required information reach authorised users reliably and in time?
R2	Data inconsistency or corruption	Can contradictory, incomplete or erroneous information enter the operational picture?
R3	Endpoint or processing uncertainty	Can confidence in a participating device, software process or interface become uncertain?
R4	Source unreliability	Can an underlying sensor or information source become degraded or insufficiently verified?
R5	Governance and trust failure	Can permissions, release rules, responsibilities or organisational misunderstandings reduce information assurance?

Table 2
IIRAM scoring criteria for risk and resilience.

Score	Likelihood	Vulnerability / dependence	Mission consequence	Resilience maturity
1	Rare or exceptional	Minimal dependence; substitutes readily available	Negligible effect	Minimal or largely absent
2	Uncommon	Limited dependence	Localised, short-lived degradation	Partial; predominantly ad hoc
3	Plausible	Moderate dependency	Noticeable degradation requiring adaptation	Defined capability with important limitations
4	Likely under adverse conditions	High dependency	Major degradation of decision support	Mature, redundant and regularly exercised
5	Persistent / high exposure	Critical dependency with few substitutes	Mission-critical information failure	Highly mature, continuously verified and adaptive

4.1 Resilience dimensions and the Resilience Capacity Index

Six complementary resilience dimensions are evaluated (Fig. 1), each addressing a distinct failure mode within a federated Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) environment:

1. Identity and Access Assurance (IAA), which captures the degree of confidence that users, devices and digital services are correctly authenticated, continuously validated and granted only the privileges required for their operational role. This dimension is particularly important in federated architectures because compromise of a single identity or endpoint can propagate across interconnected domains; accordingly, IAA reflects the Zero Trust principle that trust should not be assumed on the basis of network location or organisational affiliation alone (Rose et al. 2020; NATO 2026a).
2. Data Provenance and Integrity (DPI) that evaluates whether information can be traced to its origin, whether subsequent transformations are visible, and whether its content can be verified as complete and unaltered. In C4ISR systems, the operational value of information depends not merely on availability, but also on the ability of decision-makers and automated systems to determine where that information originated, how it was processed and whether its integrity has been preserved. Provenance therefore provides an evidential chain of trust, while integrity mechanisms reduce the risk that corrupted, manipulated or contextually distorted data are incorporated into operational decision-making (NATO 2025a, 2025b).
3. Multisource Corroboration (MSC), which assesses the extent to which operationally significant information can be independently confirmed, contradicted or qualified through alternative sensors, intelligence streams, platforms or organisations. The purpose of MSC is not simply to increase the number of available sources, but to reduce dependence on any single information channel and to improve confidence through comparison of partially independent observations. This is particularly important where sources may be incomplete, uncertain, deceptive or mutually inconsistent, making information fusion and source reconciliation central to resilient situational awareness (Looney 2001; Feng et al. 2021). A system with high information volume but low source independence may therefore remain vulnerable to common-mode error or coordinated deception.
4. Communications and Service Redundancy (CSR), which measures the capacity to preserve essential information flows and mission services when primary communication links, platforms or digital services are degraded or unavailable. Resilience in this dimension depends not only on the existence of backup assets, but also on whether alternative pathways are sufficiently independent, interoperable and rapidly deployable to sustain priority functions. Consequently, CSR captures both structural redundancy and the practical ability to re-route communications, substitute services and maintain operational continuity under disrupted conditions (Ross et al. 2021; NATO 2026a). This distinction is important because nominal duplication does not necessarily provide resilience where redundant systems share the same infrastructure, dependencies or failure mechanisms.
5. Trust-Domain Governance (TDG) that addresses the institutional and procedural dimension of resilience by assessing whether access policies, ownership responsibilities, information-release rules and decision rights are clearly defined across organisational and national boundaries. Federated C4ISR architectures frequently connect actors operating under different security classifications, legal frameworks, operational authorities and risk tolerances. In such environments, technical interoperability alone is insufficient: unclear responsibility for information ownership, release authority or incident response can delay information exchange or create inconsistent trust

decisions. TDG therefore evaluates whether governance arrangements are sufficiently explicit, coordinated and enforceable to support secure and timely information sharing across trust domains (Brannsten et al. 2015; NATO 2025a; NATO ACT 2026).

6. Finally, Detection, Recovery and Adaptation (DRA), which measures the capacity of the system to identify abnormal or degraded conditions, contain affected components, restore trusted functionality and modify operating procedures in response to evolving threats or failures. Whereas CSR focuses primarily on maintaining functionality through alternative resources, DRA captures the temporal and adaptive aspects of resilience: recognising that degradation has occurred, determining which components or information can still be trusted, recovering essential capabilities and incorporating lessons into subsequent operations. This dimension therefore links resilience to continuous monitoring, incident response, recovery planning and adaptive reconfiguration rather than treating resilience as a purely static property of system design (Ross et al. 2021).

Taken together, the six dimensions represent resilience as a multi-layered system property rather than a purely technical characteristic. IAA establishes confidence in who and what may participate, DPI establishes confidence in the information itself, MSC tests whether that information can be independently validated, CSR determines whether essential functions can continue despite disruption, TDG governs how trust and information-sharing decisions are coordinated across organisational boundaries and DRA determines whether the system can recognise, recover from and adapt to degradation. The dimensions are therefore analytically distinct but operationally interdependent. For example, redundant communications have limited value if the alternative channel cannot authenticate participants, while multisource corroboration may provide little protection if several sources depend on the same compromised data chain. The framework consequently treats C4ISR resilience as an emergent capability arising from the interaction of technical assurance, information trustworthiness, organisational governance and adaptive recovery rather than from any single control or subsystem.

The six dimensions were selected using a functional coverage principle rather than an assumption of conceptual exhaustiveness. The objective was to identify a parsimonious set of dimensions capable of representing the principal mechanisms through which a federated C4ISR environment can resist, absorb, recover from and adapt to disruption. Existing resilience and cybersecurity literature repeatedly emphasises identity assurance, information integrity, redundancy, monitoring, recovery and adaptive response as central elements of resilient digital systems (Rose et al. 2020; Ross et al. 2021).

In parallel, the specific characteristics of federated military information environments introduce additional requirements concerning multisource validation, information provenance and governance across heterogeneous organisational and trust domains (Looney 2001; Feng et al. 2021; NATO 2025a, 2025b; NATO ACT 2026). The resulting six-dimensional structure therefore combines established cyber-resilience principles with C4ISR-specific information and governance requirements (Fig. 1). Importantly, the dimensions are designed to minimise conceptual duplication. For example, CSR concerns continuity through alternative communications and service pathways, whereas DRA concerns the detection, containment, restoration and subsequent adaptation that follow degradation. Similarly, DPI concerns the

trustworthiness and traceability of individual information objects, whereas MSC concerns the independent confirmation of claims across multiple sources. The framework is therefore intended as a bounded, operationally interpretable model of resilience, rather than as an exhaustive ontology of C4ISR resilience.

Each resilience dimension receives an ordinal score from 1 to 5. A score of 1 indicates that resilience mechanisms are minimal, largely absent or implemented only informally; a score of 5 represents a highly mature capability characterised by systematic implementation, continuous verification, redundancy, regular testing and adaptive recovery mechanisms. Intermediate scores represent progressively higher levels of resilience maturity. To combine all six dimensions within one composite index, the original 1–5 scores are transformed onto a common 0–1 scale using the normalized value:

$$c'_i = (c_i - 1) / 4 \quad (3)$$

The transformation subtracts the minimum possible score (1) and divides by the full range of the scale ($5 - 1 = 4$), so the mapping becomes $1 \rightarrow 0.00$, $2 \rightarrow 0.25$, $3 \rightarrow 0.50$, $4 \rightarrow 0.75$ and $5 \rightarrow 1.00$. For example, a raw score of 4 for Multisource Corroboration becomes $c'_i = (4 - 1) / 4 = 0.75$. The normalised value should not be interpreted as a probability or as a literal statement that a capability is '75% resilient'; it represents the dimension's relative position within the IIRAM maturity scale. Normalisation places all dimensions on the same bounded scale and permits their aggregation in the Resilience Capacity Index,

$$RCI = \sum (w_i \times c'_i) \quad (4)$$

where the weights sum to 1, $\sum w_i = 1$. Equal weighting is recommended for the initial application because no empirical evidence is yet available to justify privileging one resilience dimension over another; alternative weighting assumptions are therefore examined through sensitivity analysis rather than embedded as untested model premises.

Residual Information-Integrity Risk is then expressed as

$$RIR = NIR \times (1 - RCI) \quad (5)$$

The resulting value is not a probability of mission failure. It is a comparative indicator designed to show how resilience capacity moderates a consistent initial-risk construct. A high-threat environment need not produce high residual risk if the architecture is sufficiently resilient, while moderate exposure may still create substantial residual risk when the system depends on single points of failure.

5. Synthetic application and sensitivity analysis

To demonstrate the framework without evaluating a real national military network, the analysis uses a Notional Federated Air Information Environment (NFAIE). The scenario is entirely synthetic and does not reproduce an operational network configuration. The five risk categories receive illustrative likelihood,

vulnerability and mission-impact scores shown in Table 3. The total raw score is 208 out of a theoretical maximum of 625, giving $NIR = 0.333$.

The notional resilience scores are $IAA = 4$, $DPI = 3$, $MSC = 4$, $CSR = 4$, $TDG = 4$ and $DRA = 3$. Under equal weighting, the normalised scores produce $RCI = 0.667$. Residual risk is therefore $RIR = 0.333 \times (1 - 0.667) \approx 0.111$. Again, this value should not be read as an 11.1 per cent probability of operational failure; it is a comparative residual-risk index.

Sensitivity analysis addresses the possibility that results could depend heavily on arbitrary weighting. Three alternative weighting structures were evaluated: a data-centric structure that gives greater weight to provenance and corroboration, a continuity-centric structure that emphasises service redundancy and recovery and a governance-centric structure that emphasises trust-domain governance and recovery (Table 4). Across these alternatives, the illustrative RIR varied only from approximately 0.111 to 0.116. The narrow range suggests that this synthetic result is not highly sensitive to reasonable changes in weighting, although it does not validate the weights themselves.

A second test holds NIR constant at 0.333 while varying resilience maturity. If all resilience dimensions score 2, $RCI = 0.25$ and $RIR \approx 0.250$. If all score 3, $RCI = 0.50$ and $RIR \approx 0.166$. If all score 4, $RCI = 0.75$ and $RIR \approx 0.083$. This behaviour corresponds with the model's theoretical expectation: resilience reduces residual information risk without assuming that the underlying threat disappears.

Table 3
Synthetic IIRAM application to a Notional Federated Air Information Environment.

Risk category	L	V	M	Raw risk
Communications degradation	4	3	5	60
Data inconsistency	3	3	4	36
Endpoint uncertainty	2	4	5	40
Source unreliability	3	4	4	48
Governance failure	2	3	4	24
Total				208

Table 4
Sensitivity of residual risk to alternative weighting assumptions.

Weighting structure	Emphasis	Illustrative RIR
Equal weighting	All six resilience dimensions weighted equally	0.111
Data-centric	Greater weight to provenance and multisource corroboration	0.116
Continuity-centric	Greater weight to communications redundancy and recovery	0.112
Governance-centric	Greater weight to trust-domain governance and recovery	0.112

6. Multisource corroboration and the Trusted Operational Picture

Multisource corroboration is central to the model because operational pictures are commonly constructed by combining information from multiple sensors or reporting nodes (Looney 2001). Additional sources can reduce dependence on a single observation, but the simple number of sources is a poor measure of confidence because apparently separate feeds may share the same upstream origin or failure mode. Information-fusion research therefore emphasises association, correlation, consistency and source quality rather than simple accumulation (Looney 2001), while research on shared operational pictures shows that useful situational understanding depends on how information is interpreted and coordinated among participants (Steen-Tveit and Munkvold 2021). Three systems that repeat information originating from the same underlying feed should therefore not be treated as three fully independent confirmations.

This can be expressed conceptually as

$$CE = f(N, I, Q, T) \quad (6)$$

where CE is corroboration effectiveness, N is the number of relevant sources, I is their independence, Q is information quality and T is timeliness. The variables reflect established information-fusion and data-quality concerns, particularly the need to reconcile source multiplicity with accuracy, consistency and temporal relevance (Looney 2001; NATO 2025b). Diversity may therefore be more important than simple redundancy: two pathways vulnerable to the same failure mechanism can provide less resilience than two technologically or organisationally distinct pathways (Ross et al. 2021).

The analysis consequently proposes the concept of a Trusted Operational Picture (TOP). A TOP is defined here as a dynamically generated representation of the operational environment in which authorised users can assess not only the content of information but also sufficient characteristics of its provenance, integrity, timeliness, corroboration and confidence to support mission-relevant decision-making.

The distinction is important. A Shared Operational Picture asks whether participants are receiving compatible and sufficiently common information; a Trusted Operational Picture additionally asks what confidence decision-makers should place in that information and why. Research on common operational pictures already demonstrates that shared representation is only an intermediate step toward common situational understanding and coordinated decision-making (Steen-Tveit and Munkvold 2021). TOP extends that logic by making data quality, provenance, corroboration and confidence explicit properties of the C4ISR information environment, consistent with NATO's emphasis on trusted data, provenance, lineage and quality metadata (NATO 2025a, 2025b).

6.1 From interoperability to verified interoperability

The traditional interoperability question is whether system A can exchange information with system B, a concern reflected in tactical data-link standards and FMN specifications (US Department of Defense 2024; Brannsten et al. 2015). A data-centric operational environment requires a more demanding question: can information be exchanged while preserving sufficient assurance regarding identity, authority, provenance, integrity and reliability (NATO 2025a, 2025b; NATO 2026a)? This article calls the latter verified interoperability.

Verified interoperability contains five attributes: compatibility, authorisation, provenance, corroboration and resilience. Compatibility ensures that systems can exchange interpretable information, consistent with the purpose of tactical data-link and FMN standards (US Department of Defense 2024; Brannsten et al. 2015). Authorisation ensures that access corresponds to defined permissions and least-privilege principles (Rose et al. 2020; NATO 2026a). Provenance makes relevant information about origin and transformation available (NATO 2025b). Corroboration allows important information to be compared against additional evidence (Looney 2001). Resilience allows critical information functions to continue when components or services degrade (Ross et al. 2021; NATO 2026a).

The progression can therefore be expressed as Connectivity → Interoperability → Verified Interoperability → Trusted Operational Picture. The sequence represents increasing assurance rather than simply increasing network connectivity.

7. Greece–Türkiye as an institutional case of bounded trust

Greece and Türkiye provide an analytically useful institutional case because both are NATO Allies that participate in Alliance structures while retaining national command, security and information domains (NATO 2020). The purpose of the case is not to model bilateral conflict or assess operational advantages. It is to illustrate a more general alliance problem: common standards and institutional cooperation can coexist with differentiated permissions, separate national control and explicit mechanisms for managing military interaction (NATO 2020; NATO 2025a).

NATO established a bilateral military de-confliction mechanism in October 2020 following technical meetings between Greek and Turkish military representatives, with the stated purpose of reducing the

risk of incidents and accidents and with a secure hotline to facilitate de-confliction at sea and in the air (NATO 2020). The mechanism is analytically significant because it demonstrates that resilience is not solely technological: institutional communication pathways can complement tactical and C4ISR systems when events are ambiguous or intentions require clarification. The case therefore adds a governance layer to the technical resilience concepts captured by IIRAM.

The case also illustrates why common standards should not be confused with universal information access. Tactical interoperability standards define message structures, compatibility and procedures for information exchange, but they do not themselves create a universal entitlement to all data held by every interoperable participant (US Department of Defense 2024). NATO's data strategy likewise specifies that data are shared with authorised users and systems while remaining subject to security, confidentiality and originator-defined controls (NATO 2025a). Two Allies may therefore operate systems compliant with the same standards while those systems remain part of separately governed national C4ISR environments.

This relationship is described here as bounded trust. Participants accept common standards and processes, but information sharing remains conditioned by identity, mission, purpose, classification, originator rules and authorisation—features consistent with NATO's controlled-sharing and federated-governance principles (NATO 2025a; NATO ACT 2026). Bounded trust is not necessarily a weakness. It can be an architectural requirement for sustainable multinational cooperation because states may be more willing to share sensitive information when the environment preserves differentiated permissions and national control, an observation consistent with NATO's pragmatic integration of nationally retained cyber capabilities (Jensen 2022).

The case further supports a layered understanding of resilience. Information assurance exists at machine-to-machine, system-to-system, operator-to-operator, command-to-command and state-to-state levels, reflecting the broader socio-technical nature of interoperability identified in defence capability research (Liwång et al. 2023; Paananen 2026). Technical networking and C4ISR integration can strengthen the first three layers, but they cannot entirely substitute for command relationships, governance and political communication. Alliance resilience must therefore be understood as both technical and institutional (Burton 2015; Paananen 2026).

8. Discussion

The central argument of this article is that modern military interoperability creates both capability and dependence. Distributed sensing, tactical data links and C4ISR networking can improve situational awareness by pooling information across platforms and organisations (Sorroche 2012; Looney 2001; NCIA 2025). The same dependence on distributed information increases the consequences of inconsistency, delay or source degradation (Feng et al. 2021; NATO 2025b). More connectivity can therefore amplify accurate information and inaccurate information alike. The decisive variable is not connectivity alone but trusted connectivity.

IIRAM addresses this by separating initial information risk from resilience capacity. The model does not assume that cyber or communications threats can be eliminated; instead, it asks whether technical, informational and organisational arrangements allow decision-makers to continue receiving sufficiently trustworthy information despite degradation. This perspective aligns with the broader movement in cyber resilience away from perimeter protection alone and toward anticipation, continuity, recovery and adaptation (Goldman, McQuaid and Picciotto 2011; Ross et al. 2021). It also aligns with NATO's current emphasis on trusted data, continuous verification and resilient mission-critical services (NATO 2025a; NATO 2026a).

The framework also extends existing defence-interoperability literature. FMN scholarship has long highlighted the importance of common services, security and federation at the tactical edge (Brannsten et al. 2015), while recent work emphasises interoperability as multidimensional coordination rather than simple technical compatibility (Paananen 2026). Defence Studies scholarship has additionally traced NATO's institutional adaptation to cyber operations and emerging technological domains (Burton 2015; Gottemoeller et al. 2022; Shea 2025). IIRAM contributes to these literatures by placing information integrity, confidence and C4ISR resilience at the centre of the interoperability problem rather than treating successful connectivity as the end state.

The Greece–Türkiye case illustrates why this matters inside alliances. Common technical standards facilitate cooperation but do not eliminate sovereignty or create unrestricted information sharing (NATO 2025a; US Department of Defense 2024). This should not automatically be interpreted as incomplete interoperability because federated arrangements are specifically designed to connect independently controlled capabilities (Brannsten et al. 2015; NATO ACT 2026). Secure federation may therefore depend on combining interoperability with controlled trust boundaries. Jensen's (2022) analysis of NATO offensive cyber capabilities offers a parallel: Allies can integrate military effects without full disclosure of the sensitive capabilities underlying them.

The theoretical contribution can be summarised in four concepts. First, tactical-network cyber resilience is reframed as an information-integrity problem, not merely a communications-security problem. Second, bounded trust provides a model for multinational information exchange. Third, verified interoperability distinguishes technical compatibility from trustworthy exchange. Fourth, the Trusted Operational Picture extends shared situational awareness by making confidence, provenance and corroboration explicit properties of the operational information environment.

9. Implications for NATO and defence capability development

The framework produces several implications for defence management, C4ISR capability development and digital transformation. Information integrity should be treated as a defence capability and assessed alongside communications availability because operational decision-making depends on the quality of the information delivered through networked systems (Looney 2001; NATO 2025b). NATO's current digital and data strategies similarly treat trusted, quality data and resilient mission-critical services as

prerequisites for decision-making and operational advantage (NATO 2025a, 2025b; NATO 2026a). The ability to determine that information is timely, appropriately sourced and sufficiently reliable should therefore be included explicitly in capability-development objectives.

Data provenance should become increasingly important as information passes through more automated processing layers. In data-centric C4ISR architectures, a decision-maker may receive an assessment that has been transformed by multiple services, fusion processes or analytical tools rather than directly from a single sensor (Looney 2001; NATO 2025b). Provenance and lineage offer mechanisms for preserving traceability and confidence across this chain (NATO 2025b), particularly as automated fusion and AI-assisted analysis become more common within military information systems (NATO 2025a).

Zero Trust should be interpreted as an enabler of multinational cooperation rather than an expression of political distrust. Continuous authentication, least privilege and resource-specific authorisation can make sharing safer because access is granted for defined purposes rather than inferred from broad organisational or network membership (Rose et al. 2020). NATO's 2026 Alliance Digital Strategy adopts these principles explicitly as part of mission assurance and digital resilience (NATO 2026a). In a federated C4ISR environment, stronger verification can therefore support rather than undermine cross-organisational information exchange.

Multisource corroboration should be designed around source independence. Information-fusion architectures derive value from combining distinct observations, but duplicated or correlated upstream sources can create an illusion of independent confirmation (Looney 2001). Redundant systems affected by the same underlying failure mechanism may similarly provide less resilience than heterogeneous sources or pathways that fail differently (Ross et al. 2021). C4ISR capability-development processes should therefore distinguish simple duplication from genuine diversity in sensing, transport and processing.

Resilience planning should also apply the PACE logic—Primary, Alternate, Contingency and Emergency—to information functions rather than only to communications devices. NATO's Alliance Digital Strategy explicitly calls for redundant and diversified technical solutions based on PACE to preserve mission-critical services (NATO 2026a). For C4ISR, the relevant question is therefore not merely which radio or network replaces another, but which alternative combination of sources, services and procedures preserves the minimum trusted picture required for safe decision-making when the primary information pathway is degraded.

Finally, interoperability exercises should increasingly test information quality rather than successful connectivity alone. NATO's CWIX programme already provides a federated environment for testing digital interoperability and explicitly links that testing to multi-domain C4ISR capabilities and enhanced situational awareness (NATO ACT 2025). A resilience-oriented extension should examine whether provenance survives cross-system exchange, whether confidence metadata remain interpretable, whether contradictory sources can be recognised, whether systems degrade gracefully and whether alternative information functions remain usable when primary services fail (NATO 2025b; Ross et al.

2021). The desired end state should therefore move from 'information successfully exchanged' toward 'information successfully exchanged, verified, interpreted and trusted'.

10. Limitations and validation pathway

IIRAM is currently a conceptual and semi-quantitative framework. Its numerical structure should not be interpreted as a validated probability model. Scoring contains expert judgement, and different evaluators may assign different values to the same notional architecture. The synthetic test demonstrates mathematical behaviour rather than empirical predictive accuracy.

The framework also simplifies interactions among resilience variables. Communications redundancy may offer limited protection when multiple pathways depend on the same infrastructure. Multisource corroboration may be misleading when apparently independent sources share the same upstream feed. Trust-domain governance can be strong on paper but weakened by implementation. These dependencies justify future empirical research rather than greater mathematical complexity at the conceptual stage.

A three-stage validation pathway is proposed. First, Delphi-based expert elicitation could assess construct relevance, indicator completeness, scoring definitions and weighting priorities using specialists in defence cybersecurity, C4ISR, data governance, systems engineering and defence policy. Second, multiple experts could independently score identical synthetic cases, allowing inter-rater reliability to be tested. Third, the framework could be applied to controlled exercises or simulations in which selected information functions are deliberately degraded, allowing IIRAM outputs to be compared with observed decision-quality or mission-assurance measures.

Future research could also develop a dynamic Information Confidence Index combining source reliability, independence, timeliness, provenance and consistency. Bayesian updating could adjust confidence as corroborating or contradictory information becomes available. Network-analysis methods could identify information dependencies and concentration around critical classes of nodes without disclosing specific vulnerabilities. AI-enabled command-and-control will create additional questions concerning algorithmic provenance, training-data quality and confidence in machine-generated assessments.

11. Conclusion

Digital military capability increasingly depends on the integrity of information moving among distributed systems and organisations. Tactical data links, FMN and broader C4ISR architectures allow forces to exploit information generated beyond the sensors of an individual platform and to support shared situational awareness across organisational boundaries (Sorroche 2012; Brannsten et al. 2015; NCIA 2025). This increases both capability and dependence, making information quality and resilience increasingly relevant to mission assurance (Goldman, McQuaid and Picciotto 2011; NATO 2025b). Future interoperability therefore cannot be evaluated exclusively by whether systems can communicate.

The more important question is whether decision-makers can continue to determine which information deserves confidence when the information environment becomes contested, degraded or uncertain. IIRAM provides a structured method for examining this problem without requiring classified technical vulnerability information. Its central proposition—that residual information risk depends simultaneously on exposure and resilience capacity—builds on the broader cyber-resilience principle that systems should anticipate, withstand, recover from and adapt to adverse conditions (Ross et al. 2021). Authentication, provenance, independent corroboration, service redundancy, trust governance, detection and recovery all contribute to that capacity (Rose et al. 2020; NATO 2025b; NATO 2026a).

The Greece–Türkiye institutional case demonstrates that alliance interoperability does not require unconditional technical trust. NATO's own de-confliction mechanism illustrates the coexistence of Alliance membership, military interoperability and additional institutional arrangements for managing bilateral military interaction (NATO 2020). More generally, states can share standards, procedures and mission structures while retaining national control over information, consistent with FMN federation and NATO's originator-controlled data principles (Brannsten et al. 2015; NATO 2025a; NATO ACT 2026). Federated cooperation may be sustainable precisely because trust can remain bounded and verifiable.

The resulting model of verified interoperability moves beyond simple connectivity. Its ultimate objective is not merely a Shared Operational Picture but a Trusted Operational Picture in which the quality, provenance and confidence of C4ISR information are assessable alongside its availability (NATO 2025a, 2025b). In increasingly data-centric military environments, advantage may depend not only on who possesses more information, but on who can determine more quickly and reliably which information should be trusted.

Declarations

Competing interests:

The author declares no known financial or personal relationships that could have appeared to influence the work reported in this paper.

Ethics statement

Not applicable. The study uses no human participants, animals, personal data or classified operational data.

Funding:

No external funding was received for this study.

Author contribution:

Efthymia Koliokosta was responsible for conceptualisation, methodology, analysis, visualisation, writing-original draft and writing-review and editing.

Data availability:

No external empirical dataset was used. All values in the synthetic IIRAM application are illustrative and are reported in the article.

References

1. Brannsten MR, Johnsen FT, Bloebaum TH, Lund K (2015) Toward federated mission networking in the tactical domain. *IEEE Commun Mag* 53(10):52–58.
<https://doi.org/10.1109/MCOM.2015.7295463>
2. Burton J (2015) NATO's cyber defence: strategic challenges and institutional adaptation. *Def Stud* 15(4):297–319. <https://doi.org/10.1080/14702436.2015.1108108>
3. Feng W, Li Y, Yang X, Yan Z, Chen L (2021) *Digit Commun Networks* 7(3):285–294.
<https://doi.org/10.1016/j.dcan.2020.05.007>. 'Blockchain-based data transmission control for Tactical Data Link'
4. Goldman H, McQuaid R, Picciotto J (2011) 'Cyber resilience for mission assurance', 2011 IEEE International Conference on Technologies for Homeland Security, pp. 236–241.
<https://doi.org/10.1109/THS.2011.6107877>
5. Gottemoeller R, Hedgecock K, Magula J, Poast P (2022) Engaging with emerged and emerging domains: cyber, space, and technology in the 2022 NATO Strategic Concept. *Def Stud* 22(3):516–524. <https://doi.org/10.1080/14702436.2022.2082955>
6. Huang Z, Li J, Zhang A (2024) A tactical data link model based on CCSK-FMSK. *Phys Communication* 64:102345. <https://doi.org/10.1016/j.phycom.2024.102345>
7. Jensen MS (2022) Five good reasons for NATO's pragmatic approach to offensive cyberspace operations. *Def Stud* 22(3):464–488. <https://doi.org/10.1080/14702436.2022.2080661>
8. Koliokosta E (2025) Concepts and Misconceptions in Climate Change Risk Assessment: Considerations for Sea Level Rise and Extreme Precipitation Risk. *J Geoscience Environ Prot* 13:178–214. [10.4236/gep.2025.131010](https://doi.org/10.4236/gep.2025.131010)
9. Liwång H, Andersson KE, Bang M, Malmio I, Tärnholm T (2023) How can systemic perspectives on defence capability development be strengthened? *Def Stud* 23(3):399–420.
<https://doi.org/10.1080/14702436.2023.2239722>
10. Looney CG (2001) Exploring fusion architecture for a common operational picture. *Inform Fusion* 2(4):251–260. [https://doi.org/10.1016/S1566-2535\(01\)00043-4](https://doi.org/10.1016/S1566-2535(01)00043-4)

11. NATO (2020) 'Military de-confliction mechanism between Greece and Turkey established at NATO', 1 October. Available at: https://www.nato.int/cps/en/natohq/news_178523.htm (accessed 21 September 2026)
12. NATO (2024) NATO's Digital Transformation Implementation Strategy. Brussels: North Atlantic Treaty Organization. Available at: https://www.nato.int/cps/en/natohq/official_texts_229801.htm (accessed 21 September 2026)
13. NATO (2025a) Data Strategy for the Alliance. Brussels: North Atlantic Treaty Organization. Available at: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/05/05/data-strategy-for-the-alliance> (accessed 21 September 2026)
14. NATO (2025b) Data Quality Framework for the Alliance. Brussels: North Atlantic Treaty Organization. Available at: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/08/29/data-quality-framework-for-the-alliance> (accessed 21 September 2026)
15. NATO (2026a) Alliance Digital Strategy. Brussels: North Atlantic Treaty Organization, 13 January. Available at: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/01/13/alliance-digital-strategy> (accessed 21 September 2026)
16. NATO Allied Command Transformation (NATO ACT) (2025) 'CWIX25 starts now! NATO's largest digital interoperability exercise kicks off', 3 June. Available at: <https://www.act.nato.int/article/cwix25-starts-jftc/> (accessed 21 September 2026)
17. NATO Allied Command Transformation (NATO ACT) (2026) Federated Mission Networking. Norfolk, VA: Allied Command Transformation. Available at: <https://www.act.nato.int/activities/federated-mission-networking/> (accessed 21 September 2026)
18. NATO Communications and Information Agency (NCIA) (2025) 'NCIA and Finland sign new Memorandum of Understanding for C4ISR capabilities', 25 November. Available at: <https://www.ncia.nato.int/newsroom/news/ncia-and-finland-sign-new-memorandum-of-understanding-for-c4isr-capabilities> (accessed 21 September 2026)
19. Paananen S (2026) Interoperability: an intertwined phenomenon requiring multidimensional and multilevel coordination and cooperation. *Scandinavian J Military Stud* 9(1):174–190. <https://doi.org/10.31374/sjms.364>
20. Pascoe C, Quinn S, Scarfone K (2024) The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD: National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.29>
21. Rose S, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture. NIST Special Publication 800 – 207. National Institute of Standards and Technology, Gaithersburg, MD. <https://doi.org/10.6028/NIST.SP.800-207>
22. Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800 – 160, Vol. 2 Rev. 1. Gaithersburg, MD: National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-160v2r1>

23. Shea J (2025) Space and cyberspace: NATO's new frontier of defence. Def Stud 25(3):690–698.
<https://doi.org/10.1080/14702436.2025.2474069>
24. Sorroche J (2012) Modeling Tactical Data Links. In: Tolk A (ed) Engineering Principles of Combat Modeling and Distributed Simulation. Wiley, Hoboken, NJ. Chap. 23
<https://doi.org/10.1002/9781118180310.ch23>.
25. Steen-Tveit K, Munkvold BE (2021) From common operational picture to common situational understanding: an analysis based on practitioner perspectives. Saf Sci 142:105381.
<https://doi.org/10.1016/j.ssci.2021.105381>
26. US Department of Defense (2024) MIL-STD-6016: Tactical Data Link (TDL) 16 Message Standard. Washington, DC: Department of Defense. Available at:
https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=123964 (accessed 21 September 2026)

Figures

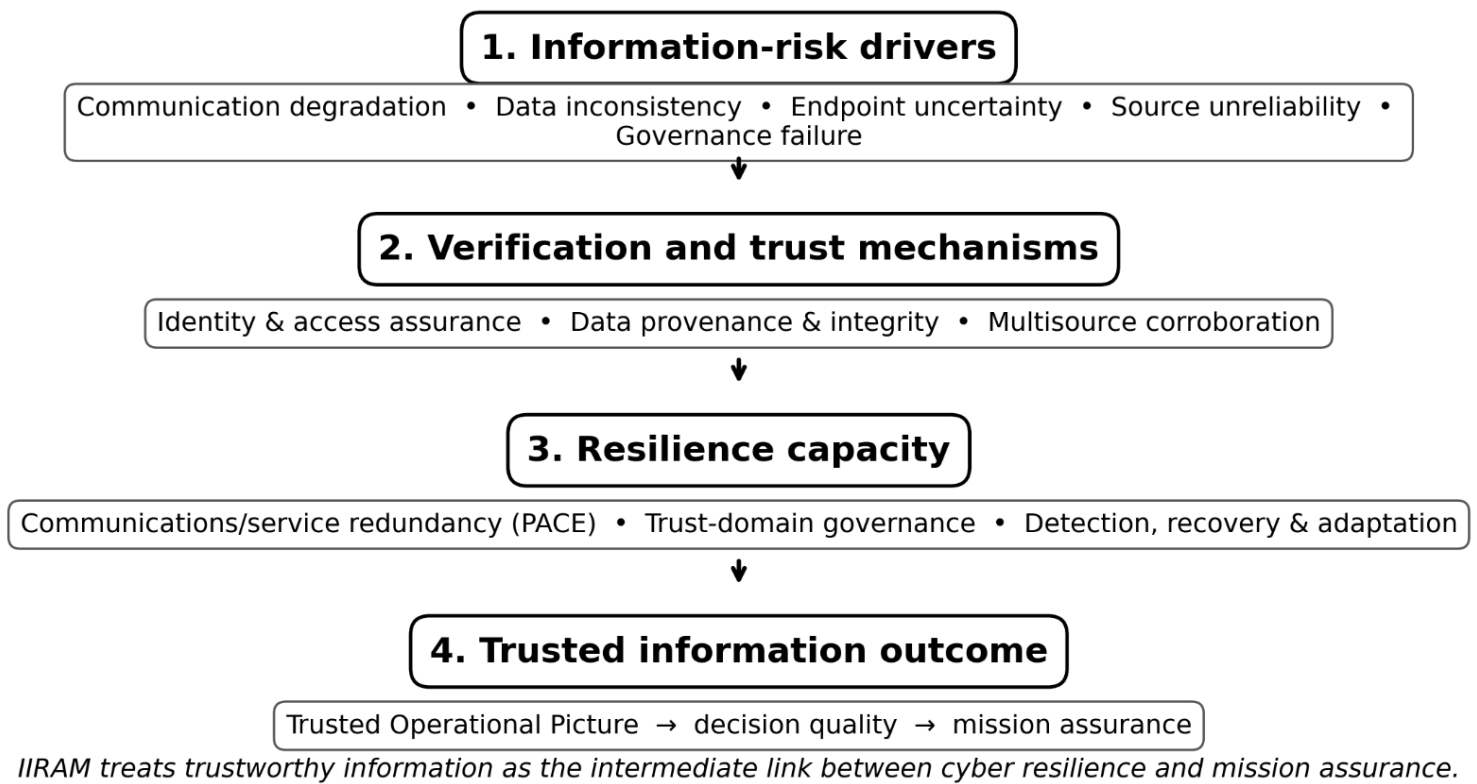


Figure 1

Information Integrity and Resilience Assessment Model (IIRAM): from information-risk drivers to trusted operational information and mission assurance.

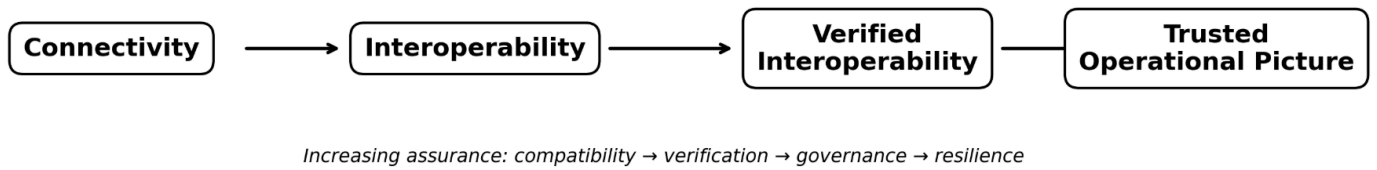


Figure 2

Analytical progression from connectivity to a Trusted Operational Picture.