

# STRATEGIC DIMENSIONS OF INFORMATION SECURITY ASSURANCE IN MILITARY NETWORKS IN THE CONTEXT OF CONTEMPORARY DEFENCE DOCTRINE

Fiodor Timercan<sup>1</sup>

---

*Delivered:* 19.6.2026.

*Language:* English

*Corrected:* 13.8.2026.

*Type of paper:* Review paper

*Accepted:* 9.9.2026.

*DOI number:* 10.5937/vojdelo2603167T

---

**A**bstract: Information security assurance has become a critical component of contemporary military capability, given the increasing reliance on networked systems for command, control, communication, and decision-making. Modern defence doctrines increasingly recognize that military networks are not only technical infrastructures, but also strategic assets whose integrity, availability, and confidentiality directly influence operational effectiveness and strategic resilience. This paper examines the strategic dimensions of information security assurance in military networks within the context of contemporary defence doctrine.

The study explores how information security considerations are integrated into doctrinal frameworks and strategic planning processes, emphasizing their role in supporting command and control, safeguarding decision superiority, and enhancing resilience against cyber and hybrid threats. By adopting a conceptual and analytical approach, the paper highlights the relationship between information security assurance, military strategy, and defence policy, rather than focusing solely on technical protection mechanisms. Particular attention is given to the implications of information security failures for operational continuity and strategic stability in modern conflict environments.

The analysis demonstrates that effective information security assurance requires a comprehensive approach that combines technical measures with organizational, doctrinal, and strategic elements. The paper argues that integrating information security assurance into defence doctrine is essential for maintaining operational credibility and ensuring the effective employment of military networks in contemporary and future security environments.

**Keywords:** *information security assurance; military networks; defence doctrine; military strategy; cyber and hybrid threats*

---

<sup>1</sup> "Alexandru cel Bun" Armed Forces Military Academy, Republic of Moldova, e-mail: [timercantudor@yahoo.com](mailto:timercantudor@yahoo.com), <https://orcid.org/0009-0001-6769-3556>

## Introduction

The contemporary security environment is characterized by persistent competition, rapid technological transformation, and the progressive dissolution of the traditional distinction between war and peace. Military organizations operate within a continuum of strategic rivalry where kinetic engagement represents only one manifestation of confrontation. Within this evolving landscape, information has become a decisive element of power projection and operational effectiveness.

Cyberspace is now formally recognized as an operational domain, alongside land, air, maritime, and space (NATO, 2020). This recognition reflects more than conceptual modernization; it acknowledges the structural dependence of modern armed forces on digital infrastructures. Military networks sustain command and control functions, intelligence fusion, targeting processes, logistics coordination, and multinational interoperability. Their integrity directly influences operational tempo, decision-making accuracy, and force survivability.

Contemporary defence doctrine increasingly emphasizes multi-domain operations, integration of joint capabilities, and accelerated decision cycles (U.S. Department of the Army, 2022). These developments amplify reliance on secure and resilient information systems. Network-centric approaches, while enhancing situational awareness and coordination, simultaneously expand the attack surface available to adversaries (Alberts & Garstka, 1998). State and non-state actors exploit vulnerabilities through advanced persistent threats, supply chain manipulation, cyber espionage, electronic warfare integration, and hybrid influence operations. Under such conditions, information security assurance transcends technical administration and becomes a matter of strategic resilience.

Military networks are no longer isolated infrastructures protected by static perimeter defenses. They are dynamic, distributed, and interconnected ecosystems. Coalition operations, multinational commands, and interoperability frameworks require data exchange across different security architectures and regulatory environments. This interconnectedness enhances operational capability but also introduces systemic vulnerabilities. Strategic assurance must therefore balance openness required for cooperation with controlled access necessary for protection.

The shift from reactive cybersecurity to resilience-based security architecture reflects doctrinal adaptation to adaptive adversaries. Absolute protection is unattainable in contested cyberspace. Strategic advantage lies in the capacity to detect, contain, recover, and adapt while maintaining operational continuity. Concepts such as layered defense, zero trust architecture, secure-by-design engineering, and continuous monitoring are increasingly embedded in military planning. These are not technical preferences but strategic necessities (U.S. Department of Defense, 2023).

The integration of artificial intelligence, autonomous systems, and cloud-based infrastructures further complicates the security landscape. Decision-support algorithms, sensor fusion platforms, and predictive analytics depend on data integrity and software reliability. Compromise at the data or algorithmic level may distort operational awareness and strategic judgment. Information security assurance must therefore encompass protection of data provenance, validation of algorithms, and secure lifecycle management of digital capabilities (European Commission, 2020).

Network compromise carries strategic consequences beyond immediate operational disruption. Breaches undermine deterrence credibility, expose force structure vulnerabilities, and may alter adversarial calculations. In the contemporary environment, the perception of cyber weakness can be as strategically damaging as physical force degradation. Information security assurance thus contributes directly to national resilience and strategic signaling.

Effective implementation requires alignment between doctrine, policy, organizational structure, and operational culture. Cybersecurity cannot remain confined to specialized technical units. It must be integrated into command responsibility, planning processes, and training regimes. Discipline in digital practices, awareness at leadership level, and institutionalized security culture form essential components of strategic assurance.

In an era defined by accelerated information flows and compressed decision cycles, the protection of military networks is inseparable from the preservation of combat power. Digital infrastructure represents both a vulnerability and a strategic asset. Ensuring its resilience is no longer a supporting function; it is a foundational requirement of contemporary defence doctrine.

## Strategic positioning of information security within contemporary defence doctrine

The contemporary security environment is defined by persistent strategic competition, accelerated technological transformation, and the erosion of clear boundaries between peace and conflict. Within this framework, military effectiveness depends not only on kinetic capability but on the integrity of digital infrastructures that sustain command authority and operational coordination. Information security assurance is therefore positioned as a structural component of defence doctrine rather than a peripheral technical function.

The formal recognition of cyberspace as an operational domain reconfigures how vulnerability and protection are conceptualized in military planning. Allied doctrine establishes that Communication and Information Systems (CIS) are mission-critical assets whose protection is essential for operational continuity across strategic, operational,

and tactical levels (NATO Standardization Office, 2024). Information assurance, defined through the protection of availability, integrity, and confidentiality of information systems, directly conditions the effectiveness of command and control processes.

Operational doctrine further emphasizes that modern joint operations depend on synchronized effects across land, maritime, air, space, and cyber domains. This integration is enabled through interconnected digital networks that aggregate sensor inputs, intelligence products, targeting data, and logistical information into unified decision environments. Any degradation of these systems generates cascading operational consequences: delayed decision cycles, distorted situational awareness, and reduced force synchronization (NATO Standardization Office, 2025).

The structural centrality of military networks is conceptually illustrated by the architecture of the Department of Defense Information Network (DoDIN), previously known as the Global Information Grid (NIST, 2007). The model reflects the interconnected digital backbone that supports joint and combined operations.

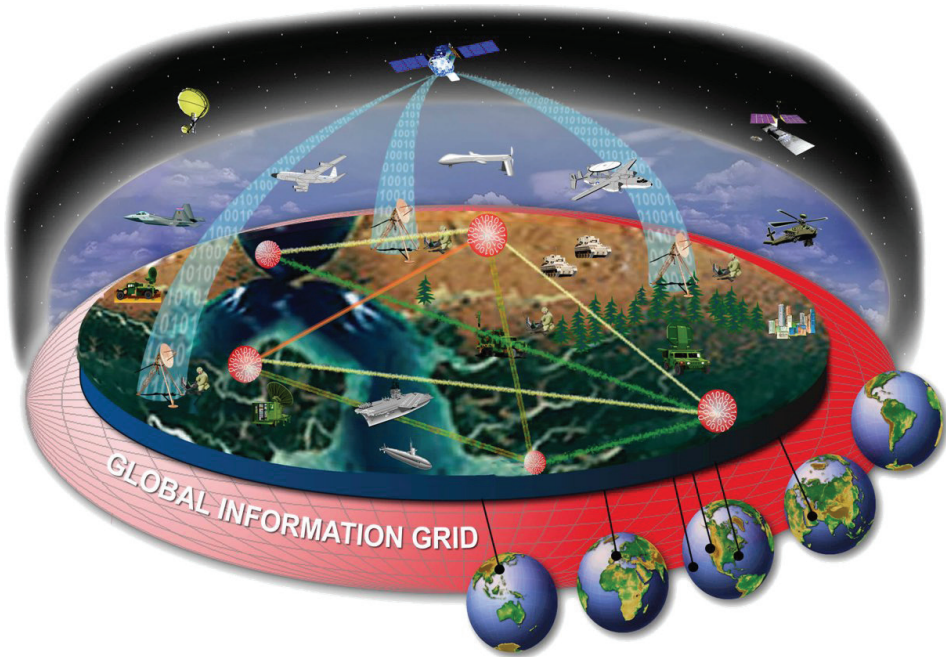


Fig. 1: Schematic view of the Global Information Grid (GIG), representing the interconnected information capabilities supporting the collection, processing, storage, dissemination, and management of information across the defence environment.

Source: National Institute of Standards and Technology (NIST, 2007)

The figure 1 demonstrates the integration of operational domains through shared digital infrastructure. It highlights a critical doctrinal reality: operational effectiveness is inseparable from network reliability. The same connectivity that enables rapid coordination also expands the attack surface available to adversaries. Under such conditions, assurance mechanisms become strategic enablers of mission continuity.

The conceptual foundations of network-centric warfare further reinforce this dependency. Shared situational awareness and distributed decision-making architectures increase operational agility but simultaneously amplify systemic vulnerability if data integrity cannot be guaranteed. In digitally interconnected force structures, information compromise translates directly into operational degradation (Alberts & Garstka, 1998, p. 34).

Strategically positioned information security assurance therefore fulfills three core functions:

**First**, it sustains decision superiority by protecting the integrity of data flows within compressed operational timelines.

**Second**, it mitigates systemic vulnerability created by network interdependence and multinational interoperability.

**Third**, it reinforces deterrence credibility by reducing adversarial incentives to exploit perceived cyber weaknesses.

In contemporary defence doctrine, information security assurance operates as the protective layer of the military's digital nervous system. Its robustness sustains operational coherence, institutional credibility, and strategic stability. Its failure produces effects comparable to disruption in traditional domains of warfare.

Beyond operational dependency, the strategic positioning of information security assurance must also be understood through the lens of risk calculus at the national defence level. Military decision-makers increasingly evaluate cyber risk not only in technical terms but in relation to mission assurance. Mission assurance refers to the capacity of defence institutions to continue essential functions under adverse conditions (U.S. Department of Defense, 2016). Within this framework, secure networks are treated as critical enablers of national defence objectives. A disruption affecting strategic command networks, intelligence fusion centers, or logistics management systems has implications extending beyond tactical inconvenience; it influences force projection credibility and alliance reliability.

Another dimension concerns interoperability within multinational environments. Contemporary operations rarely occur in isolation. Joint task forces, NATO command structures, and coalition deployments require secure data exchange across heterogeneous systems. This introduces structural tension between operational openness and security control. Excessive compartmentalization undermines collaboration, while excessive connectivity increases exposure. Information security assurance therefore functions as a balancing mechanism between integration and protection. Doctrine

increasingly addresses this challenge through standardized security protocols, federated identity management systems, and layered access controls (NATO, 2023).

Strategic positioning is further reinforced by the role of cyber resilience in deterrence posture. Traditional deterrence relied on visible military capabilities. In the digital era, resilience itself becomes a signaling instrument. An adversary that perceives hardened networks, rapid recovery capacity, and robust incident response mechanisms may reassess the expected gains of cyber intrusion. Conversely, systemic vulnerabilities invite probing and escalation. In this sense, information security assurance contributes to strategic stability by shaping adversarial risk assessments.

The acceleration of digital transformation within armed forces intensifies this positioning. Cloud migration, artificial intelligence integration, and data-centric operational models increase efficiency but also amplify dependency. Defence modernization programs implicitly expand the attack surface. Without doctrinally embedded assurance mechanisms, modernization risks creating fragility. Contemporary defence doctrine therefore increasingly incorporates secure-by-design principles into capability development cycles, ensuring that protection is embedded at the architecture level rather than appended post-deployment (U.S. Department of Defense, 2023).

Taken together, these dimensions demonstrate that information security assurance is structurally interwoven with strategic readiness, alliance cohesion, and deterrence credibility. It is not an adjunct to operational capability; it conditions the reliability of military power in a digitally contested environment.

## Operational Resilience and Multi-Domain Integration of Military Networks

Operational resilience represents the functional expression of information security assurance within the conduct of modern military operations. In contemporary doctrine, operations are increasingly conceived as multi-domain, synchronized across land, air, maritime, space, and cyberspace, requiring continuous data exchange and integrated command structures (U.S. Department of the Army, 2022).

Multi-domain operations (MDO) compress decision cycles and intensify dependency on digital infrastructures (NATO Cooperative Cyber Defence Centre of Excellence, 2020). Command and control (C2), intelligence fusion, targeting coordination, and logistical sustainment rely on uninterrupted data flows between distributed units and higher echelons of command. Field manuals addressing operations in contested environments emphasize the importance of maintaining operational tempo under conditions of disruption and adversarial interference. Under such conditions, resilience becomes the decisive attribute of military networks.

Resilience differs from traditional defensive security. Classical perimeter-based protection assumed identifiable boundaries and episodic threats. Contemporary threat environments are persistent, adaptive, and hybrid. Adversaries integrate cyber intrusion, electronic warfare, and information operations to degrade network reliability and create cognitive friction within command systems. Operational doctrine acknowledges that forces must expect degraded communications and contested information environments as a normal condition of warfare rather than an exception (U.S. Department of Defense, 2018; NATO Standardization Office, 2020).

Within this framework, operational resilience in military networks rests on four structural principles:

**Redundancy** – ensuring alternative communication paths and distributed architectures;

**Segmentation** – limiting lateral movement within compromised systems;

**Continuous monitoring** – detecting anomalies in real time;

**Rapid recovery capability** – restoring mission-critical functions without strategic delay.

These mechanisms support what doctrine identifies as mission continuity in contested domains.

The integration of cyber capabilities into operational planning reinforces this approach. Multi-domain battle concepts explicitly recognize cyberspace operations as shaping and supporting maneuver across other domains. This interdependence implies that network failure in the cyber layer produces ripple effects in kinetic domains. A compromised data link may disrupt targeting cycles; degraded satellite communications may affect navigation and synchronization; manipulated intelligence feeds may distort operational assessment.

The architecture of resilient military networks can be conceptualized as layered defense aligned with operational functions.

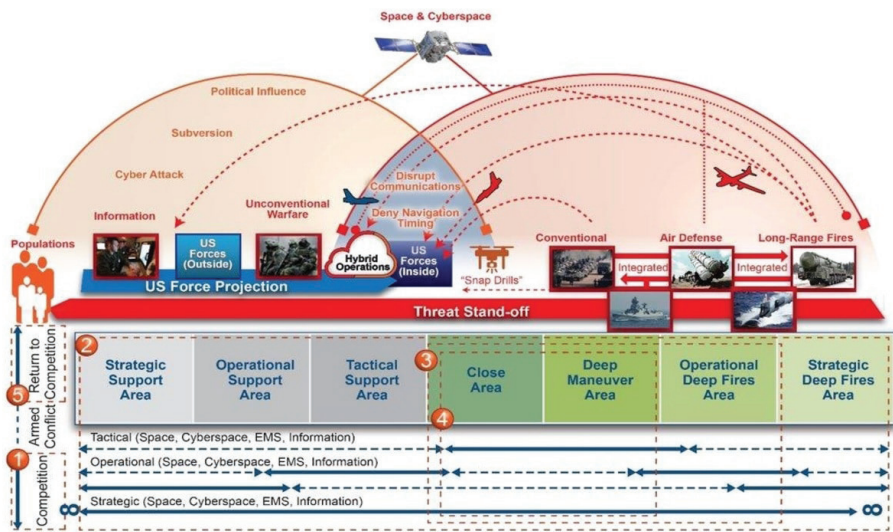


Fig. 2: Layered Operational Resilience Model in Multi-Domain Military Networks. Source: Singh (2025).

This layered model reflects a doctrinal reality: resilience is cumulative. Failure at lower layers propagates upward, affecting operational and strategic outcomes. Conversely, robust protection at foundational layers stabilizes higher-level mission functions.

An additional dimension concerns coalition operations. NATO and partner forces operate within federated network architectures that must balance interoperability and sovereignty (NATO, 2023). Federated mission networking frameworks require shared standards while preserving national control over sensitive data. This structural complexity increases the importance of standardized cyber defense procedures and coordinated incident response mechanisms.

Operational resilience also depends on training and procedural discipline. Field doctrine stresses that units must operate under conditions of degraded communications and partial system failure. Exercises increasingly simulate cyber-electromagnetic interference scenarios to validate recovery procedures and command adaptability. Resilience, therefore, is not only technological but procedural and cognitive (U.S. Department of the Army, 2022).

In contemporary multi-domain operations, secure networks are not passive enablers. They are maneuver space. Protecting them requires synchronization between

cyber defence units, operational commanders, and strategic leadership. The assurance of military networks becomes a precondition for sustaining operational initiative in contested environments.

Beyond structural redundancy and layered protection, operational resilience must be analyzed in relation to the cyber-electromagnetic spectrum. Contemporary doctrine increasingly treats cyberspace and the electromagnetic spectrum as an integrated battlespace. Electronic warfare, spectrum denial, signal interference, and cyber intrusion operate in coordination to disrupt network-dependent forces. In such an environment, military networks must be designed to function under conditions of degraded bandwidth, intermittent connectivity, and spectrum contestation. Resilience therefore implies adaptive communication pathways, spectrum agility, and decentralized command capabilities capable of operating under partial isolation (U.S. Department of Defense, 2018).

Another critical dimension concerns data integrity within AI-enabled operational environments. Multi-domain operations rely on sensor fusion, automated targeting support systems, and predictive analytics. These systems depend on trusted datasets. Manipulation of data inputs, whether through cyber intrusion, spoofing, or algorithmic poisoning, may generate distorted operational outputs without immediately disabling network infrastructure. This represents a higher-order vulnerability. Defence digital modernization strategies increasingly recognize the need to secure data provenance, model validation processes, and software supply chains as integral components of operational assurance (European Commission, 2020).

Operational resilience must also be embedded within planning methodologies. Contemporary operational design incorporates risk assessment matrices that evaluate vulnerabilities across domains (U.S. Department of the Army, 2022). However, cyber risk assessment differs from traditional kinetic threat evaluation. Cyber threats may remain latent until activated, and their operational impact may unfold non-linearly. This requires dynamic risk modeling and continuous vulnerability assessment embedded within operational planning cycles.

## Governance, Deterrence and Technological Sovereignty in Military Information Assurance

Strategic information security assurance extends beyond operational resilience and technical architecture. At the highest level, it is shaped by governance structures, deterrence posture, and the degree of technological sovereignty retained by the state. Military networks operate within national legal frameworks, alliance obligations, industrial dependencies, and political oversight mechanisms. Their protection therefore becomes a matter of strategic governance rather than solely operational management.

Effective governance begins with clarity of authority. Cyber defence responsibilities must be delineated across strategic command levels, operational headquarters, and specialized cyber units. Joint doctrine emphasizes unity of command and synchronized effects across domains (NATO Standardization Office, 2022). In the cyber domain, fragmentation of responsibility produces exploitable seams. Consequently, defence institutions increasingly centralize cyber oversight while preserving decentralized operational execution.

Policy coherence is equally critical. Information security standards, procurement regulations, classification protocols, and incident reporting mechanisms must operate under unified doctrinal guidance. NATO frameworks stress the importance of harmonized security standards across allied networks to preserve interoperability without compromising national control. Governance therefore functions as the connective tissue linking alliance integration and sovereign authority (NATO, 2023).

Deterrence in the digital domain introduces additional complexity. Classical deterrence relied on visible capabilities and clearly attributable consequences. Cyberspace complicates attribution and proportional response. Nevertheless, strategic documents increasingly recognize resilience and response capability as components of deterrence posture. An adversary calculating the value of cyber intrusion must consider not only potential gains but also the defender's recovery speed, retaliatory capacity, and alliance support mechanisms (NATO, 2020).

Information security assurance thus contributes to deterrence in two complementary ways. First, by reducing vulnerability, it lowers the expected effectiveness of adversarial operations. Second, by demonstrating coordinated governance and readiness, it signals preparedness. Strategic communication surrounding cyber capabilities increasingly forms part of national defence narratives. This signaling dimension influences adversarial risk assessments even in the absence of kinetic escalation.

Technological sovereignty represents another decisive factor. Military networks depend on hardware components, software platforms, cloud infrastructures, and supply chains that may extend beyond national jurisdiction. Excessive reliance on external vendors introduces strategic risk. Supply chain vulnerabilities, embedded backdoors, and software lifecycle opacity can undermine long-term assurance. Defence modernization agendas therefore emphasize secure supply chains, trusted vendors, and domestic capability development (U.S. Department of Defense, 2023).

Sovereignty does not imply isolation. Multinational operations require interoperable systems. The strategic challenge lies in balancing interdependence with autonomy. Federated network models and zero trust architectures offer partial solutions, enabling collaboration without unconditional trust. However, governance mechanisms must ensure that national critical information remains protected within alliance frameworks.

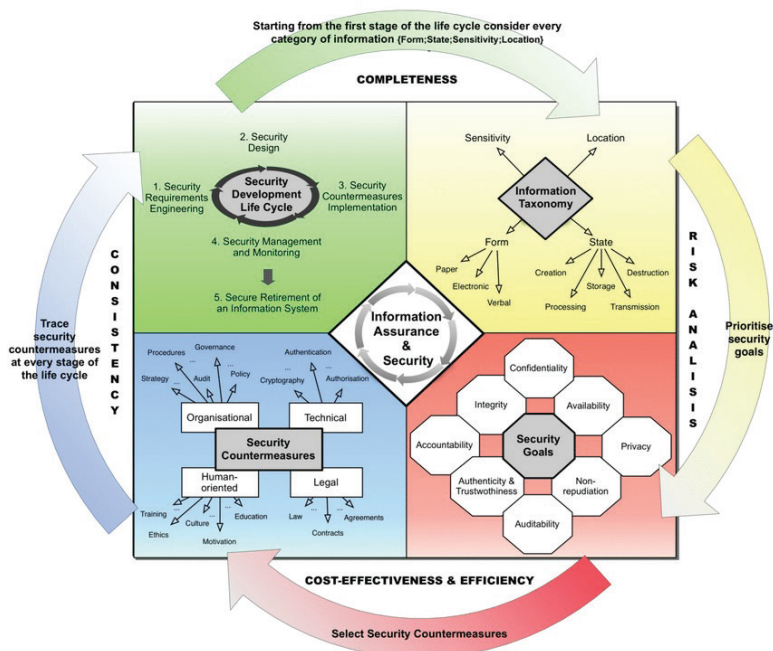


Fig. 3: Strategic Framework of Information Security Assurance.  
Source: Sellitto et al. (2020)

Strategic dimension concerns legal and normative structures. Cyber operations intersect with international law, rules of engagement, and alliance commitments. Governance mechanisms must define thresholds for response, attribution procedures, and coordination protocols with civilian authorities. The blurring of civilian and military infrastructure in cyberspace requires integrated civil-military coordination mechanisms. National cyber security strategies increasingly reflect this integrated approach. Taken together, governance, deterrence, and technological sovereignty define the strategic environment within which operational resilience functions. Without coherent governance, resilience becomes fragmented. Without credible deterrence, resilience remains reactive. Without technological sovereignty, resilience becomes externally dependent (Schmitt, 2017).

In the contemporary security environment, military information assurance is therefore not merely a technical discipline but a strategic instrument. It supports operational

continuity, reinforces alliance cohesion, and shapes adversarial calculations. Its strategic value lies not only in preventing disruption but in preserving freedom of action within a contested digital battlespace.

## *Conclusion*

The contemporary defence environment confirms that military power is inseparable from the resilience of its digital architecture. Information security assurance has moved beyond technical safeguarding and now functions as a structural condition for operational coherence and strategic credibility. Modern armed forces do not merely use networks; they operate through them. Command authority, intelligence fusion, logistical sustainment, and joint fires synchronization depend on the integrity of data flows across contested domains (NATO, 2020; U.S. Department of Defense, 2023).

The analysis demonstrates that information security assurance occupies three interdependent dimensions. First, it is doctrinally embedded within the recognition of cyberspace as an operational domain and within the evolution of multi-domain operations. Second, it manifests operationally through resilience mechanisms designed to sustain mission continuity under cyber-electromagnetic contestation. Third, it is strategically governed through institutional authority, deterrence posture, and technological sovereignty.

Operational resilience emerges as the decisive characteristic of contemporary military networks. Absolute protection is neither feasible nor doctrinally realistic. The objective is continuity under pressure, maintaining command functionality despite disruption attempts. Redundancy, segmentation, decentralized execution, and rapid recovery mechanisms are not technical luxuries but operational necessities in environments where degradation is expected rather than exceptional.

At the strategic level, governance coherence determines whether resilience translates into credible defence posture. Clear command responsibility, harmonized standards, secure procurement practices, and alliance coordination ensure that network assurance does not fragment across institutional boundaries. In parallel, visible resilience contributes to deterrence by shaping adversarial risk assessments. A force capable of absorbing and recovering from cyber aggression reduces the perceived utility of such aggression.

Technological sovereignty further conditions long-term assurance. Dependence on vulnerable supply chains or opaque digital ecosystems introduces structural risk. Strategic autonomy in critical digital capabilities strengthens national resilience while preserving alliance interoperability. The balance between integration and sovereignty defines a central tension of contemporary defence policy.

In a security environment characterized by persistent competition and rapid technological change, information security assurance must be treated as an enduring strategic function. It sustains operational effectiveness, reinforces alliance cohesion, and preserves freedom of action within contested digital battlespaces. The protection of military networks is no longer an auxiliary task; it is a foundational requirement of credible defence in the twenty-first century. The strategic dimensions outlined in this study confirm a broader doctrinal transformation: digital resilience is now integral to combat power. Where information flows are secure and resilient, operational initiative can be maintained. Where they are fragile, strategic posture erodes. In modern warfare, the defence of networks is inseparable from the defence of the state.

## References

- [1] Alberts, D. S., & Garstka, J. J. (1998). Network centric warfare: Developing and leveraging information superiority. CCRP Publication Series. [https://www.dodccrp.org/files/Alberts\\_NCW.pdf](https://www.dodccrp.org/files/Alberts_NCW.pdf)
- [2] European Commission. (2020). EU cybersecurity strategy for the digital decade. <https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-strategy-digital-decade>
- [3] NATO. (2020). NATO 2030: United for a new era. <https://www.nato.int/nato2030/>
- [4] NATO. (2023). Comprehensive cyber defence policy. [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm)
- [5] NATO Cooperative Cyber Defence Centre of Excellence. (2020). Cyber threats and NATO 2030: Horizon scanning and analysis. <https://ccdcoe.org/library/publications/cyber-threats-and-nato-2030/>
- [6] NATO Standardization Office. (2022). Allied Joint Doctrine (AJP-01), Edition F, Version 1. North Atlantic Treaty Organization. [https://assets.publishing.service.gov.uk/media/659ea238e96df5000df843f3/AJP\\_01\\_EdF\\_with\\_UK\\_elements.pdf](https://assets.publishing.service.gov.uk/media/659ea238e96df5000df843f3/AJP_01_EdF_with_UK_elements.pdf)
- [7] NATO Standardization Office. (2025). Allied Joint Doctrine for the Conduct of Operations (AJP-3), Edition D, Version 1. North Atlantic Treaty Organization. [https://assets.publishing.service.gov.uk/media/6964e72799fbdc498faecce2/AJP\\_3\\_Ed\\_D\\_V1-O.pdf](https://assets.publishing.service.gov.uk/media/6964e72799fbdc498faecce2/AJP_3_Ed_D_V1-O.pdf)
- [8] NATO Standardization Office. (2020). Allied joint doctrine for cyberspace operations (AJP-3.20). [https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine\\_nato\\_cyberspace\\_operations\\_ajp\\_3\\_20\\_1\\_.pdf](https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf)
- [9] NATO Standardization Office. (2024). Allied Joint Doctrine for Communication and Information Systems (AJP-6), Edition B, Version 1. North Atlantic Treaty Organization. [https://www.coemed.org/files/stanags/01\\_AJP/AJP-6\\_EDB\\_V1\\_E\\_2525.pdf](https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDB_V1_E_2525.pdf)
- [10] National Institute of Standards and Technology. (2007). Global Information Grid (GIG). Computer Security Resource Center Glossary [https://csrc.nist.gov/glossary/term/global\\_information\\_grid](https://csrc.nist.gov/glossary/term/global_information_grid)

- [11] Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press. <https://doi.org/10.1017/9781316822524>
- [12] Sellitto, G. P., Aranha, H., Masi, M., & Pavleska, T. (2020). Security and safety by design in the Internet of Actors: An architectural approach. In M. Freitag, A. Kinra, H. Kotzab, H.-J. Kreowski, & K.-D. Thoben (Eds.), Subject-Oriented Business Process Management. The Digital Workplace – Nucleus of Transformation (Communications in Computer and Information Science, Vol. 1278, pp. 133–142). Springer, Cham. [https://doi.org/10.1007/978-3-030-64351-5\\_9](https://doi.org/10.1007/978-3-030-64351-5_9)
- [13] Singh, K. (2025). America's multi-domain operations at 250: A strategy, concept or mirage? Centre for Aerospace Power and Strategic Studies (CAPSS). <https://capssindia.org/americas-multi-domain-operations-at-250-a-strategy-concept-or-mirage/>
- [14] U.S. Department of Defense. (2018). Joint publication (JP) 3-12: Cyberspace operations. Joint Chiefs of Staff. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf)
- [15] U.S. Department of Defense. (2023). 2023 Department of Defense cyber strategy. <https://media.defense.gov/2023/Aug/25/2003288669/-1/-1/1/2023-DOD-CYBER-STRATEGY.PDF>
- [16] U.S. Department of Defense. (2016). DoD directive 3020.40: Mission assurance. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf>
- [17] U.S. Department of the Army. (2022). Field manual (FM) 3-0: Operations. [https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB\\_ID=1024908](https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1024908)

## Summary

Information security assurance has become a critical component of contemporary military capability, given the increasing reliance on networked systems for command, control, communication, and decision-making. Modern defence doctrines increasingly recognize that military networks are not only technical infrastructures, but also strategic assets whose integrity, availability, and confidentiality directly influence operational effectiveness and strategic resilience. This paper examines the strategic dimensions of information security assurance in military networks within the context of contemporary defence doctrine.

The study explores how information security considerations are integrated into doctrinal frameworks and strategic planning processes, emphasizing their role in supporting command and control, safeguarding decision superiority, and enhancing resilience against cyber and hybrid threats. By adopting a conceptual and analytical approach, the paper highlights the relationship between information security assurance, military strategy, and defence policy, rather than focusing solely on technical protection mechanisms. Particular attention is given to the implications of information

security failures for operational continuity and strategic stability in modern conflict environments.

The analysis demonstrates that effective information security assurance requires a comprehensive approach that combines technical measures with organizational, doctrinal, and strategic elements. The paper argues that integrating information security assurance into defence doctrine is essential for maintaining operational credibility and ensuring the effective employment of military networks in contemporary and future security environments.

*Keywords: information security assurance; military networks; defence doctrine; military strategy; cyber and hybrid threats*

© 2026 The Author. Published by Vojno delo (<http://www.vojnodelo.mod.gov.rs>). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).



