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

Fiodor Timercan[1]

Delivered: 19.6.2026. *Language*: English
Corrected: 13.8.2026. *Type of paper*: Review paper
Accepted: 9.9.2026. *DOI number*: 10.5937/vojdelo2603167T

Abstract: 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*

1 “Alexandru cel Bun” Armed Forces Military Academy, Republic of Moldova, e-mail: 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.

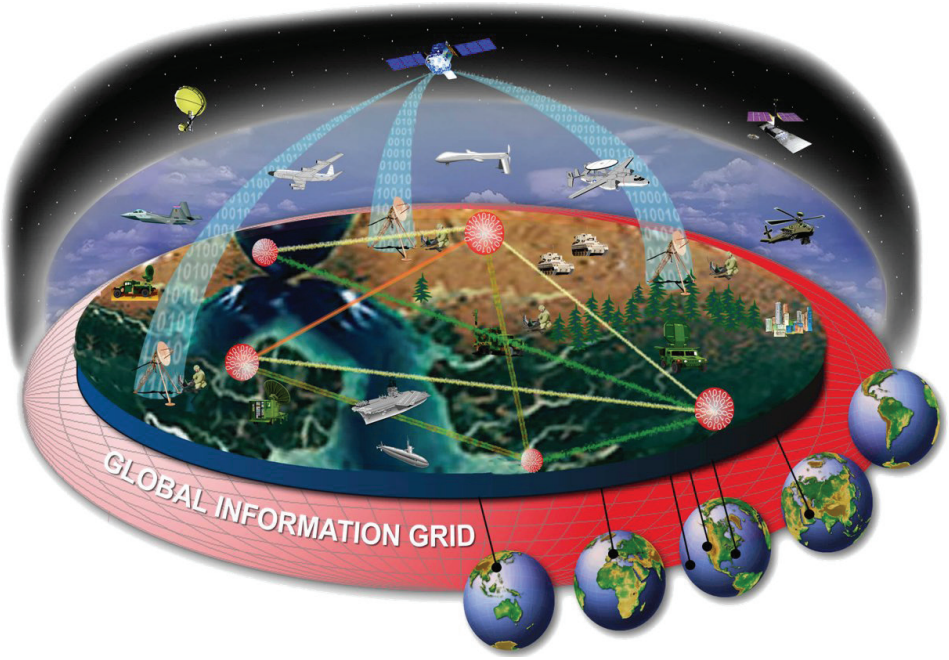


Fig. 1: Schematic view of the Global Information Grid (GIG), representing the interconnected information capabilities supporting the collection, processing, storage, dissemination, and management of information across the defence environment.

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.

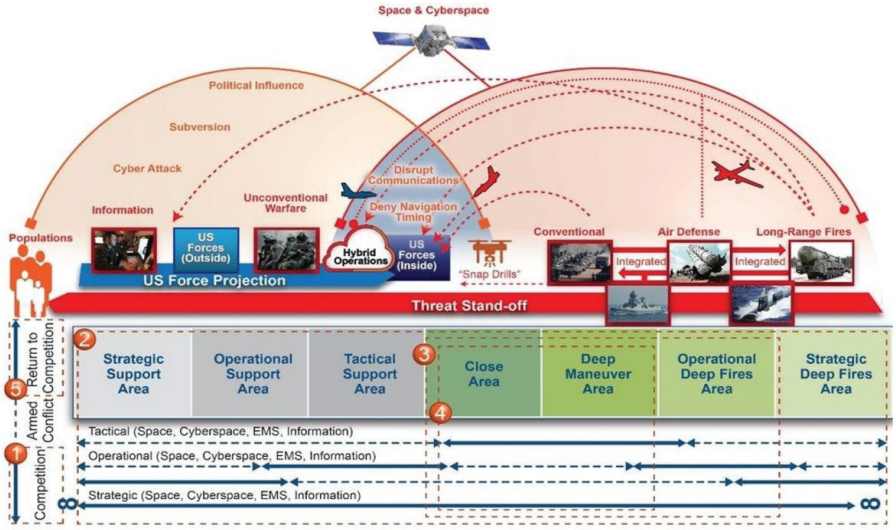


Fig. 2: Layered Operational Resilience Model in Multi-Domain Military Networks. Source: Singh (2025).

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.

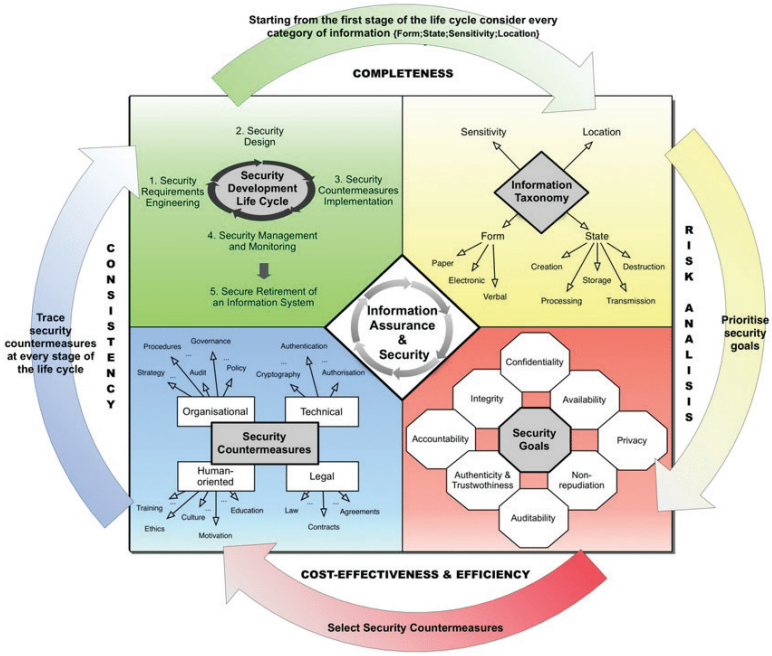


Fig. 3: Strategic Framework of Information Security Assurance.
Source: Sellitto et al. (2020)

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

[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

[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

[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

[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

[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

[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

[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

[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

[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

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/).



СТРАТЕШКЕ ДИМЕНЗИЈЕ ОБЕЗБЕЂЕЊА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ У ВОЈНИМ МРЕЖАМА У КОНТЕКСТУ САВРЕМЕНЕ ДОКТРИНЕ ОДБРАНЕ

Фјодор Тимеркан[1]

Достављен:	19.6.2026.	*Језик рада*:	Српски
Кориговано:	13.8.2026.	*Тип рада*:	Прегледни рад
Прихваћен:	9.9.2026.	*DOI број*:	10.5937/vojdelo2603167T

Апстракт: Обезбеђивање информационе безбедности постало је критична компонента савремених војних способности имајући у виду све већу зависност од умрежених система у области командовања, контроле, комуникације и доношења одлука. Савремене доктрине одбране све више препознају да војне мреже нису само техничка инфраструктура већ и стратешка средства чији интегритет, расположивост и поверљивост непосредно утичу на оперативну ефикасност и стратешку отпорност. У раду се разматрају стратешке димензије обезбеђења информационе безбедности у војним мрежама у контексту савремене доктрине одбране.

Истраживање анализира начин на који се питања информационе безбедности интегришу у доктринарне оквире и процесе стратешког планирања, са посебним нагласком на њихову улогу у подршци командовању и контроли, очувању надмоћи у одлучивању и јачању отпорности на сајбер и хибридне претње. Применом концептуалног и аналитичког приступа, у раду се указује на однос између обезбеђења информационе безбедности, војне стратегије и политике одбране, а не искључиво на техничке механизме заштите. Посебна пажња посвећена је импликацијама пропуста у области информационе безбедности по оперативни континуитет и стратешку стабилност у савременим конфликтним окружењима.

Анализа показује да делотворно осигурање информационе безбедности захтева свеобухватан приступ који обједињује техничке мере са организационим, доктринарним и стратешким елементима. У раду се заступа становиште да је интеграција обезбеђења информационе безбедности у доктрину одбране од суштинског значаја за

1 Војна академија Оружаних снага „Александру чел Бун”, Кишињев, Република Молдавија, e-mail: timercantudor@yahoo.com, https://orcid.org/0009-0001-6769-3556

очување оперативног кредибилитета и обезбеђивање ефикасне употребе војних мрежа у савременом и будућем безбедносном окружењу.

Кључне речи*: обезбеђивање информационе безбедности, војне мреже, доктрина одбране, војна стратегија, сајбер и хибридне претње*

Увод

Савремено безбедносно окружење карактеришу трајно надметање, убрзана технолошка трансформација и постепено нестајање традиционалне разлике између рата и мира. Војне организације делују у оквиру континуума стратешког супарништва, у којем кинетичко ангажовање представља само једну од манифестација конфронтације. У таквом развојном окружењу информација је постала одлучујући елемент пројекције моћи и оперативне ефикасности.

Сајбер простор је данас формално признат као оперативни домен, заједно са копном, ваздушним простором, поморским простором и свемиром (NATO, 2020). Ово признање одражава више од концептуалне модернизације; оно потврђује структурну зависност савремених оружаних снага од дигиталне инфраструктуре. Војне мреже подржавају функције командовања и контроле, обједињавање обавештајних података, процесе циљања, координацију логистике и мултинационалну интероперабилност. Њихов интегритет непосредно утиче на оперативни темпо, тачност доношења одлука и преживљавање снага.

Савремена доктрина одбране све више наглашава мултидоменске операције, интеграцију здружених способности и убрзане циклусе одлучивања (U.S. Department of the Army, 2022). Ови развојни процеси додатно повећавају ослањање на безбедне и отпорне информационе системе. Мрежноцентрични приступи, иако унапређују ситуациону свест и координацију, истовремено проширују површину напада доступну противницима (Alberts & Garstka, 1998). Државни и недржавни актери искоришћавају рањивости путем напредних упорних претњи, манипулације ланцима снабдевања, сајбер шпијунаже, интеграције електронског ратовања и хибридних операција утицаја. У таквим условима обезбеђивање информационе безбедности превазилази оквире техничке администрације и постаје питање стратешке отпорности.

Војне мреже више нису изолована инфраструктура заштићена статичним периметарским одбранама. Оне представљају динамичне, дистрибуиране и међусобно повезане екосистеме. Коалиционе операције, мултинационалне команде и оквири интероперабилности захтевају размену података између различитих безбедносних архитектура и регулаторних окружења. Ова међусобна повезаност унапређује оперативне способности, али истовремено уводи системске рањивости. Стратешко обезбеђење зато мора да успостави равнотежу између отворености неопходне за сарадњу и контролисаног приступа неопходног за заштиту.

Прелазак са реактивне сајбер безбедности на безбедносну архитектуру засновану на отпорности одражава доктринарно прилагођавање адаптивним противницима. Апсолутна заштита је недостижна у оспораваном сајбер простору. Стратешка предност лежи у способности откривања, ограничавања, опоравка и прилагођавања, уз истовремено очување оперативног континуитета. Концепти као што су слојевита одбрана, архитектура нултог поверења, инжењеринг заснован на принципу безбедности од самог пројектовања и континуирано праћење све више се уграђују у војно планирање. Они не представљају техничке преференције, већ стратешке нужности (U.S. Department of Defense, 2023).

Интеграција вештачке интелигенције, аутономних система и инфраструктуре засноване на облаку додатно усложњава безбедносно окружење. Алгоритми за подршку одлучивању, платформе за фузију сензорских података и предиктивна аналитика зависе од интегритета података и поузданости софтвера. Компромитовање на нивоу података или алгоритама може искривити оперативну свест и стратешко расуђивање. Зато обезбеђење информационе безбедности мора да обухвати заштиту порекла података, валидацију алгоритама и безбедно управљање животним циклусом дигиталних способности (European Commission, 2020).

Компромитовање мреже носи стратешке последице које превазилазе непосредни оперативни поремећај. Безбедносни пробоји подривају кредибилитет одвраћања, излажу рањивости структуре снага и могу изменити противничке процене. У савременом окружењу перцепција сајбер слабости може бити стратешки штетна у истој мери као и деградација физичке силе. Обезбеђење информационе безбедности, сходно томе, непосредно доприноси националној отпорности и стратешком сигнализирању.

Ефикасна примена захтева усклађеност доктрине, политике, организационе структуре и оперативне културе. Сајбер безбедност не може остати ограничена на специјализоване техничке јединице. Она мора бити интегрисана у командну одговорност, процесе планирања и режиме обуке. Дисциплина у дигиталним праксама, свест на нивоу руководства и институционализована безбедносна култура представљају суштинске компоненте стратешког обезбеђења.

У ери обележеној убрзаним протоком информација и сажетим циклусима одлучивања, заштита војних мрежа неодвојива је од очувања борбене моћи. Дигитална инфраструктура представља и рањивост и стратешко средство. Обезбеђивање њене отпорности више није помоћна функција; оно је темељни захтев савремене доктрине одбране.

Стратешко позиционирање информационе безбедности у оквиру савремене доктрине одбране

Савремено безбедносно окружење одређено је трајним стратешким надметањем, убрзаном технолошком трансформацијом и нарушавањем јасних граница између мира и сукоба. У таквом оквиру војна ефикасност не зависи само од кинетичких способности већ и од интегритета дигиталне инфраструктуре која подржава командни ауторитет и оперативну координацију. Обезбеђење информационе безбедности стога се позиционира као саставни део доктрине одбране, а не као споредна техничка функција.

Формално признавање сајбер простора као оперативног домена мења начин на који се рањивост и заштита концептуализују у војном планирању. Савезничка доктрина утврђује да су комуникационо-информациони системи (*Communication and Information Systems* – CIS) средства од критичног значаја за извршење мисије, чија је заштита неопходна за очување оперативног континуитета на стратешком, оперативном и тактичком нивоу. Информационо обезбеђење, дефинисано кроз заштиту расположивости, интегритета и поверљивости информација и информационих система, непосредно условљава ефикасност процеса командовања и контроле.

Оперативна доктрина додатно наглашава да савремене здружене операције зависе од синхронизованих ефеката у копненом, поморском, ваздушном, свемирском и сајбер домену. Ова интеграција омогућава се посредством међусобно повезаних дигиталних мрежа које обједињују улазне податке са сензора, обавештајне производе, податке о циљевима и логистичке информације у јединствена окружења за доношење одлука. Свако нарушавање ових система производи каскадне оперативне последице: успоравање циклуса одлучивања, искривљену ситуациону свест и смањену синхронизацију снага (NATO Standardization Office, 2025).

Структурна централност војних мрежа концептуално је приказана архитектуром Информационе мреже Министарства одбране Сједињених Америчких Држава (*Department of Defense Information Network* – DoDIN), раније познате као Глобална информациона мрежа (*Global Information Grid*). Овај модел одражава међусобно повезану дигиталну окосницу која подржава здружене и комбиноване операције.

На Слици 1 приказана је интеграција оперативних домена посредством заједничке дигиталне инфраструктуре. Она истиче критичну доктринарну реалност – оперативна ефикасност неодвојива је од поузданости мреже. Иста повезаност која омогућава брзу координацију истовремено проширује површину напада доступну противницима. У таквим условима механизми обезбеђења постају стратешки омогућавајући фактори континуитета мисије.



Слика 1: Шематски приказ Глобалне информационе мреже. Глобална информациона мрежа (GIG) обухвата сваки систем, опрему, софтвер или услугу Министарства одбране САД који преносе, чувају или обрађују информације Министарства одбране САД, као и све друге повезане услуге неопходне за постизање информационе надмоћи

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

Концептуални темељи мрежноцентричног ратовања додатно потврђују ову зависност. Заједничка ситуациона свест и дистрибуиране архитектуре одлучивања повећавају оперативну агилност, али истовремено појачавају системску рањивост уколико се не може гарантовати интегритет података. У дигитално међусобно повезаним структурама снага, компромитовање информација непосредно се претвара у оперативну деградацију (Alberts & Garstka, 1998).

Стратешки позиционирано обезбеђење информационе безбедности због тога испуњава три основне функције:

- Ø прво, одржава надмоћ у одлучивању заштитом интегритета токова података у оквиру сажетих оперативних временских рокова;
- Ø друго, ублажава системску рањивост насталу услед мрежне међузависности и мултинационалне интероперабилности;

- Ø треће, јача кредибилитет одвраћања смањивањем подстицаја противника да искористе уочене сајбер слабости.

У савременој доктрини одбране обезбеђење информационе безбедности представља заштитни слој дигиталног нервног система војске. Његова робусност одржава оперативну кохерентност, институционални кредибилитет и стратешку стабилност. Његов неуспех производи ефекте упоредиве са поремећајима у традиционалним доменима ратовања.

Поред оперативне зависности, стратешко позиционирање обезбеђења информационе безбедности мора се разумети и кроз призму процене ризика на нивоу националне одбране. Војни доносиоци одлука све више процењују сајбер ризик не само у техничком смислу већ и у односу на обезбеђење мисије. Обезбеђење мисије односи се на способност одбрамбених институција да наставе са извршавањем суштинских функција у неповољним условима (U.S. Department of Defense, 2016). У овом оквиру безбедне мреже третирају се као критични омогућавајући фактори остваривања циљева националне одбране. Поремећај који погађа стратешке командне мреже, центре за обједињавање обавештајних података или системе за управљање логистиком има импликације које превазилазе тактичку непријатност; он утиче на кредибилитет пројекције снага и поузданост савезништва.

Друга димензија односи се на интероперабилност у мултинационалним окружењима. Савремене операције ретко се одвијају изоловано. Здружене наменске снаге, командне структуре НАТО-а и коалиционо распоређивање захтевају безбедну размену података између хетерогених система. То уводи структурну напетост између оперативне отворености и безбедносне контроле. Прекомерна подела информација на затворене целине подрива сарадњу, док прекомерна повезаност повећава изложеност. Обезбеђење информационе безбедности услед тога има улогу као механизам уравнотежавања између интеграције и заштите. Доктрина све више разматра овај изазов кроз стандардизоване безбедносне протоколе, федеративне системе управљања идентитетом и слојевите контроле приступа (NATO, 2023).

Стратешко позиционирање додатно је ојачано улогом сајбер отпорности у положају одвраћања. Традиционално одвраћање ослањало се на видљиве војне способности. У дигиталној ери сама отпорност постаје инструмент сигнализирања. Противник који уочава ојачане мреже, способност брзог опоравка и робусне механизме реаговања на инциденте може преиспитати очекиване добити од сајбер упада. Насупрот томе, системске рањивости подстичу испитивање слабости и ескалацију. У том смислу обезбеђење информационе безбедности доприноси стратешкој стабилности обликујући противничке процене ризика.

Убрзање дигиталне трансформације у оквиру оружаних снага додатно појачава ово позиционирање. Миграција ка облаку, интеграција вештачке интелигенције и оперативни модели засновани на подацима повећавају ефикасност, али истовремено појачавају зависност. Програми модернизације одбране им-

плицитно проширују површину напада. Без доктринарно уграђених механизама обезбеђења, модернизација носи ризик стварања крхкости. Савремена доктрина одбране отуда све више у циклусе развоја способности уграђује принципе безбедности од самог пројектовања, обезбеђујући да заштита буде уграђена на нивоу архитектуре, а не додата тек након распоређивања (U.S. Department of Defense, 2023).

Узете заједно, ове димензије показују да је обезбеђење информационе безбедности тесно повезано са стратешком спремношћу, кохезијом савезништва и кредибилитетом одвраћања. Оно није додатак оперативној способности; оно условљава поузданост војне моћи у дигитално оспораваном окружењу.

Оперативна отпорност и мултидоменска интеграција војних мрежа

Оперативна отпорност представља функционални израз обезбеђења информационе безбедности у извођењу савремених војних операција. У савременој доктрини операције се све више схватају као мултидоменске, синхронизоване у копненом, ваздушном, поморском, свемирском и сајбер домену, што захтева континуирану размену података и интегрисане командне структуре (U.S. Department of the Army, 2022).

Мултидоменске операције (*multi-domain operations* – MDO) сажимају циклусе одлучивања и појачавају зависност од дигиталне инфраструктуре (NATO Cooperative Cyber Defence Centre of Excellence, 2020). Командовање и контрола (*command and control* – C2), обједињавање обавештајних података, координација циљања и логистичка подршка ослањају се на непрекинуте токове података између дистрибуираних јединица и виших ешалона командовања. Приручници који се баве операцијама у оспораваним окружењима наглашавају значај одржавања оперативног темпа у условима поремећаја и противничког ометања. У таквим условима отпорност постаје одлучујуће својство војних мрежа.

Отпорност се разликује од традиционалне одбрамбене безбедности. Класична заштита заснована на периметру полазила је од претпоставке о препознатљивим границама и епизодичним претњама. Савремена окружења претњи су трајна, адаптивна и хибридна. Противници интегришу сајбер упаде, електронско ратовање и информационе операције како би деградирали поузданост мреже и створили когнитивно трење унутар командних система. Оперативна доктрина признаје да снаге морају очекивати деградиране комуникације и оспоравана информациона окружења као уобичајено стање ратовања, а не као изузетак (U.S. Department of Defense, 2018).

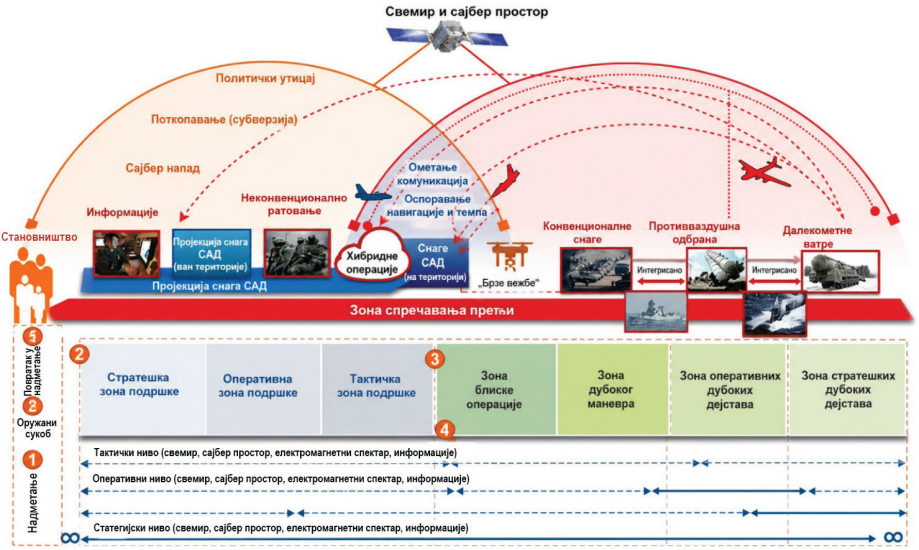
У овом оквиру, оперативна отпорност војних мрежа почива на четири структурна принципа:

Ø редундантност – обезбеђивање алтернативних комуникационих путева и дистрибуираних архитектура;
Ø сегментација – ограничавање латералног кретања унутар компромитованих система;
Ø континуирано праћење – откривање аномалија у реалном времену;
Ø способност брзог опоравка – обнављање функција од критичног значаја за мисију без стратешког одлагања.

Ови механизми подржавају оно што доктрина означава као континуитет мисије у оспораваним доменима.

Интеграција сајбер способности у оперативно планирање додатно учвршћује овај приступ. Концепти мултидоменске битке изричито препознају операције у сајбер простору као средство обликовања и подршке маневру у другим доменима. Ова међузависност подразумева да отказ мреже у сајбер слоју производи таласне ефекте у кинетичким доменима. Компромитована веза за пренос података може пореметити циклусе циљања; деградиране сателитске комуникације могу утицати на навигацију и синхронизацију; манипулисани обавештајни токови могу искривити оперативну процену.

Архитектура отпорних војних мрежа може се концептуализовати као слојевита одбрана усклађена са оперативним функцијама.



Слика 2: Слојевити модел оперативне отпорности у мултидоменским војним мрежама (https://capssindia.org/americas-multi-domain-operations-at-250-a-strategy-concept-or-mirage/).

Овај слојевити модел одражава доктринарну реалност: отпорност је кумулативна. Отказ на нижим слојевима преноси се навише, утичући на оперативне и стратешке исходе. Насупрот томе, робусна заштита на темељним слојевима стабилизује функције мисије на вишим нивоима.

Додатна димензија односи се на коалиционе операције. НАТО и партнерске снаге делују у оквиру федеративних мрежних архитектура које морају да успоставе равнотежу између интероперабилности и суверенитета (NATO, 2023). Оквири федеративног умрежавања мисија захтевају заједничке стандарде, уз истовремено очување националне контроле над осетљивим подацима. Ова структурна сложеност повећава значај стандардизованих процедура сајбер одбране и координисаних механизама реаговања на инциденте.

Оперативна отпорност зависи и од обуке и процедуралне дисциплине. Доктрина на терену наглашава да јединице морају бити способне да делују у условима деградираних комуникација и делимичног отказа система. Вежбе све чешће симулирају сценарије сајбер-електромагнетног ометања ради провере процедура опоравка и командне прилагодљивости. Отпорност, због тога, није само технолошка већ и процедурална и когнитивна (U.S. Department of the Army, 2022).

У савременим мултидоменским операцијама безбедне мреже нису пасивни омогућавајући фактори. Оне представљају простор маневра. Њихова заштита захтева синхронизацију између јединица за сајбер одбрану, оперативних команданата и стратешког руководства. Обезбеђење војних мрежа постаје предуслов за одржавање оперативне иницијативе у оспораваним окружењима.

Поред структурне редундантности и слојевите заштите, оперативна отпорност мора се анализирати и у односу на сајбер-електромагнетни спектар. Савремена доктрина све више третира сајбер простор и електромагнетни спектар као интегрисано бојиште. Електронско ратовање, ускраћивање приступа спектру, ометање сигнала и сајбер упади делују координисано ради нарушавања снага зависних од мрежа. У таквом окружењу војне мреже морају бити пројектоване тако да функционишу у условима смањеног пропусног опсега, повремене повезаности и оспоравања спектра. Отпорност стога подразумева адаптивне комуникационе путеве, агилност у коришћењу спектра и децентрализоване командне способности које могу функционисати у условима делимичне изолације (U.S. Department of Defense, 2018).

Још једна критична димензија односи се на интегритет података у оперативним окружењима подржаним вештачком интелигенцијом. Мултидоменске операције ослањају се на фузију сензорских података, аутоматизоване системе подршке циљању и предиктивну аналитику. Ови системи зависе од поузданих скупова података. Манипулација улазним подацима, било путем сајбер упада, лажирања сигнала или алгоритамског тровања, може произвести искривљене оперативне излазе без непосредног онеспособљавања мрежне инфраструктуре. То представља рањивост вишег реда. Стратегије дигиталне модернизације

одбране све више препознају потребу за обезбеђивањем порекла података, процеса валидације модела и софтверских ланаца снабдевања као интегралних компоненти оперативног обезбеђења (European Commission, 2020).

Оперативна отпорност мора бити уграђена и у методологије планирања. Савремено оперативно пројектовање укључује матрице процене ризика којима се вреднују рањивости у различитим доменима (U.S. Department of the Army, 2022). Међутим, процена сајбер ризика разликује се од традиционалне процене кинетичких претњи. Сајбер претње могу остати латентне све до активирања, а њихов оперативни утицај може се развијати нелинеарно. То захтева динамичко моделирање ризика и континуирану процену рањивости уграђену у циклусе оперативног планирања.

Управљање, одвраћање и технолошки суверенитет у војном информационом обезбеђењу

Стратешко обезбеђење информационе безбедности превазилази оперативну отпорност и техничку архитектуру. На највишем нивоу оно је обликовано структурама управљања, положајем одвраћања и степеном технолошког суверенитета који држава задржава. Војне мреже функционишу у оквиру националних правних оквира, савезничких обавеза, индустријских зависности и механизама политичког надзора. Њихова заштита отуда постаје питање стратешког управљања, а не искључиво оперативног руковођења.

Ефикасно управљање почиње јасноћом надлежности. Одговорности у области сајбер одбране морају бити разграничене између стратешких командних нивоа, оперативних штабова и специјализованих сајбер јединица. Здружена доктрина наглашава јединство командовања и синхронизоване ефекте у различитим доменима (NATO Standardization Office, n.d.). У сајбер домену фрагментација одговорности ствара пукотине које противник може искористити. Сходно томе, одбрамбене институције све више централизују сајбер надзор, уз очување децентрализованог оперативног извршења.

Кохерентност политике подједнако је критична. Стандарди информационе безбедности, прописи о набавкама, протоколи класификације и механизми пријављивања инцидената морају функционисати у оквиру јединственог доктринарног усмерења. НАТО оквири наглашавају значај усклађених безбедносних стандарда у савезничким мрежама ради очувања интероперабилности без угрожавања националне контроле. Управљање због тога представља везивно ткиво које повезује савезничку интеграцију и суверену власт (NATO, 2023).

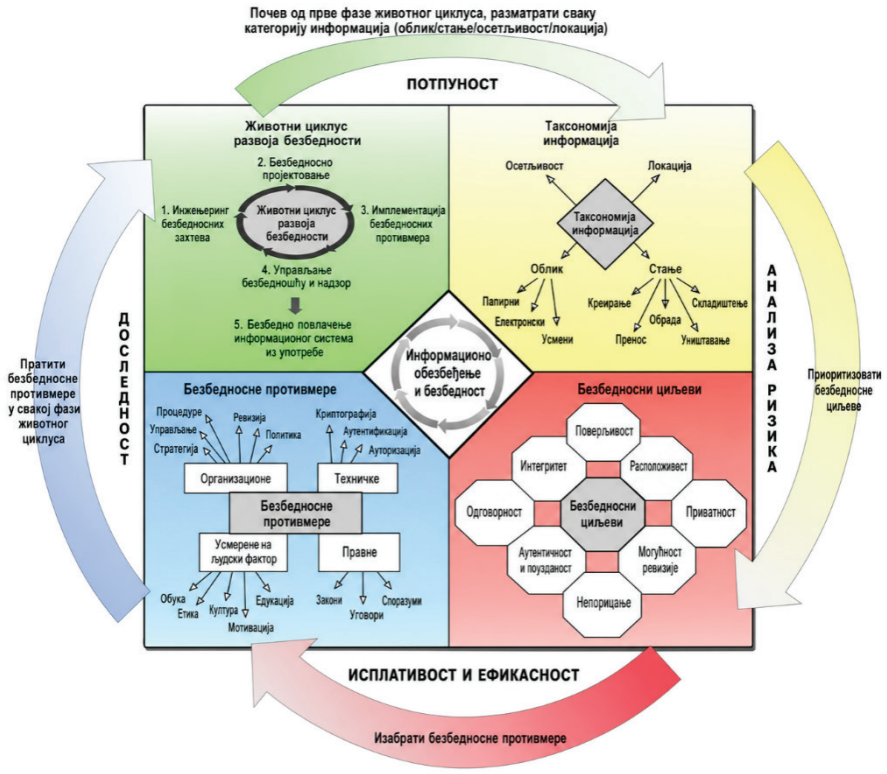
Одвраћање у дигиталном домену уводи додатну сложеност. Класично одвраћање ослањало се на видљиве способности и јасно приписиве последице.

Сајбер простор усложњава атрибуцију и пропорционалан одговор. Ипак, стратешки документи све више препознају отпорност и способност реаговања као компоненте положаја одвраћања. Противник који процењује вредност сајбер упада мора узети у обзир не само потенцијалне добити већ и брзину опоравка браниоца, способност узвратног деловања и механизме савезничке подршке (NATO, 2020).

Осигуравање информационе безбедности стога доприноси одвраћању на два комплементарна начина. Прво, смањењем рањивости оно умањује очекивану ефикасност противничких операција. Друго, демонстрирањем координисаног управљања и спремности, оно сигнализира припремљеност. Стратешка комуникација у вези са сајбер способностима све више постаје део националних одбрамбених наратива. Ова димензија сигнализирања утиче на противничке процене ризика чак и у одсуству кинетичке ескалације.

Технолошки суверенитет представља још један одлучујући фактор. Војне мреже зависе од хардверских компоненти, софтверских платформи, инфраструктуре у облаку и ланаца снабдевања који могу излазити изван националне јурисдикције. Прекомерно ослањање на спољне добављаче уводи стратешки ризик. Рањивости ланца снабдевања, уграђена „задња врата" и непрозирност животног циклуса софтвера могу да подривају дугорочно обезбеђење. Због тога агенде модернизације одбране наглашавају безбедне ланце снабдевања, поуздане добављаче и развој домаћих способности (U.S. Department of Defense, 2023).

Суверенитет не подразумева изолацију. Мултинационалне операције захтевају интероперабилне системе. Стратешки изазов лежи у успостављању равнотеже између међузависности и аутономије. Федеративни мрежни модели и архитектуре нултог поверења нуде делимична решења, омогућавајући сарадњу без безусловног поверења. Међутим, механизми управљања морају обезбедити да националне информације од критичног значаја остану заштићене у оквиру савезничких структура.



Слика 3: Стратешки оквир обезбеђења информационе безбедности (https://link.springer.com/chapter/10.1007/978-3-030-64351-5_9)

Стратешка димензија односи се на правне и нормативне структуре. Сајбер операције укрштају се са међународним правом, правилима ангажовања и савезничким обавезама. Механизми управљања морају дефинисати прагове за реаговање, процедуре атрибуције и протоколе координације са цивилним властима. Замагљивање граница између цивилне и војне инфраструктуре у сајбер простору захтева интегрисане механизме цивилно-војне координације. Националне стратегије сајбер безбедности све више одражавају овај интегрисани приступ.

Узети заједно, управљање, одвраћање и технолошки суверенитет одређују стратешко окружење у којем функционише оперативна отпорност. Без кохерентног управљања, отпорност постаје фрагментисана. Без кредибилног одвраћања, отпорност остаје реактивна. Без технолошког суверенитета, отпорност постаје спољa зависна (Schmitt, 2017).

У савременом безбедносном окружењу војно информационо обезбеђење због тога није само техничка дисциплина већ стратешки инструмент. Оно подржава оперативни континуитет, јача кохезију савезништва и обликује противничке процене. Његова стратешка вредност не лежи само у спречавању поремећаја већ и у очувању слободе деловања у оспораваном дигиталном бојишту.

Закључак

Савремено одбрамбено окружење потврђује да је војна моћ неодвојива од отпорности њене дигиталне архитектуре. Обезбеђење информационе безбедности превазишло је оквире техничке заштите и данас представља структурни предуслов оперативне кохерентности и стратешког кредибилитета. Савремене оружане снаге не користе мреже само као средство; оне посредством њих функционишу. Командовање, обједињавање обавештајних података, логистичко обезбеђење и синхронизација здружених ватрених дејстава зависе од интегритета токова података у оспораваним доменима (NATO, 2020; U.S. Department of Defense, 2023).

Анализа показује да се обезбеђење информационе безбедности остварује у три међусобно зависне димензије. Прво, оно је доктринарно утемељено у признавању сајбер-простора као оперативног домена и у развоју вишедоменских операција. Друго, на оперативном нивоу испољава се кроз механизме отпорности чија је сврха очување континуитета извршења мисије у условима сајбер-електромагнетног супротстављања. Треће, на стратешком нивоу њиме се управља посредством институционалних овлашћења, положаја у систему одвраћања и технолошког суверенитета.

Оперативна отпорност издваја се као одлучујућа карактеристика савремених војних мрежа. Апсолутна заштита није ни остварива нити је доктринарно реалистична. Циљ је очување континуитета функционисања под притиском, односно одржавање способности командовања упркос покушајима ометања. Редундантност, сегментација, децентрализовано извршавање и механизми брзог опоравка нису технички луксуз, већ оперативна нужност у окружењима у којима се деградација способности очекује, а не представља изузетак.

На стратешком нивоу, кохерентност управљања одређује да ли ће се отпорност преточити у кредибилан одбрамбени положај. Јасно дефинисана одговорност у командовању, усклађени стандарди, безбедне праксе набавке и координација у оквиру савеза обезбеђују да се заштита и поузданост мрежа не фрагментишу дуж институционалних граница. Истовремено, видљива отпорност доприноси одвраћању тако што утиче на процену ризика потенцијалног противника. Снага способна да апсорбује последице сајбер-агресије и да се од њих опорави умањује перципирану корисност такве агресије.

Технолошки суверенитет додатно условљава дугорочно обезбеђење. Зависност од рањивих ланаца снабдевања или нетранспарентних дигиталних екосис-

тема уводи структурне ризике. Стратешка аутономија у критичним дигиталним способностима јача националну отпорност, уз истовремено очување интероперабилности у оквиру савеза. Равнотежа између интеграције и суверенитета представља једну од кључних противречности савремене одбрамбене политике.

У безбедносном окружењу које карактеришу трајно надметање и брзе технолошке промене, обезбеђење информационе безбедности мора се посматрати као трајна стратешка функција. Оно подржава оперативну ефикасност, јача кохезију савеза и чува слободу деловања у оспораваном дигиталном борбеном простору. Заштита војних мрежа више није помоћни задатак; она представља темељни предуслов кредибилне одбране у двадесет првом веку.

Стратешке димензије изложене у овом раду потврђују ширу доктринарну трансформацију: дигитална отпорност сада представља саставни део борбене моћи. Тамо где су токови информација безбедни и отпорни, могуће је задржати оперативну иницијативу. Тамо где су они рањиви, стратешки положај слаби. У савременом ратовању, одбрана мрежа неодвојива је од одбране државе.

Литература

[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

[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

[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

[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

[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

[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

[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

[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

[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

[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

Р е з и м е

Обезбеђивање информационе безбедности постало је критична компонента савремених војних способности имајући у виду све већу зависност од умрежених система у области командовања, контроле, комуникације и доношења одлука. Савремене доктрине одбране све више препознају да војне мреже нису само техничка инфраструктура већ и стратешка средства чији интегритет, расположивост и поверљивост непосредно утичу на оперативну ефикасност и стратешку отпорност. У раду се разматрају стратешке димензије обезбеђења информационе безбедности у војним мрежама у контексту савремене доктрине одбране.

Истраживање анализира начин на који се питања информационе безбедности интегришу у доктринарне оквире и процесе стратешког планирања, са посебним нагласком на њихову улогу у подршци командовању и контроли, очувању надмоћи у одлучивању и јачању отпорности на сајбер и хибридне претње. При-

меном концептуалног и аналитичког приступа, у раду се указује на однос између обезбеђења информационе безбедности, војне стратегије и политике одбране, а не искључиво на техничке механизме заштите. Посебна пажња посвећена је импликацијама пропуста у области информационе безбедности по оперативни континуитет и стратешку стабилност у савременим конфликтним окружењима.

Анализа показује да делотворно осигурање информационе безбедности захтева свеобухватан приступ који обједињује техничке мере са организационим, доктринарним и стратешким елементима. У раду се заступа становиште да је интеграција обезбеђења информационе безбедности у доктрину одбране од суштинског значаја за очување оперативног кредибилитета и обезбеђивање ефикасне употребе војних мрежа у савременом и будућем безбедносном окружењу.

Кључне речи*: обезбеђивање информационе безбедности, војне мреже, доктрина одбране, војна стратегија, сајбер и хибридне претње*

© 2026 Аутор. Објавило *Војно дело* (http://www.vojnodelo.mod.gov.rs). Ово је чланак отвореног приступа и дистрибуира се у складу са лиценцом Creative Commons (http://creativecommons.org/licenses/by/4.0/).

