Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Project „Misijomis grįstų mokslo ir inovacijų programų įgyvendinimas“ (Project Nr. 02-002-P-0001) report

Project name: ***EPMwDC***

Responsible/Implementation partner (-s): ***MRU***

Action result: ***Cybersecurity Standards According to NATO Requirements***

Table of Contents

Cybersecurity Standards According to NATO Requirements
Project Deliverable – Research Report Section
Project: Implementation of Mission-Based Science and Innovation Programs (Project No. 02-002-P-0001)

1. Scope and Methodological Note

This section addresses the requirement to document cybersecurity standards according to NATO requirements as they apply to AI-powered dual-use systems. During the course of the research, consultations were held with military stakeholders, which confirmed that the primary NATO cybersecurity governance instruments – the NATO Information Assurance Policy (NIAP), the NATO Security Policy (NSP), and the NATO Cyber Defence Policy – are classified or restricted-access documents. Their full content is not available for open publication or direct reproduction in unclassified research outputs.

Consequently, this section does not attempt to reproduce the content of these instruments. Instead, it draws on publicly available NATO policy documents, academic literature analysing NATO's cybersecurity governance architecture, and the proceedings of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) to provide a structured account of:

- the architecture of NATO's cybersecurity governance and accreditation framework;
- the publicly known principles and requirements that flow from these instruments;
- how the layered compliance model operates for dual-use systems deployed in both EU and NATO contexts;
- how the EPMwDC ontological framework models obligations derived from NATO instruments without reproducing restricted content.

This approach ensures that the research deliverable remains both substantive and compliant with information security requirements.

2. NATO's Cybersecurity Governance Architecture

2.1 Strategic Evolution

NATO's engagement with cybersecurity has evolved through a series of strategic milestones. Following the 2007 cyberattacks on Estonia – which were later retrospectively reclassified within NATO's hybrid threat framework (Attila, 2025) – NATO established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn and began formalising its cyber defence policy architecture.

The 2014 Wales Summit endorsed the Enhanced NATO Policy on Cyber Defence, which remains the Alliance's foundational policy document. This was followed by the 2016 Warsaw Summit, at which NATO recognised cyberspace as an operational domain alongside land, sea, air, and space – a decision described by Bigelow (2017) as "both long-expected due to growing awareness of cyber security challenges within the Alliance and bold in its willingness to recognise what is still an immature and evolving discipline." The recognition of cyberspace as an operational domain meant that the NATO Command Structure assumed responsibility for implementing doctrine, organisation, and capabilities for operations in cyberspace (Bigelow, 2017; Robinson, 2017).

More recently, the 2024 revised NATO AI Strategy emphasises reliable implementation of AI within NATO structures, requiring adherence to six governance principles: lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, and bias mitigation (NATO, 2024a). The 2025 Data Strategy for the Alliance underscores the transition to a data-centric organisation, implementing security-by-design and privacy-by-design principles through a Data Centric Reference Architecture and standards such as STANAG 5636 for semantic interoperability (NATO, 2025). NATO's Digital Transformation Implementation Strategy further requires interoperability across domains and the integration of cybersecurity and cyber defence practices into operational environments (NATO, 2024b).

2.2 The Three Core Governance Instruments

Three classified or restricted instruments constitute the backbone of NATO's cybersecurity accreditation framework:

NATO Information Assurance Policy (NIAP). NIAP defines the requirements for protecting information processed, stored, or transmitted within NATO communications and information systems. While its full content is not publicly available, publicly accessible literature indicates that NIAP mandates multi-layered security controls, including encryption, access controls, and incident response capabilities. NIAP establishes the requirements against which systems must be evaluated during the security accreditation process (Sabaliauskaite et al., 2026; Domingo & Wietgrefe, 2012).

NATO Security Policy (NSP). The NSP establishes the overarching framework for protecting classified information within NATO. Publicly known requirements include access controls, physical security measures, and personnel security training for handling classified information. The NSP defines the classification levels and handling procedures that govern how AI systems that process or display classified material must be designed and operated (Sabaliauskaite et al., 2026).

NATO Cyber Defence Policy. This instrument governs the protection of digital assets from cyber threats, including – relevantly for the espionage detection system case study – unauthorised data capture through non-networked means such as cameras. The Cyber Defence Policy requires detection mechanisms, secure incident reporting through encrypted channels, and threat intelligence sharing across NATO entities (Sabaliauskaite et al., 2026).

2.3 Accreditation Rather Than Conformity Assessment

A fundamental distinction between NATO and EU compliance pathways is the mechanism of enforcement. EU regulatory compliance is achieved primarily through conformity assessment under market legislation (e.g., AI Act, CRA, NIS2). NATO compliance, by contrast, is achieved through *security accreditation* – a process by which a designated authority formally certifies that a system meets the security requirements defined by NIAP, NSP, and the Cyber Defence Policy before it may be deployed within Alliance-controlled infrastructures (Sabaliauskaite et al., 2026; Simola et al., 2024).

This distinction is significant for dual-use systems. A system placed on the EU market is subject to conformity assessment under EU legislation. The same system deployed within NATO environments must additionally satisfy NATO accreditation requirements. The compliance structure is cumulative rather than substitutive: EU market obligations operate alongside defence accreditation requirements, subject to applicable exemptions under EU law.

3. The Information-Sharing and Interoperability Architecture

3.1 NATO Network-Enabled Capabilities (NNEC) and the Future Mission Network

NATO's approach to information sharing in operations has been formalised through the NATO Network-Enabled Capabilities (NNEC) concept and its implementation as the Future Mission Network (FMN). NNEC enables NATO to maximise information and service sharing across missions characterised by uncertainty about service requirements, partner composition, and command structures (Domingo & Wietgrefe, 2012).

The FMN implements a NNEC-aligned set of networks, systems, and services – together with the necessary doctrine and processes – to facilitate federation of mission information in future operations. Lessons from ISAF (Afghanistan) and Operation Unified Protector (Libya) demonstrated that deploying NNEC capabilities from scratch is complex and time-consuming, motivating the formalisation of FMN as a flexible, tailorable, and scalable capability (Domingo & Wietgrefe, 2012).

A critical challenge in this architecture is the federation of information across multiple security domains. Domingo and Wietgrefe (2013) describe how a clearinghouse function and release gateway enable semi-automatic transfer of releasable information between security domains, creating the perception of a single information domain while maintaining classification boundaries. This architecture has direct implications for dual-use AI systems that must transmit alerts or intelligence across different security domains.

3.2 Cyber Defence Information Sharing in Federated Networks

Kantola and Jaitner (2016) examine the specific challenge of cyber defence information sharing within federated military networks such as FMN. They identify that federated networks should form groups of interest where not only technical information but also analysed tactical and operational information, and to a certain extent intrusion method

information, is shared within the group. Their key finding is a set of information categories that should be shared in a federated network to enable responsive cyber defence.

This is directly relevant to the EPMwDC framework's modelling of the NATO Cyber Defence Policy sub-requirement DEF-USAGE-R4-ART7 (Threat Intelligence Sharing), which captures the obligation to share threat intelligence across NATO entities through secure channels.

3.3 Deployable Communications and Information Systems (DCIS)

Van Selm et al. (2018) describe the architecture of NATO's next-generation Deployable Communications and Information Systems (DCIS), which includes information assurance as a core service. The DCIS Cube architecture defines vendor-neutral, software-defined building blocks providing infrastructure-as-a-service, including security services. This architecture enables NATO to provision all deployable functionality on standard hardware through software configuration, with independent evolution of hardware, infrastructure, application, and orchestration layers.

For AI systems intended for deployment in NATO field environments, compliance with DCIS architecture principles – including the information assurance service layer – would be an additional consideration beyond the core NIAP/NSP/Cyber Defence Policy requirements.

4. The EU-NATO Compliance Interface

4.1 Comparative Frameworks

The relationship between the EU and NATO cybersecurity frameworks is one of complementarity rather than duplication, though challenges of harmonisation persist. Stitilis et al. (2017) compare EU and NATO cybersecurity strategies and their correspondence with national strategies, finding that despite similar goals of ensuring cyber resilience, the harmonisation approaches and norms of national cybersecurity strategies differ significantly between the two frameworks.

Parmar and Miles (2024) compare the NIST CSF v2.0 with EU standards for the defence sector, addressing the need for holistic cybersecurity coverage at the intersection of NATO operational requirements and EU regulatory obligations. Simola et al. (2024) analyse how EU-level cybersecurity requirements (particularly NIS2) affect standardisation for cybersecurity governance in operational technology environments, identifying four governance levels – political, strategic, operational, and tactical – that map to both EU regulatory and NATO accreditation structures.

Shopina et al. (2020) examine the legal and organisational dimensions of cybersecurity support across leading countries and NATO/EU standards, providing a comparative perspective on how different jurisdictions implement cybersecurity governance frameworks.

4.2 The Layered Compliance Model for Dual-Use Systems

For dual-use AI systems, the compliance landscape can be understood as a set of cumulative layers, each governed by different instruments and enforcement mechanisms:

Compliance Layer	Governing Instruments	Enforcement Mechanism
EU Data Protection	GDPR, Law Enforcement Directive, national laws	Supervisory authority oversight; DPIA
EU Cybersecurity	NIS2 Directive, CRA, GDPR Art. 32	National authority compliance attestation
EU AI Regulation	AI Act (for civilian deployment)	Conformity assessment; CE marking
NATO Information Assurance	NIAP, NSP	Security accreditation
NATO Operational Security	NATO Cyber Defence Policy	Accreditation; operational directives
Certification Standards	TEMPEST, STANAG (where applicable)	NATO certification processes

A system deployed exclusively in civilian contexts needs to satisfy only the first three layers. A system deployed within NATO environments must satisfy all six. The key design implication, as established by Sabaliauskaite et al. (2026), is that the system architecture should accommodate the most stringent (defence) requirements, enabling civilian deployment as a subset configuration.

4.3 The Role of NATO CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence, based in Tallinn, Estonia, serves as a primary public-facing source of knowledge on NATO's approach to cyber defence. Its contributions include the Tallinn Manual on the International Law Applicable to Cyber Operations (Schmitt, 2017), which provides the most comprehensive publicly available analysis of how international law applies to cyber warfare and cyber operations. While the Tallinn Manual addresses international law rather than technical accreditation standards, it establishes the legal framework within which NATO's cybersecurity governance operates.

The CCDCOE also organises the annual CyCon conference and the Crossed Swords and Locked Shields exercises, which generate publicly available proceedings and technical reports. Recent work by Ferazza et al. (2026) demonstrates the use of MITRE ATT&CK-enriched meta-alerts, validated on data from the Crossed Swords exercise, illustrating how NATO exercise environments contribute to the development of publicly available cybersecurity methodologies.

Crandall and Allan (2015) document how Estonia – home to the CCDCOE – has leveraged its NATO membership to function as a norm entrepreneur in cybersecurity, promoting international norms and standards that extend beyond the Alliance.

5. Publicly Known NATO Cybersecurity Principles and Requirements

While the specific technical requirements of NIAP, NSP, and the Cyber Defence Policy remain classified, the following principles and requirement categories can be identified from publicly available policy documents and academic literature:

5.1 Security-by-Design

NATO policy documents consistently emphasise security-by-design as a foundational principle. The AI Strategy requires that technologies used in NATO or dual-use contexts adhere to security-by-design principles and confirm compliance with international law before deployment (NATO, 2024a). The Data Strategy operationalises this by requiring a Data-Centric Reference Architecture that implements security-by-design and privacy-by-design (NATO, 2025).

5.2 Encryption and Access Control

Publicly available descriptions of NIAP requirements reference multi-layered security controls, including NATO-approved cryptographic modules – distinct from the commercial TLS/AES standards that suffice for EU civilian compliance under GDPR Art. 32 and NIS2 Art. 21. Access controls in NATO environments involve security clearance verification and need-to-know enforcement, supplementing the role-based access controls typical of civilian deployments (Sabaliauskaite et al., 2026).

5.3 Personnel Security

The NSP establishes requirements for personnel security, including security clearances and training for handling classified information. This extends to operators of AI systems deployed in NATO environments: dedicated security personnel receiving alerts from systems such as the espionage detection system must hold appropriate clearances and receive training specific to their role.

5.4 Incident Detection, Reporting, and Threat Intelligence Sharing

The Cyber Defence Policy requires detection mechanisms for cyber threats – including non-traditional vectors such as unauthorised visual capture of classified information. Detected incidents must be reported through secure, encrypted channels. Threat intelligence must be shared among NATO entities to support collective defence in cyberspace (Sabaliauskaite et al., 2026; Kantola & Jaitner, 2016).

5.5 TEMPEST and Electromagnetic Security

For systems that display or process classified information, TEMPEST certification may be required to protect against compromise through electromagnetic emanations. This is particularly relevant to the espionage detection system case study, where the monitor displays classified content and must be protected against electromagnetic intelligence gathering as well as visual surveillance.

5.6 Interoperability and Semantic Standards

NATO's Data Strategy and Digital Transformation Implementation Strategy require interoperability across domains, supported by standards such as STANAG 5636 for semantic interoperability (NATO, 2022; NATO, 2025). For AI systems that process or share information across NATO networks, compliance with these interoperability standards is an additional requirement beyond the cybersecurity baseline.

6. How the EPMwDC Ontology Models NATO Requirements

The EPMwDC ontological framework (Sabaliauskaite et al., 2026; Paskauskas, 2026) addresses the challenge of modelling obligations derived from classified instruments through several design decisions:

Structural representation without content reproduction. The ontology represents NIAP, NSP, and the NATO Cyber Defence Policy as named entities within the regulatory framework class hierarchy (NATORegulations), and links them to the defence compliance domain (RegComplyforDefenceUse) via standard object properties (derivedFrom, appliesToDomain). The *structure* of the obligations is modelled – their allocation to lifecycle phases, their classification as privacy-related or security-related, their decomposition into sub-requirements – without reproducing the classified content of the source instruments.

Obligation-level rather than instrument-level modelling. Requirements such as DEF-DESIGN-R2 (NATO Security Controls) and DEF-USAGE-R4 (NATO Cyber Defence Compliance) capture the *categories* of obligation (encryption, access control, detection mechanisms, incident reporting, threat intelligence sharing) at a level of abstraction that is publicly known, without specifying the classified technical parameters that would be required for actual accreditation.

Hierarchical decomposition for extensibility. The sub-requirement structure (e.g., DEF-USAGE-R4-ART3, DEF-USAGE-R4-ART5, DEF-USAGE-R4-ART7) is designed to accommodate future refinement as additional detail becomes available – whether through declassification, through engagement with accreditation authorities during prototype development, or through the evolution of NATO's public-facing guidance.

Domain tagging for deployment-specific retrieval. The appliesToDomain property enables SPARQL queries that retrieve defence-specific requirements separately from civilian requirements, supporting the generation of deployment-specific compliance checklists. A query filtered to rc:DefenceDomain returns only those requirements that apply to NATO deployment contexts, including the obligations modelled from NIAP, NSP, and the Cyber Defence Policy.

This approach ensures that the ontological framework is both useful (it captures the structure and categories of NATO obligations) and responsible (it neither reproduces nor implies access to classified content).

7. Limitations and Recommendations for Future Work

The principal limitation of this analysis is that the NATO cybersecurity governance instruments at its core – NIAP, NSP, and the Cyber Defence Policy – are not publicly available for direct analysis. The account provided here is necessarily derived from secondary sources: publicly available NATO policy summaries, academic literature, and the abstracted representation of the ontological framework as described in Sabaliauskaite et al. (2026).

For prototype development and eventual deployment in NATO environments, the following steps are recommended:

1. *Engagement with national accreditation authorities***.** Each NATO member state maintains a national security authority responsible for accrediting systems that process classified information. Early engagement with the relevant Lithuanian authority (the State Security Department or its designated body) would enable the prototype developer to obtain guidance on the specific accreditation requirements applicable to the system.

2. *TEMPEST assessment.* If the system is intended to display classified information, a formal TEMPEST assessment should be conducted to determine the applicable emission security requirements and any necessary shielding or zoning measures.

3. *NATO CCDCOE engagement***.** The CCDCOE offers a range of publicly accessible resources, exercises, and collaborative programmes that could support the refinement of the ontological framework's NATO compliance modelling.

4. *Ontology refinement during accreditation.* As the prototype progresses through the accreditation process, the EPMwDC ontology's defence requirements module should be iteratively refined to incorporate the specific technical parameters and control requirements identified during accreditation. The hierarchical decomposition structure is designed to accommodate this refinement without alteration to the overall ontology architecture.

8. References

- Attila AN (2025). Retrospective securitisation and hybrid threats: reframing the 2007 Estonian cyberattacks in NATO's strategic discourse. *European Security*. DOI: 10.1080/09662839.2025.2581171.
- Bigelow B (2017). Mission Assurance: Shifting the Focus of Cyber Defence. *9th International Conference on Cyber Conflict (CyCon)*, 43–54.
- Costea AM (2023). Private-Public Partnerships in Cyber Space as Deterrence Tools: The Trans-Atlantic View. *Europolity*, 17(2): 111–134.
- Crandall M, Allan C (2015). Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms. *Contemporary Security Policy*, 36(2): 346–368.
- Domingo A, Wietgrefe H (2012). A NNEC-Compliant Approach for a Future Mission Network. *IEEE MILCOM 2012*.
- Domingo A, Wietgrefe H (2013). On the federation of information in coalition operations: building single information domains out of multiple security domains. *IEEE MILCOM 2013*, 1462–1469.
- Ferazza F, Melella C, Mersinas K, Lugo R, Ottis R (2026). From logs to tactics: unsupervised reconstruction of APT campaigns with MITRE-enriched meta-alerts. *International Journal of Information Security*, 25(3): 79.
- Kantola H, Jaitner ML (2016). Cyber Defence Information Sharing in a Federated Network. *IEEE CyCon U.S. 2016*, 86–93.
- NATO (2022). NATO Core Metadata Specification (NCMS) – ADatP-5636 Edition A.
- NATO (2024a). Summary of NATO's Revised Artificial Intelligence (AI) Strategy.
- NATO (2024b). NATO's Digital Transformation Implementation Strategy.
- NATO (2025). Data Strategy for the Alliance.
- Parmar M, Miles A (2024). Cyber Security Frameworks (CSFs): An Assessment Between the NIST CSF v2.0 and EU Standards. *IEEE Security for Space Systems Conference (3S)*.
- Paskauskas RA (2026). SecOntologyLab/regulatory-compliance-ontology: Initial Public Release. Zenodo. DOI: 10.5281/zenodo.18763491.
- Robinson N (2017). Cyber Defense at NATO: From Wales to Warsaw, and Beyond. *Turkish Policy Quarterly*, 16(3): 133–143.
- Sabaliauskaite G, Paskauskas RA, Bružė E, Matulytė R, Lavišius T (2026). Automated regulatory compliance for AI systems in the security domain: The case of dual-use deployment. *Open Research Europe*, 6:83. DOI: 10.12688/openreseurope.23137.1.
- Schmitt M (2017). *Tallinn Manual on the International Law Applicable to Cyber Operations*. Cambridge University Press. DOI: 10.1017/9781316822524.
- Shopina I, Khomiakov D, Khrystynchenko N, Zhukov S, Shpenov D (2020). Cybersecurity: Legal and Organizational Support in Leading Countries, NATO and EU Standards. *Journal of Security and Sustainability Issues*, 9: 977–992.
- Simola J, Takala A, Lehkonen R, Frantti T, Savola R (2024). The Importance of Cybersecurity Governance Model in Operational Technology Environments. *23rd European Conference on Cyber Warfare and Security*, 502–511.
- Stitilis D, Pakutinskas P, Malinauskaite I (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal*, 30(4): 1151–1168.
- Van Selm M, Wietgrefe H, Varanda J, Janezic D (2018). DCIS Cube: Defining Architecture Building Blocks for Next Generation Deployable IT systems. *IEEE MILCOM 2018*, 672–677.
- Vollmer B (2021). NATO's Mission-Critical Space Capabilities under Threat: Cybersecurity Gaps in the Military Space Asset Supply Chain. *arXiv*: 2102.09674.

Editor
<<Main Editor>>

Contributors
Evaldas Bruze (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)
Saulius Kvedaravičius (MRU)

Reviewers
Evaldas Bružė (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)
Saulius Kvedaravičius (MRU)

Disclaimer