HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 4. szám 17–38.
DOI: 10.32567/hm.2025.4.2

Károly Kassai[1]

Cybersecurity Challenges of the Integration of Artificial Intelligence (AI) Solutions

Military Requirements, Question Marks and Efforts

Abstract

The applicability of artificial intelligence (AI) is no longer in question today. AI has become so integrated into countless areas of the economy and society that we no longer even notice that a given service is provided by an AI system. The use of AI systems is a sensitive issue in many areas, such as the armed forces. This paper draws attention to the diversity of military applications of AI and the general risks involved. The armed forces need to use not just one or two AI systems, but dozens of AI solutions that must be integrated into military information systems. These AI systems perform tasks at different operational levels or support the operation of other systems.

The study provides guidance on the most important steps in the necessary risk management, based on the legal framework, standards and best practices. Tailored risk management provides the basis for local, system-specific regulation of military organisations, which must be compiled from existing cybersecurity framework elements. The study emphasises that AI systems cannot be exempt from cybersecurity regulations, so it is necessary to review and supplement existing tools and provide training.

Keywords: artificial intelligence (AI), military information system, cybersecurity, trustworthiness, risk

[1] Section Head, Ludovika University of Public Service, Faculty of Military Science and Officer Training, Department of Military National Security, e-mail: karoly.kassai@yahoo.com

Introduction

Artificial intelligence (AI) is introducing new military capabilities and augmenting existing ones at *strategic, operational* and *tactical* levels. Military organisations operate a diverse ecosystem of AI systems and AI-supported services that must interoperate with legacy platforms, communications networks and each other.

Some systems deliver advanced technical effects through speed, scale and precision; others collect and analyse critical operational data and sensitive tactical sensor streams, contribute to strategic decision preparation, or support decisions where errors can cause military operational disadvantage, injury or serious damage.

This complexity creates new design, operational and governance challenges for military information systems.

We can recognise that, alongside these characteristics, the situation is further complicated by the fact that cybersecurity considerations are an integral part of integrating AI into the military information environment.

A dedicated literature review shows that AI-related issues are receiving growing attention within military science. Hungarian scholarship documents the evolution of AI technologies,[2] illustrates the diversity of military AI system solutions (dozens of land, air and naval devices).[3]

Broader reviews of AI and other disruptive technologies emphasise the need for holistic perspectives and illustrate diverse applications (for example, healthcare; education; energy; finance; supply chains; social media; law enforcement; intelligence). Those studies also highlight legal, ethical, economic and social implications and governance challenges such as oversight and control.[4]

Another Hungarian study examines AI's military application within intelligence branches, exploring analytic and evaluative capabilities in this sensitive domain.[5]

A dedicated Hungarian volume examines AI's social and ethical impacts; general regulatory and legal issues (robot law and human rights); data protection and communications; and economic considerations.[6]

Alongside these extensive, high-level studies, domain-specific functional examinations also exist that address security in various formulations. However, such works treat cybersecurity and operational security issues *only marginally*.

This paper pursues two objectives. The primary research objective is to review and compare regulatory and governance elements from policy domains analogous to AI (for example, cybersecurity, data protection, critical infrastructure protection, classified information protection) to identify institutional functions and pillars that support AI safety and security, without performing a formal legal analysis.

The practical research objective is to synthesise cybersecurity considerations for AI as an information system to support organisational implementation and strategic risk analysis.

[2] Négyesi 2022: 194–195.
[3] Négyesi 2023.
[4] Kovács 2023.
[5] Erdész 2023.
[6] Török–Ződi 2021.

In order to achieve the research objectives, we shall establish two guiding hypotheses for testing:

- H1. Organisational processes and governance elements relevant to cybersecurity for AI systems are broadly comparable to those in regulated domains, permitting transfer of useful regulatory and organisational design lessons.
- H2. The traditional cybersecurity risk analysis approach is a viable starting framework for AI cybersecurity, provided it is extended with AI-specific trustworthiness dimensions (for example, privacy, auditability, fairness and safety).

The study employs a targeted qualitative, comparative content analysis. Selected EU and Hungarian legislation, ISO[7] standards and ENISA[8] recommendations, sectoral regulatory documents and relevant scholarly literature were examined to map the functional elements and institutional pillars of domains analogous to AI.

The selection of high-level comparison pillars is based on practical experience. We can easily see that these are the most important requirements, which provide the framework for organisational-level regulation.

The analytical framework overlays traditional cybersecurity objectives (confidentiality, integrity, availability) with AI-specific trustworthiness dimensions. Identified regulatory and operational functions were mapped into an analytic matrix against these dimensions.

Risk analysis in this study is high-level and qualitative. Rather than performing a full quantitative risk assessment, the second part focuses on a compact, three-parameter framework – threats, affected security objectives and AI-specific trustworthiness factors supplemented by attention to life-cycle stages –, to demonstrate a practicable, logically coherent basis. In this examination, the selection of sources serves to test the logical line of "mandatory", "recommended" and "optional".

NATO key aspects of the military application of AI systems

The NATO Secretary General noted in 2023 that the AI, the autonomous systems and other emerging technologies *are transforming conflict dynamics,* thereby requiring new capability development, enhanced private-sector partnerships and global standards.[9]

The NATO's revised AI Strategy accelerates and mainstreams the integration of AI into Allied defence capabilities under six principles of responsible use. The document emphasises the indispensable role of AI-ready quality data, harmonised standards and a comprehensive testing, evaluation, verification and validation framework, while actively shaping international norms for the secure and transparent use of AI.[10]

The NATO Science and Technology Strategy guides the Alliance to lead both AI development and its rapid adoption. Its strategic objectives – Anticipate and Invest (fostering AI R & D), Safeguard and Protect (securing AI assets and expertise) and

[7] ISO: International Organization for Standardization.
[8] ENISA: European Network and Information Security Agency.
[9] NATO 2023.
[10] NATO 2024: 2, 5 and 13.

Orchestrate and Energise (fast-track AI deployment in operations) – provide a clear roadmap.[11]

EU high-level approach

President von der Leyen emphasised in 2025 that European AI underpins the EU's strategic autonomy and sectoral resilience, from healthcare to defence. She called for precise mandates under the proposed Cloud and AI Development Act and the Quantum Sandbox, and underscored public-private cooperation via the European AI & Tech Declaration.[12]

The European Parliament welcomes proposals for joint European defence projects, including AI development for sovereign infrastructure and critical support assets. Where possible, development should focus on *rapidly available European technologies* (reducing dependency).[13]

We must accept as a limitation that a detailed comparison of the EU and NATO AI objectives and processes is not possible due to the lack of publicly available information. However, the presented high-level statements illustrate similar approach to the strategic requirements and future plans regarding AI application.

Ethical and legal considerations

An EU parliamentary report notes that most current AI systems fall into the low-risk category. However, systems designed, developed or operated under inadequate supervision in military command centres *pose significant risks* and may contribute to conflict escalation.[14]

A fundamental question regarding autonomous weapon systems is that human involvement and oversight *must play a central role* in the lethal decision-making process. The European Parliament emphasises that it is extremely important to prevent the development and production of lethal autonomous weapon systems that lack human control in critical functions, such as target selection and engagement.[15]

Scientists, industrial experts and Pentagon officials are predicting the emergence of fully autonomous lethal weapons in the U.S. Human control will still remain, but the question is whether this is real control or just some sort of supervisory role. The U.S. military is heavily working on human–machine collaboration (e.g. the Air Force's "loyal wingman" programme, where F-16 pilots and autonomous drones work together).[16]

Strict prohibitions regarding the application of AI systems provoke new ideas that examine the legitimacy of traditional prohibitions in the current context, and

[11] NATO 2025b: 4, 11, 18.
[12] European Commission 2025.
[13] European Parliament 2025a: 58.
[14] Voss 2022: 4.
[15] European Parliament 2018: G and point 4.
[16] Bajak 2023.

encourage a modern assessment of the advantages and disadvantages, which may be particularly important in the field of nuclear deterrence.

AI systems provide opportunities to strengthen nuclear deterrence by increasing precision and efficiency. Thus, the capability for nuclear deterrence becomes *more credible*. Due to concerns related to AI, it should not be excluded from the reinforcement of nuclear deterrence. At the same time, the reinforcement using AI systems must serve a strategic purpose; it cannot be merely a routine deployment. A balance must be struck on this difficult issue, as science is still unable to answer every question accurately.[17]

We can assume that the aforementioned air force solutions, alongside nuclear deterrent systems, involve AI systems that support intelligence, strategic decision-making preparation, target identification and tactical combat management operations, *employing a wide range of technical solutions*.

Consequently, it is *unlikely that a single model could address the issue of integrating* – or substituting – the human control point. At present, we can state that, given knowledge of the specific processes, elements and operational mechanisms, it is possible to identify approximate points for assessing the transition from human oversight to full autonomy, as well as the associated risks.

We will later observe the latest development regarding the international approach.

Emerging international cooperation

An international initiative has been established to solve the problems related to AI and autonomous systems, initiated by the U.S.

The purpose of the Declaration is to establish guidelines and norms regarding the military application of AI and autonomous systems. The document provides an opportunity for participants (with Hungary as a founding member) to create a normative framework, establish international consensus, as well as to facilitate the exchange of experiences and capacity building.[18] The outcome of the initiative is greatly influenced by the number and capabilities of the participating states, and the group of non-participating countries can also be regarded as a *clear signal*. The need for international cooperation related to AI systems can also be identified in the civil sector.

The aim of the cooperation established by the EU Member States (Declaration of Cooperation on Artificial Intelligence) is to leverage the opportunities offered by AI systems and to collectively address the challenges (e.g. legal and ethical considerations, trust and accountability).[19]

AI systems that operate without human supervision raise moral, social and legal questions and problems. Due to the pace of technological development, there is a need for the development of policies, procedures and standards related to applications,

[17] Puwal 2024.
[18] U.S. Department of State 2024.
[19] European Commission 2018.

going beyond the best practices currently considered "human-in-the-loop" solutions. Additionally, there is a need to rethink the human-machine relationship, as future AI-based systems will have *both humans and AI systems as users.*[20]

The technical levels of EU–NATO cooperation are not public information, but the annual report on EU–NATO collaboration provides guidance on the role of AI. We can see that the political dialogue section considers AI as an important objective, alongside other goals, such as resilience, quantum technologies, arms control, military mobility, energy security, space cooperation, digital transformation, capability development and countering hybrid threats. Within the Emerging and Disruptive Technologies (EDT) domain, a key area of cooperation is the defence and dual-use applications of AI, quantum technologies and biotechnology, as well as related investments, technology testing, validations and innovation standards. Among research areas, AI and its responsible use are also highlighted, alongside technical foresight, research security and energy security.[21]

The UN Secretary-General's report (A/79/88) signals strong support for a legally binding instrument to ensure meaningful human control. Following informal consultations in 2025, a concrete proposal is expected in 2026, potentially forming the basis of a future international legal framework on lethal autonomous weapons systems.[22]

We can see that the positions presented so far are clear indicators for us that AI operations, including security issues, *need to be addressed on a priority basis.*

We can also perceive that international initiatives reflect significant interest and the necessity of sharing resources, which accelerates the pace of development and introduces *numerous new perspectives.*

At the same time, it is also clear to us that *significant challenges must still be addressed* before the successful establishment of international regulations for military applications.

After highlighting some examples of AI applications, the following chapters will present the Hungarian military situation based on the available information, including the significant regulatory measures with a security focus that have been taken so far.

Trends and directions

Recent public announcements clearly illustrate the speed of adaptation of AI:

- NATO's Smart Indication and Warning Broad Area Detection (SINBAD) satellite surveillance system maps change along the eastern flank at unprecedented frequency, issuing AI-driven threat warnings[23]
- The Maven Smart System of NATO Communications and Information Agency (NCIA), procured in just six months, delivers intelligence fusion, targeting, battlespace awareness and decision support[24]

[20] Jenkins 2023.
[21] European Council – NATO 2025: 3, 10.
[22] United Nations 2024: 1–3, 15–17.
[23] Fratsyvir 2025.
[24] NATO 2025a.

- SAAB's Gripen E "Centaur" tests integrate AI-driven autonomous manoeuvres directly into the aircraft, bypassing separate test and experimental environments.[25] (The Hungarian Air Force has Gripen fighters in service)
- France's Collaboration Homme-Machine (CoHoMa) programme trials legged, wheeled and tracked autonomous platforms in realistic battlefield simulations, emphasising the transition from lab prototypes to operational environments and a complementary human–machine partnership[26]

These examples represent a subset of global military AI projects. In the following, we can see that the Hungarian approach to the military application of artificial intelligence systems follows international trends.

Kristóf Szalay-Bobrovniczky (Hungarian Minister of Defence), in his presentation titled *Algorithms on the Frontline* at the AI Summit Conference 2025 in Budapest, stressed Hungary's political-level AI requirements for the armed forces. Digitalisation is central to force modernisation: the digital battlefield and personal-equipment sensors demand AI-driven data processing. Key military AI application areas include autonomous systems, training and logistics, with attention to cybersecurity, legal and ethical issues.[27]

According to Gergely Németh, Chief Executive Officer (2025), the new technology laboratory at the Defence Innovation Research Institute offers novel opportunities for Hungarian military development. Development programmes focus on machine-learning-based data analysis and drone control, with additional objectives including the testing and operational implementation of unmanned systems, training modules and autonomous capabilities.[28]

We can clearly see that the political and leadership opinion argues in favour of using AI, which is also reflected in the national strategy.

The second-generation Hungarian Artificial Intelligence Strategy (2025–2030) builds on its predecessor, summarising achievements and outlining new objectives. The Strategy defines military and national military security objectives at a high level (for example, automation of decision support; predictive analytics; development of autonomous systems and human–machine collaboration; modelling and simulation; data collection, processing and analysis) and introduces the new "Chief Artificial Intelligence Officer" function.[29]

After a brief examination, we can state that currently no other published official Hungarian military strategic-level document (e. g. strategy, action plan, roadmap or blueprint) can be identified, but the scientific examination of the topic has begun.

In summary, we can conclude that rejecting the use of AI and seeking other alternative solutions is *not a realistic approach.* Furthermore, the rapid pace of AI development precludes hesitation, despite current legal, social and other reservations.

[25] Defensemirror.com 2025.
[26] Kajal 2025.
[27] Erős 2025.
[28] Honvéd Vezérkar 2025.
[29] Magyarország Mesterséges Intelligencia Stratégiája (2025–2030) 2025: 78, 79.

These examples demonstrate that the challenge lies not in a single AI solution but in integrating multiple AI systems and embedded AI services.

This dual challenge requires armed forces to prepare existing systems and networks for AI integration and identify essential AI capabilities, select candidate systems, assess emerging risks and define integration parameters.

We can state that a critical step is to identify or develop AI systems that meet the military operational requirements of the Hungarian land and air forces, followed by comprehensive testing, where necessary.

Implementation decisions should be made based on early-stage data on AI solution architecture, operational characteristics, functional and security risks, development processes and prior deployment experiences. This underlines the importance of *effective military – defence industrial cooperation* and common thinking.

To shorten procurement cycles, defining precise operational requirements must be strengthened, and procurement planning and procedures streamlined and accelerated. Considering *life cycle stages and supply chain processes is essential.* Threats can cause *cascade risks,* potentially undermining the trustworthiness of the AI system.

We can confirm that successful AI implementation also depends on factors such as NATO and EU interoperability, preparing forces for AI–human teaming across all command levels, and close collaboration with research institutes, universities and defence-tech companies.

The examples also illustrate that, beyond concerns about lethal autonomous weapons, there is a growing emergence of AI platforms that replace humans – autonomous "combat robots" – driven by advanced human–machine collaboration, which raise *control, regulatory* and *operational* challenges.

In the Hungarian Defence Forces, core requirements for autonomous weapons and defence systems are set at the legislative level (for example, human-intervention capability, awareness of system operation and adherence to operational rules) under the National Defence Act.[30] These regulations require further specification at subordinate levels and integration of emerging international standards.

The military Chief Artificial Intelligence role can prioritise land and air force AI developments, minimise resource competition and ensure adequate resourcing. Defining its authority and position within the organisational hierarchy is essential.

The following sections will provide us with an overview of important high-level risk considerations regarding the military application of AI systems in Hungary.

High-level risk considerations of AI systems

The European Commission Recommendation (2023) ranked AI as one of the top *four threats among ten critical technical areas.* The Commission calls on Member States to conduct a collective risk assessment to identify major threat categories; threatening actors (including geopolitical adversaries); likelihood of occurrence; the technology

[30] Act CXL of 2021, para. 3, para. 92. Section (1).

value chain; and chokepoints. The risk assessment focuses on risks with European wide impact.[31]

Based on the EU's proposal, we can assume that the investigations conducted by the member states contribute to the identification of AI threats and the development of risk management through synergistic effects across various domains.

Reviewing the EU and national frameworks provides an opportunity to explore security-related analogies. Among the possible areas, we examine those that appear to be significant from the perspective of AI: on the infrastructure side, *general network security* and *critical infrastructures,* and on the data management side, the *protection of classified information* as well as *personal data.*

As an introduction, we need to identify a specific limitation. The main EU and national requirements are considered publicly accessible information. NATO regulatory documents in similar areas (e.g. directives and supporting guidelines) are classified information or not publicly accessible; therefore, their examination or comparison with EU rules cannot be carried out in this study.

Identifying parameters of different areas based on the same criteria enables the formulation of general conclusions.

Table 1 shows that the structure of the regulatory framework at EU and national level is clear and understandable, so that important steps in the field of AI can also be predicted at national level. We can observe that, despite the EU-level exemption for the defence sector, according to the Hungarian approach, *national legislation also covers the military domain.*

We also note that, in the four areas, the relevant national legislation specifies the designation of the national competent authorities.

Similarly, it can be identified that implementing organisations must designate the responsible organisational element or individual and develop organisation-specific regulations based on risk analysis. To address threats at the national level, organisational entities are required to report incidents to the national authorities.

The draft Hungarian AI Act indicated in the table sets out the establishment of AI authorities as defined by the EU AI Act and the reporting procedure, and lays down rules for the Hungarian AI Council and the regulatory sandbox for AI.[32]

The draft decree designates the AI authorities, the reporting procedure, possible fines and detailed rules relating to the Council.[33]

These drafts were developed based on the government resolution on the establishment of a national framework for AI[34] and a subsequent government resolution.[35]

[31] European Commission 2023: 1–3.
[32] Act of 2025 (draft) on the implementation of the European Union Regulation on Artificial Intelligence, paras. 4, 5, 8, 9 and 10.
[33] Decree of Government (draft) on the implementation of the European Union Regulation on Artificial Intelligence Act, paras. 1–5.
[34] Government Resolution of 1301/2024 (IX. 30.), point 2.
[35] Government Resolution of 1149/2025 (V. 14.), points 2–3.

Table 1: Regulatory frameworks related to AI

Area	**Data protection**	**Cybersecurity**	**Resilience of critical entities**	**Classified information protection**	**Artificial Intelligence**
Identification of EU regulation	Regulation (EU) 2016/679 (GDPR)[36]	Directive (EU) 2022/2555 (NIS2 Directive)	Directive (EU) 2022/2557 (CER Directive)[37]	Council Decision 2013/488/EU (EUCI)[38]	Regulation (EU) 2024/1689 (AI Act)
Type of enforcement	Directly applicable	Enforced by national legislation	Enforced by national legislation	Enforced by national legislation	Directly applicable
Type of national regulation	Act	Strategy, Act, supporting decrees	Strategy, Act, supporting decrees	Act, supporting decrees	Act (draft), supporting decree (draft)
National responsible organisation	National Authority for Data Protection and Freedom of Information	National Cyber Security Centre	National Directorate General for Disaster Management, Ministry of the Interior	National Security Authority	National AI Office (planned)
Designation of a responsible person or organisational element	Yes	Yes	Yes	Yes	Yes
Organisational-level risk management obligation	Yes	Yes	Yes	Yes	Yes
Organisational level regulatory obligation	Yes	Yes	Yes	Yes	Yes
Obligation to notify the national responsible organisation	Yes	Yes	Yes	Yes	Yes
Incident reporting obligation	Yes	Yes	Yes	Yes	Yes
Applicable to the Hungarian Defence Forces	Yes	Yes	Yes	Yes	Yes

Source: compiled by the author

[36] Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR).
[37] Directive (EU) 2022/2557 of the European Parliament and of the Council.
[38] Council Decision of 23 September 2013 (2013/488/EU).

In the topic of the responsible organisational element, the question is about the representation of the military role (e.g. an independent military responsible organisational element or integration into the national authority).

After studying the AI related drafts, we can conclude that *they do not address AI-specific cybersecurity requirements.* Based on this, we can state that measures related to the security of AI systems should be developed and maintained *within the framework of general, cross-sector security regulations.*

The EU AI Act (2024) mandates that high-risk AI systems operate under a documented, maintained risk-management system covering the entire lifecycle and addressing known and foreseeable risks.[39] While the regulation is clear, a recurring question is whether general standards can be applied to AI.

An ENISA report (2023) responds that, despite AI's unique attributes, it remains fundamentally software; hence, established software requirements and procedures can be adapted.[40]

The EU NIS2[41] Directive (2024) obliges Member States to implement security requirements and controls for the cybersecurity of electronic systems and services, including supply chain risk management procedures.[42]

We have previously observed the emergence of procurement and supply chain security issues. Going forward, it will become apparent that these issues may pose significant risks in relation to AI systems.

The associated NIS2 Implementation Regulation (2024) elaborates basic requirements for risk management frameworks, incident management, business continuity and crisis management and supply chain security.[43]

These high-level provisions can be applied to AI system security, with domain-specific adaptations.

The Cybersecurity Act (2024)[44] at national level sets out the general security requirements in line with EU NIS2 and the Implementing Regulation, while details are provided in Decree 7/2024 (VI. 24.).[45]

To establish the protective measures for an AI system – as an electronic information system – we need to review the elements that are more significant from a risk analysis perspective. The general cybersecurity framework does not define an exact risk management methodology, thereby granting applying organisations considerable decision-making flexibility.

Among the key issues, we should identify the *cyber threats, cybersecurity objectives* and *critical lifecycle stages* to consider. Other mandatory elements of risk analysis, such as the severity and likelihood of occurrence, may perhaps be more easily adopted for AI cases.

[39] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, Section (9).
[40] Bezombes et al. 2023: 17.
[41] Network and Information Security.
[42] Directive (EU) 2022/2555, Section (21).
[43] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024, Section (11)–(15) and Annex points 1–5.
[44] Act LXIX of 2024 on the cyber security of Hungary.
[45] Decree 7/2024 (VI. 24.) of the Prime Minister's Office on the requirements for security classification and the specific protective measures applicable to each security classification.

As an initial step, we can select general cybersecurity considerations, which can then be further developed. During the development process, following the line of *regulations (requirements), international standards, recommendations* and other sources provides comprehensive solutions.

This approach offers a general, flexible model that can be finalised based on organisational and technical specific parameters, as well as other sensitive information.

We need to clarify two important factors in advance:

- These regulations set out a framework and allow organisations to tailor security measures to their specific needs
- The decree combines security measures with traditional cybersecurity objectives (confidentiality, integrity and availability), which must be supplemented with "identification" in accordance with the EU NIS2 Directive (Article 6) – a factor that is also significant in the case of AI systems

The decree sets out minimum requirements (Annex 3), that must be applied to threat aspects ("threat list"), which must also be applied to AI systems. The Hungarian National Cyber Security Centre published a guide on security classification and practical application of national requirements to support organisations.[46] The guide outlines general risk-management tasks – such as defining procedures, assigning responsibilities, assessing and approving risks and periodic reviews – that apply regardless of technology, leaving room for AI-specific adaptations.

The ENISA 2020 report, following ISO 27005 standard, identifies asset, threat, and threat-actor mapping as essential to risk analysis. Based on the report, we can clearly identify that the traditional security objectives (confidentiality, integrity, availability) apply to artificial intelligence, complemented by authentication, access control and non-repudiation.

AI-specific attributes include robustness, trustworthiness, safety, transparency, explainability, accountability and data protection. The report categorises 74 AI-related cyber threats into eight groups, mapped to lifecycle stages to guide responsible stakeholders.[47] The "security-by-design" principle embeds security considerations throughout the product lifecycle. The ENISA 2023 report proposes AI evaluation criteria slightly different from the previous report – privacy protection, explainability, robustness, fairness – each of which is related to risk assessment and management processes (these aspects have also been incorporated into the cybersecurity goals in Table 2).[48]

The ISO/IEC[49] 5338 Standard defines lifecycle stages as inception, design and development, verification and validation, implementation, operation and monitoring, continuous validation, reassessment and withdrawal.[50]

[46] National Cyber Security Centre 2025: 3.
[47] Malatras–Dede 2020: 12, 25, 27 and Annex B, D.
[48] Pascu – Barros Lourenco 2023: 11.
[49] ISO/IEC: International Organization for Standardization/International Electrotechnical Commission.
[50] ISO/IEC 2023a: 5.

The U.S. national AI risk management standard applies a different approach, namely plan and design, collect and process data, build and use models, verify and validate, deploy and use, operate and monitor.[51]

As an interesting point, we observe that beyond the life cycle phases of standards, it is worthwhile to examine a scientific approach (Table 2), which clearly illustrates flexible solution options.

Table 2: Threats, cybersecurity goals and life cycle stages of AI

Threat categories	**Cybersecurity goals and supplements**
Elements of the threat catalogue (Decree 7/2024, Annex 3) Elements of ENISA 2020 report, in 8 groups: Nefarious activity/abuse Eavesdropping/Interception/ Hijacking Physical attacks Unintentional damage Failures or malfunctions Outages Disaster Legal Elements of EU AI threat reports Elements of EU and NATO military threat reports	Confidentiality, integrity, availability and identification (as basic cybersecurity elements) and AI specific supplements (ENISA 2020): Authentication Authorisation Non-repudiation Robustness Trustworthiness Safety Transparency Explainability Accountability Data protection Possible additions based on ISO/IEC 23894:52 AI expertise Environmental impact Fairness Maintainability Privacy Robustness Other military speciality, depends on functions, elements
Life cycle stages	
ISO/IEC 5338: inception, design and development, verification and validation, implementation, operation and monitoring, continuous validation, reassessment and withdrawal AI RMF: Plan and design, collect and process data, build and use model, verify and validate, deploy and use, operate and monitor Technical approach:[53] Data sources, input data, data cleaning, data storage, data processing, data analysis, model development, machine learning, output data and communication networks	

Source: compiled by the author

[51] NIST 2023: 10.
[52] ISO/IEC 2023b: Annex A, A3, A5–9.
[53] Kollár 2019: 62.

We can identify that the elements related to threats and security objectives have been *significantly expanded* in Table 2. Subsequently, it becomes possible to supplement these with organisation and military specifications (or to remove non-essential elements). We note that this option also represents a limitation. If security management does not filter the organisation-specific and the applied (or planned) AI parameters, the establishment of a risk analysis will not be feasible.

We also recognise that, compared to the standards and recommendations, the lifecycle phases included in the academic classification are more detailed and practical. This also supports a more refined risk-based approach. The modular structure allows us to adapt a risk analysis methodology that aligns with organisational characteristics and AI specifications.

Table 2 also supports another conclusion. The situation for security management will become more difficult because as the number of parameters increases, the possible combinations multiply. In the case of a complex information system, *manual risk analysis is practically impossible*.

We must not forget that integrating AI into an organisational information system involves examining both the existing system (and its elements) and the software (or AI-containing platform) that comprises the AI together.

In summary, the presented method enables an organisation to define the security objectives for a specific AI product, the relevant lifecycle stages and the scope of applicable threats. The table indicates the necessity of incorporating military specifications, but we strongly emphasise that processing and integrating military operational and tactical requirements is essential, as failing to do so *may lead to serious issues*.

The key question is whether the implementing organisation is capable of customising the set of mandatory and optionally selectable elements. It can also be observed that the terminology and conceptual framework appearing in international AI standards (and other sources) have not yet been fully clarified. The components of "trustworthiness", considered a fundamental attribute of AI, are not unified, which allows for different interpretations. Therefore, the security management has a key responsibility in establishing an approved and functional organisational risk methodology or model, providing clear framework for the interpreted parameters. Based on the experience from Table 1, it is advisable to establish a working group whose members are experienced in risk analysis across various domains.

The collected information provides a basis for further conclusions that we can also draw.

The examination of AI platforms (system components), which consist of existing and new infrastructure elements, should begin at the earliest possible stage. The organisation's existing risk assessment documentation (as well as incident management and audit reports) should be reviewed, and the tests and evaluation materials carried out in previous lifecycle phases of the planned AI system should also be examined. This again requires close cooperation and institutionalisation of horizontal organisational relationships, as well as collaboration between the military organisation and defence industry actors (including necessary authorisations and information security considerations).

Furthermore, based on what we have observed so far, we can also conclude that the assessment and quantification of new organisational security objectives (e.g. trustworthiness and its components) must be ensured to meet the criterion of verifiability.

Cybersecurity considerations

Risk analysis is not an end in itself, but rather a practical tool for determining system-specific security controls.

The AI-specific additions to security objectives outlined in Table 2, by themselves, do not contain implementable security controls (e.g. in the case of "accountability" or "explainability"). Therefore, it is necessary to apply system-specific frameworks that include *technically interpretable, measurable parameters and repeatable procedures* aligned with general objectives.

We present that in the domains of security objectives, one of the tools for gradually establishing measurability is the application of the AI Trust Framework and Maturity Model (AI-TMM) which is aligned with risk analysis. Within the framework of the Maturity Indicator Levels (MIL 1–3), each objective (or domain) begins with the documentation of fundamental principles (L1: formulation of principles), continues with the introduction of initial indicators and management practices (L2: indicators, managed processes), and culminates in a fully integrated, continuously monitored and audited system (L3: monitoring and audit).

The model thus serves as a diagnostic instrument for identifying risks and provides the foundation for appropriate protective measures, ensuring the transparent traceability of trustworthiness.[54]

In another solution, we demonstrate that the AI Trustworthiness Assessment Framework (AI TAF) is capable of mapping human risks in detail. The framework identifies the affected groups and models, based on specific scenarios, how an AI failure or misuse could cause physical, economic or psychological harm. To what extent are the harms reversible? The method takes into account exposure and vulnerability, assigns controls (preventive, detective, corrective) to each risk, establishes go/no-go thresholds, and is intended to be complemented by integration into the lifecycle.[55]

We can see that these models provide measurability and enable the development of specific parameters related to the AI system to ensure the enforceability of security controls.

The aforementioned Hungarian decree (7/2024), which defines national cybersecurity requirements, contains hundreds of security controls, grouped into several categories and assigned to three security classes (low, medium, and high).

We know that military organisations regulate the cybersecurity of their information systems (including AI systems) according to their operational maturity and mission profile. This may take the form of a comprehensive, lengthy regulation or

[54] Mylrea–Robinson 2023.
[55] Seralidou et al. 2025: 4.

a structured framework consisting of high-level requirements supported by detailed procedural documents.

When developing and maintaining cybersecurity controls and procedures, it is essential to understand and correctly manage dependencies between systems. AI capabilities operated by tactical units – or their failure – can have cascading effects, causing significant disadvantages at the operational or even strategic level.

We can state that during the design phase of an AI capability, the technical operational requirements and the security classification of the system must be identified as early as possible. Failure to do so can lead to complex interoperability issues between the host network and the AI system, necessitating costly retroactive investments.

Unique procedures must be established to ensure the cooperation (integration, interconnection of services) of platforms with different security classifications. A higher security classification may also compel the operating organisation to make substantial additional security investments.

In addition to the aforementioned, we must also *highlight the role of incident management*. Due to the possibility of cascade-type security incidents, incident management procedures must be continuously refined during development and deployment in order to minimise damage.

These considerations underscore the importance of *close cooperation between developers, producers and the military organisation* during the design phase. Early engagement with cybersecurity specialists and alignment with recognised international standards can reduce long-term costs and improve resilience.

Finally, we emphasise that higher command has the authority to influence the regulatory practices of subordinate military organisations and to coordinate tasks when shared resources are involved. This top-down alignment is critical to ensuring consistent security postures, avoiding duplication of effort and maintaining operational readiness.

We present the following high-level recommendations outlining the practical steps for integrating robust security practices into AI-supported military systems:

- early security classification
- tailored control implementation
- cross-disciplinary design teams
- dependency and interoperability management
- alignment with international standards
- continuous monitoring and audit
- top-down regulatory coordination
- lifecycle security management
- secure supply chain oversight
- incident response preparedness

By using these guides, military stakeholders can ensure that AI-enabled capabilities remain secure, resilient and aligned with mission objectives throughout their operational lifecycle.

Conclusion

The paper demonstrates that military forces must adopt AI with the same urgency seen in social and economic domains. The military force modernisation requires integrating AI systems and services; failure to do so invites significant operational and strategic risks.

The issue of lethal autonomous weapons remains urgent, with evolving regulatory and ethical challenges. Hungary must continuously harmonise its national military requirements with international norms.

When the military uses AI capabilities, numerous technical, operational, legal, and ethical considerations demand attention. The paper points out that secure deployment is not possible without knowledge of the necessary technical, operational, and procedural parameters.

We can summarise that the planned review of regulations in the analogous field, as well as the examination of opportunities for developing elements supporting risk analysis, yield practical, usable results.

We can observe that, according to H1, existing organisational starting points can, with further efforts, support the operation of AI systems. Similar steps can be expected in the case of regulatory needs for new technologies (e.g. quantum). During the examination, we can conclude that, based on the presented existing legal requirements, the regulation of AI cybersecurity is not unrealistic, but it requires a great deal of clarification and refinement. Based on this, hypothesis H1 can be validated.

We can confirm that in the area specialised for risk analysis, based on H2, organisation-specific models and methods can be developed, and it can be seen through examples that the new parameters can be made measurable (enabling their verification). Based on the examples presented, we can confirm as a general observation that alongside legal, international standards and best practice (recommendation) sources, it is also advisable to *take academic initiatives into consideration.* Based on this, we can state that hypothesis H2 is valid. This is further reinforced by the fact that the new perspectives and factors significantly complicate the task of security management.

Given budgetary and personnel constraints, prioritising AI support for land or air forces is essential. Effective prioritisation and resource allocation can be facilitated by the Chief Artificial Intelligence Officer role, ideally positioned within the Ministry of Defence. We note that the best tool for determining the priority order of tasks and scheduling resources is to develop a *military AI strategy (or action plan).* This can represent the requirements, the responsibilities of the participants (including operational and security management requirements, development and integration plans), deadlines, as well as visible training tasks, in order to ensure the success of further progress.

Based on the presented information, it is clear that the reviewed sources emphasise that AI is not exempt from cybersecurity requirements. The protective measures mapped to predefined security classes – augmented with AI-specific clarifications – can fulfil system cybersecurity requirements.

The future will show whether this prediction will be fulfilled or refuted. A follow-up study in several years is recommended.

References

Bajak, Frank (2023): Pentagon's AI initiatives Accelerate Hard Decisions on Lethal Autonomous Weapons. *AP News,* 25 November 2023. Online: https://apnews.com/article/us-military-ai-projects-0773b4937801e7a0573f44b57a9a5942

Bezombes, Patrick – Brunessaux, Stéphan – Cadzow, Scott (2023): *Cybersecurity of AI and Standardisation.* European Union Agency for Cybersecurity (ENISA). Online: https://doi.org/10.2824/277479

DefenseMirror.com (2025): Saab Tests AI co-Pilot in Gripen Fighter Jet for First Time. *DefenseMirror.com,* 11 June 2025. Online: www.defensemirror.com/news/39650

Erdész, Viktor (2023): *A mesterséges intelligencia alkalmazása a katonai nemzetbiztonsági hírszerzésben* [The Use of Artificial Intelligence in Military National Security Intelligence]. Budapest: Katonai Nemzetbiztonsági Szolgálat.

Erős, Hunor (2025): A mesterséges intelligencia a magyar honvédségbe is beépült [Artificial Intelligence has also been Integrated into the Hungarian Military]. *Magyar Nemzet,* 9 September 2025. Online: https://magyarnemzet.hu/belfold/2025/09/a-mesterseges-intelligencia-a-magyar-honvedsegbe-is-beepult

European Commission (2018): *EU Member States Sign Up to Cooperate on Artificial Intelligence.* 10 April 2018. Online: https://digital-strategy.ec.europa.eu/en/news/eu-member-states-sign-cooperate-artificial-intelligence

European Commission (2023): *Commission Recommendation of 03 October 2023 on Critical Technology Areas for the EU's Economic Security for Further Risk Assessment with Member States.* C(2023) 6689 final. Online: https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en

European Commission (2025): State of the Union Address by President von der Leyen, 10 September 2025. Online: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_25_2053

European Council – NATO (2025): *Tenth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.* Online: www.consilium.europa.eu/media/f54kvokr/250605-progress-report-nr10-eu-nato.pdf

European Parliament (2018): European Parliament Resolution of 12 September 2018 on Autonomous Weapon Systems (2018/2752(RSP). Online: www.europarl.europa.eu/doceo/document/TA-8-2018-0341_EN.html

European Parliament (2025): *White paper on the future of European Defence.* European Parliament Resolution of 12 March 2025 on the White Paper on the Future of European Defence (2025/2565(RSP)). Online: www.europarl.europa.eu/doceo/document/TA-10-2025-0034_EN.pdf

Fratsyvir, Anna (2025): NATO Expands Satellite Surveillance to Monitor Ukraine, Eastern Flank. *The Kyiv Independent,* 12 June 2025. Online: https://kyivindependent.com/nato-expands-satellite-surveillance-to-monitor-ukraine-eastern-flank/

Honvéd Vezérkar [Armed Forces General Staff] (2025): Újdonságok a védelmi innováció területén [News in the Field of Defence Innovation]. *Honvédelem.hu,*

2 June 2025. Online: https://honvedelem.hu/hirek/ujdonsagok-a-vedelmi-innovacio-teruleten.html

ISO/IEC (2023a): Information Technology – Artificial Intelligence – AI System Life Cycle Processes. ISO/IEC 5338. First edition.

ISO/IEC (2023b): Information Technology – Artificial intelligence – Guidance on Risk Management. ISO/IEC 23894. First edition.

Jenkins, Michael P. (2023): The Impact and Associated Risks of AI on Future Military Operations. *Federal News Network,* 18 October 2023. Online: https://federalnewsnetwork.com/commentary/2023/10/the-impact-and-associated-risks-of-ai-on-future-military-operations/

Kajal, Kapil (2025): France Plans to Deploy Combat Robots by 2027, Eyes Full Robot Army by 2040. *Interesting Engineering,* 8 May 2025. Online: https://interestingengineering.com/military/france-eyes-all-robot-army-by-2040

Kollár, Csaba (2019): A mesterséges intelligencia, mint komplex rendszer információbiztonsági kihívásai [Information Security Challenges of Artificial Intelligence as a Complex System]. In Rajnai, Zoltán (ed.): *Kiberbiztonság/Cybersecurity*. Budapest: Biztonságtudományi Doktori Iskola, 62–70. Online: https://drkollar.hu/wp-content/uploads/2020/01/kiadvany-2019.pdf

Kovács, Zoltán ed. (2023): *A mesterséges intelligencia és egyéb felforgató technológiák hatásainak átfogó vizsgálata* [Comprehensive Review of the Impact of Artificial Intelligence and Other Disruptive Technologies]. Budapest: Katonai Nemzetbiztonsági Szolgálat.

Magyarország Mesterséges Intelligencia Stratégiája (2025–2030) [Hungary's Artificial Intelligence Strategy (2025–2030)]. (2025). Online: https://cdn.kormany.hu/uploads/document/c/c0/c0d/c0dfdbd37cfa520ae37361a168d244c85e7295af.pdf

Malatras, Apostolos – Dede, Georgia (2020): *AI Cybersecurity Challenges. Threat Landscape for Artificial Intelligence.* European Union Agency for Cybersecurity (ENISA). Online: https://doi.org/10.2824/238222

Mylrea, Michael – Robinson, Nikki (2023): Artificial Intelligence (AI) Trust Framework and Maturity Model: Applying an Entropy Lens to Improve Security, Privacy, and Ethical AI. *Entropy,* 25(10). Online: https://doi.org/10.3390/e25101429

NATO (2023): *Speech by Secretary General Jens Stoltenberg at the NATO-Industry Forum.* 25 October 2023. Online: www.nato.int/cps/en/natohq/opinions_219128.htm

NATO (2024): *Summary of NATO's revised Artificial Intelligence (AI) Strategy.* 10 July 2024. Online: www.nato.int/cps/en/natohq/official_texts _227237.htm

NATO (2025a): *NATO Acquires AI-Enabled Warfighting System.* 14 April 2025. Online: https://shape.nato.int/news-releases/nato-acquires-aienabled-warfighting-system-

NATO (2025b): *NATO Science & Technology Strategy. Defending the future, today!* Online: www.nato.int/content/dam/nato/webready/documents/sto/STO-strategy-2025.pdf

Négyesi, Imre (2022): *A mesterséges intelligencia katonai felhasználásának lehetőségei: Első kötet* [The Possibilities of Military Use of Artificial Intelligence Vol. I]. Budapest: HM Zrínyi Média Közhasznú Nonprofit Kft.

NÉGYESI, Imre (2023): *A mesterséges intelligencia katonai felhasználásának lehetőségei: II. kötet* [The Possibilities of Military Use of Artificial Intelligence Vol. II]. Budapest: HM Zrínyi Média Közhasznú Nonprofit Kft.

Nemzeti Kiberbiztonsági Intézet [National Cyber Security Centre] (2025): *Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója. Kozkázatkezelés* [Guideline for the Application of the Cybersecurity Requirements Catalogue of Electronic Information Systems and Organisations. Risk Management]. Online: https://nki.gov.hu/wp-content/uploads/2025/09/15.-Kockazatkezeles-ver.-1.1.pdf

NIST (2023): *Artificial Intelligence Risk Management Framework* (AI RMF 1.0). Online: https://doi.org/10.6028/NIST.AI.100-1

PASCU, Corina – BARROS LOURENCO, Marco eds. (2023): *Artificial Intelligence and Cybersecurity Research.* ENISA Research and Innovation Brief. European Union Agency for Cybersecurity (ENISA). Online: https://data.europa.eu/doi/10.2824/808362

PUWAL, Steffan (2024): Should Artificial Intelligence Be Banned from Nuclear Weapons Systems? *NATO Review,* 12 April 2024. Online: https://archives.nato.int/uploads/r/nato-archives-online/d/3/8/d388000c2ba6b51ffb20865bb71d1828203cb6e45312f46ec1cf202fe918ca81/2024-04-12_Should_artificial_intelligence_be_banned_from_nuclear_weapons_systems_ENG.pdf

SERALIDOU, Eleni – KIOSKLI, Kitty – FOTIS, Theofanis – POLEMI, Nineta (2025): AI_TAF: A Human-Centric Trustworthiness Risk Assessment Framework for AI Systems. *Computers,* 14(7). Online: https://doi.org/10.3390/computers14070243

TÖRÖK, Bernát – ZŐDI, Zsolt eds. (2021): *A mesterséges intelligencia szabályozási kihívásai* [The Regulatory Challenges of AI]. Budapest: Ludovika Egyetemi Kiadó.

U.S. Department of State (2024): *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy.* Online: www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy

United Nations (2024): *Lethal Autonomous Weapons Systems: Report of the Secretary-General* (A/79/88). Online: https://digitallibrary.un.org/record/4059475

VOSS, Axel (2022): *Report on Artificial Intelligence in a Digital Age.* European Parliament Report A9 0088/2022. Online: www.europarl.europa.eu/doceo/document/A-9-2022-0088_EN.html

Legal sources

2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről [Act CXL of 2021 on National Defence and Hungarian Defence Forces]

2024. évi LXIX. törvény Magyarország kiberbiztonságáról [Act LXIX of 2024 on the Cyber Security of Hungary]

2025. évi … törvény az Európai Unió mesterséges intelligenciáról szóló rendeletének magyarországi végrehajtásáról [Act of 2025 (draft) on the implementation of the European Union Regulation on Artificial Intelligence]. Online: https://cdn.

kormany.hu/uploads/document/b/b9/b92/b929cdec547b87da4bd23bce694d-b86ce328e1c6.pdf

1301/2024. (IX. 30.) Korm. határozat a mesterséges intelligenciáról szóló európai parlamenti és tanácsi rendelet végrehajtásához szükséges intézkedésekről [Government Resolution of 1301/2024 (IX. 30.) on measures necessary for the implementation of the Regulation of the European Parliament and of the Council on artificial intelligence]

1149/2025. (V. 14.) Korm. határozat a mesterséges intelligenciáról szóló európai parlamenti és tanácsi rendelet végrehajtásához szükséges intézkedésekről szóló 1301/2024. (IX. 30.) Korm. határozatban foglalt feladatok végrehajtásáról [Government Resolution of 1149/2025 (V. 14.) on the implementation of the tasks set out in GR of 1301/2024 (IX. 30.) on the measures necessary for the implementation of the Regulation of the European Parliament and of the Council on artificial intelligence]

7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről [Decree 7/2024 (VI. 24.) of the Prime Minister's Office on the requirements for security classification and the specific protective measures applicable to each security classification]

A Kormány rendelete az Európai Unió mesterséges intelligenciáról szóló rendeletének magyarországi végrehajtásáról szóló 2025. évi … törvény végrehajtásáról [Decree of Government (draft) on the implementation of the on the implementation of the European Union Regulation on Artificial Intelligence]

Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU)

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)