DUAL-USE TECHNOLOGIES AND CYBERSECURITY CHALLENGES IN THE CURRENT MILITARY DEFENSE ENVIRONMENT

Adriana NIȚESCU[*,], Tiberiu TĂNASE[*,**]**

[*]"Politehnica" University of Bucharest, Romania
[**] Romanian Academy | DIS - CRIFST

DOI: 10.19062/2247-3173.2026.27.30

Abstract: *Dual-use technologies—systems and capabilities applicable to both civilian and military domains—have become a central component of modern defense ecosystems, situated at the intersection of accelerated technological innovation and evolving strategic security requirements.*

This paper analyzes the cybersecurity challenges arising from the integration of dual-use technologies into the defense architectures of NATO, the European Union, and Romania, with a particular focus on regulation as a key instrument for control, security, and strategic governance.

The study highlights that dual-use regulation, including international frameworks such as the Wassenaar Arrangement and European Union legislation (Regulation EU 2021/821), directly shapes access to, transfer of, and deployment of critical technologies such as artificial intelligence, cloud computing, and advanced semiconductors. In this context, regulation functions not only as a mechanism for mitigating proliferation risks, but also as a strategic factor influencing technological sovereignty and competitive advantage.

Beyond the normative dimension, the paper examines cybersecurity risks associated with dual-use ecosystems, including supply chain vulnerabilities, reliance on commercial digital infrastructure, cyber espionage, and risks arising from the use of artificial intelligence systems in hybrid civil–military environments. Institutional limitations are also addressed, particularly slow procurement cycles and interoperability fragmentation within NATO and the EU.

In conclusion, securing dual-use technologies requires an integrated approach combining regulation, technological innovation, and international cooperation to strengthen resilience and ensure security in the contemporary defense landscape.

Keywords: *dual-us technologies, cybersecurity, regulation, export control, defense ecosystem, NATO, European Union, technological sovereignty*

1. INTRODUCTION

According to the Draghi Report, the European Union is simultaneously facing three major strategic pressures: the innovation gap compared to the United States and China, the imperative of economic decarbonization, and the urgent need to strengthen defense capabilities through accelerated innovation and rearmament.

Within this geopolitical and economic framework, dual-use technologies represent not merely an efficient method, but the only financially viable solution capable of sustaining the required pace of military rearmament and technological modernization in defense.

While the EU's traditional defense industry remains deeply fragmented along national lines a phenomenon that generates redundant duplication and prohibitively high equipment costs dual-use technologies capitalize on the advantages of mass production within the commercial civilian sector. Thus, manufacturing high volumes of sensor systems or aerial vectors (drones) on civilian industrial production lines reduces the unit cost by up to 80% compared to production processes specific to exclusive military infrastructures.

Moreover, the dynamics of the conflict in Ukraine have demonstrated that innovations in the digital spectrum, such as artificial intelligence, edge computing, and cryptography, undergo transformation cycles measured in weeks. Ministries of Defense within EU member states are unable to develop or procure software solutions at such speed through traditional public procurement procedures. Consequently, the integration and adaptation of existing civilian algorithms compress the operational deployment timeline on the battlefield from years to mere days.

However, dual-use technologies do not constitute a universal solution. They cannot replace the need for large-caliber ammunition and heavy combat platforms, while also presenting severe structural limitations regarding strategic dependencies on critical raw materials and the cybersecurity gap between civilian and military standards.

In order to remedy this resilience deficit in an accelerated manner, the present doctoral research is focused on the development of a dynamic cybersecurity auditing algorithm for dual-use technologies generated within the civilian sector.

This study, entitled ***"Dual-Use Technologies and Cybersecurity Compliance Challenges in the Current Military Defense Environment"*** constitutes the analytical pillar through which essential security requirements are identified, ranked, and prioritized in concrete dual-use projects of a classical, convergent, hybrid, and emerging nature.

2. CONTEXT

2.1 Dual-Use Technologies as Mixed Technologies

The concept of dual-use technologies is almost contemporaneous with the invention of the first tools. Throughout history, numerous innovations have simultaneously served both civilian and military purposes. Relevant examples include stone and metal processing (used for agricultural tools, construction, and weaponry), the bow and arrow (employed in hunting and warfare), gunpowder (initially used in pyrotechnics and medicine, later revolutionizing military warfare), and internal combustion engines (applied in automotive transport as well as civil and military aviation).

The term acquired significant geopolitical importance during the twentieth century, particularly after the Second World War and throughout the Cold War, with the proliferation of nuclear weapons and ballistic missiles. Many of these technologies had direct applications within the civilian energy sector (nuclear reactors) and aerospace infrastructure (space propulsion), requiring the establishment of strict regulations aimed at preventing proliferation.

2.2 When Did the Fracture Between Civilian and Military Technologies Emerge?

The fracture, defined as a pronounced structural divergence between the development of civilian and military technologies, became visible with the Industrial Revolution and consolidated during the twentieth century. As research and development (R&D) activities became institutionalized at governmental and corporate levels, distinct objectives, funding mechanisms, technical requirements, and implementation timelines emerged for each sector.

The post-Second World War period marks the moment when this divergence reached its peak. Massive investments in military R&D (the Manhattan Project, the aerospace industry, and advanced electronics) generated unique requirements for armed forces characterized by extreme robustness, absolute security, and operational performance in hostile environments standards that exceeded the needs of the commercial market. Simultaneously, the civilian sector focused primarily on cost optimization, scalability, and comfort.

2.3 Causes That Contributed to the Separation of Dual-Use Technologies

Table 1 - Comparative analysis of civil-military structural separation vectors

No	Cause	Effect at military level	Effect at civilian level
1	Distinct performance requirement	Durability in extreme conditions (temperatures, shocks, vibrations), resistance to cyber attacks, operation without critical errors, maximum performance at any cost, specific stealth requirements, ballistic resistance, long system life.	Low costs, ease of use, aesthetics, energy efficiency, fast development speed, shorter product life cycle.
2	Different development cycles	Long development, testing and certification cycles (years, even decades), due to complexity and strict safety and reliability requirements.	Much shorter development cycles ("time-to-market" or time-to-market is essential), frequent releases of new versions/products.
3	Budgets and funding sources	Predominantly funded by governments, with often large budgets, but subject to slow and bureaucratic procurement processes.	Market-funded, private investors, with a strong focus on profitability and rapid adoption.
4	Regulations and standards	Subject to very strict regulations regarding national security, export (ITAR, Wassenaar Arrangement), specific operating environments (MIL-STD).	Subject to consumer safety regulations, data protection (GDPR), industrial standards (ISO), but much less restrictive than military ones.
5	Organizational culture	Military and Defense: Traditional, focused on reliability, secrecy, risk management.	Civil and Commercial: Innovative, fast, open to experimentation, information sharing, tolerance for early errors to accelerate learning.

2.4 Military vs. Civilian Regulatory Asymmetry – A Fundamental Cause of Separation

In recent decades, the innovation ecosystem has been marked by structural convergence and the intensification of bidirectional technology flows between the civilian and military sectors. Nevertheless, a pronounced gap persists at the level of regulation, standardization, and, most critically, cybersecurity.

Defense institutions operate under the imperative of national security, being guided by rigid normative frameworks such as restrictive public procurement systems, MIL-STD technical specifications, and strict export control regimes (such as ITAR in the United States or EU Regulation 2021/821). This structural bureaucracy generates substantial costs and operational delays absent from the commercial environment.

The asymmetry manifests itself most significantly in the area of cybersecurity requirements. The military environment requires resilience against advanced state-level cyberattacks, secure processing of classified data, and absolute availability in operational theaters.

The technical architecture imposes physical and logical isolation (air-gapping), high-security encryption, dedicated intrusion detection systems, and continuous auditing processes — elements that generate exponential costs.

The civilian sector operates according to a commercially optimized risk model focused on the protection of personal data (GDPR compliance), business continuity, and the prevention of financial fraud. In this environment, innovation is accelerated through the rapid adoption of emerging technologies (such as artificial intelligence) in the absence of unified cybersecurity standards.

Although legislative initiatives such as the Cyber Resilience Act (CRA) impose the principle of security-by-design for commercial digital products, their full mandatory implementation is scheduled for the second half of 2027.

In conclusion, this regulatory asymmetry directly influences the dynamics of technology transfer flows and generates significant challenges for both dimensions:

1. Civil-to-Military Transfer (Spin-in / COTS): The fundamental challenge consists in the necessity to adapt and militarize (hardening) commercial technologies in order to comply with rigid military standards of robustness, interoperability, and security.

2. Military-to-Civilian Transfer (Spin-off): This dimension faces severe barriers represented by strict secrecy regimes, prohibitively high initial R&D development costs, and the absence of an early-stage commercialization and validation strategy within the civilian market.

3. PROBLEM

The analysis presented in the previous chapter highlights the fact that the development of hybrid civilian-military technological chains capable of rapid scaling and operational interoperability remains obstructed by a profound structural gap and by the asymmetry of compliance criteria. The level of depth, cyber resilience, and technological robustness required to counter hybrid and military threats is rarely achieved or even necessary within the standard architecture of products developed in the commercial civilian ecosystem.

This security asymmetry is empirically confirmed by the operational data of the NATO DIANA (Defence Innovation Accelerator for the North Atlantic) program. Of the more than 2,600 proposals submitted by civilian companies for the 2025 cohort, a critically low rate of under 3% (73 companies) succeeded in advancing to Phase 1 (“Bootcamp”). Furthermore, the selection process narrowed dramatically in Phase 2 (“Scale”), where only 15 companies were promoted to the hybrid development phase and direct operational demonstrations in cooperation with military end-users.

In order to remedy this civilian-military compliance gap in an accelerated manner, the doctoral thesis proposes the design of a dynamic cybersecurity compliance auditing and adjustment algorithm. Within this framework, the present study identifies, ranks, and prioritizes the essential security requirements applicable to concrete dual-use projects of a classical, convergent, hybrid, and emerging nature.

4. RESEARCH METHODOLOGY

4.1 Research Objectives

General Objective:

Evaluating cybersecurity compliance challenges at the intersection of civilian and military ecosystems in order to establish the foundation for a dynamic auditing algorithm capable of optimizing the integration of technologies into hybrid dual-use technological chains.

Specific Objectives:

1. Identifying and mapping the points of structural divergence between civilian standards (NIS2 Directive, Cyber Resilience Act) and stringent military security requirements (CMMC 2.0, NATO standards);
2. Analyzing the success and failure metrics recorded within innovation accelerators through a case study centered on the NATO DIANA program;
3. Formalizing the logical rules and decision trees that will govern the integrated matrix of the dynamic auditing algorithm.

4.2 Research Hypotheses

Main Hypothesis: Prioritizing an integrated and dynamic approach to cybersecurity compliance substantially reduces the time interval and alignment costs for economic entities operating within hybrid civilian-military technological networks.

Secondary Hypothesis: Standardizing a model based on "control inheritance" between civilian-sector regulations and defense industry requirements increases the operational compatibility rate of deep-tech startups with NATO technical requirements.

4.3 Selected Research Methods

In order to validate the hypotheses and collect the data necessary for algorithm modeling, the scientific investigation employs a mixed and transdisciplinary approach based on the following methods:

Comparative Matrix Benchmarking Analysis: Used to juxtapose textual requirements from horizontal civilian regulations (Cyber Resilience Act - CRA) with those from restrictive defense frameworks (CMMC 2.0). The purpose is to isolate a Common Control Baseline aimed at eliminating redundancies in the auditing process.

Structural Documentary Analysis: Applied in the systematic examination of European directives regarding the digital transformation of defense, export control regulations for dual-use goods (EU Regulation 2021/821), and emerging artificial intelligence policies (EU AI Act).

Empirical Case Study Methodology: Applied to aggregated data from the operational cohorts of NATO DIANA (2025–2026). This method enables the isolation of technical and compliance-related causes generating the high rejection rates of commercial solutions within military selection processes.

Algorithmic Modeling and Graph-Based Logic Analysis: Used to translate legal and technical norms into dynamic logical structures. The method ensures the adaptive character of the algorithm, enabling it to adjust its set of questions according to the technological profile and hybridization level of the evaluated company.

Risk-Based and Dynamic Weighting Approach: Implemented in order to develop the algorithm's scoring model. This method guarantees that vulnerabilities identified within the critical supply chain receive a mathematically higher evaluation weight compared to purely administrative deviations.

Research Limitations: The principal limitation identified at this stage consists in the restricted access to classified or specially regulated defense-related data (military standards specific to certain NATO member states). The research operates exclusively with public data, open standards, and declassified reports issued by international organizations.

4.4 Data Collection Methodology

In order to ensure the validity, reliability, and applicability of the proposed auditing algorithm, the data collection process is structured across three complementary levels using the triangulation technique. This approach enables the correlated collection of both normative indicators (the legislative dimension) and empirical indicators (operational data from programs such as NATO DIANA).

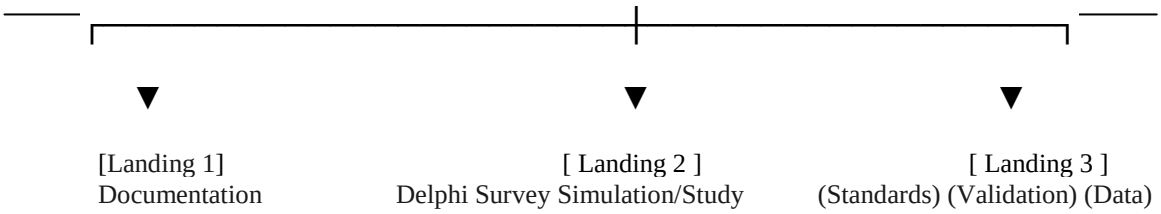

FIG.1 Data Triangulation

5. RESULTS

The study began in January 2026 and is currently in Tier 1 of the documentation phase, presenting several of the highlighted findings.

5.1 Dual-Use Paradigms and Specific Cybersecurity Requirements

5.1.1 Current Paradigms

According to the European Commission White Paper (2024) and the strategic reports of the NATO Parliamentary Assembly (Baldwin, 2024)

Table 2 - The focus of the cyber algorithm according to current dual-use paradigms

Dual-use paradigm	Description	Examples	Focus Argoritm cybersecurity
Spin-in/out Transfer	civilian - military military - civilian	Edge computing & Edge AI Defense-grade cyber operations platforms	The modifications needed to "militarize" a ready-made civilian product.
Hibrid (Convergent)	1. Interaction through Communication Interfaces (API-Driven / Data-Level Hybrid) Civilian and military products are separate, but connected through a continuous flow of data.	Interoperability A military command (C2) software takes in real-time data from civilian commercial satellites.	Interface Security (API Security) and the risk of malicious code injection into the military network.
	2. Interaction through Shared Infrastructure (Infrastructure-Level Hybrid) Civilian and military applications run simultaneously on the same physical infrastructure, but separated by logical walls.	The national 5G/6G network used by civilians, where a portion is isolated through network slicing for the military.	The resistance of virtual isolation to cross-tenant attacks (hackers jumping from civilian to military).
	3. Embedded / Co-Existence Interaction (Product-Level Hybrid) Entirely civilian hardware or software components are incorporated directly into complex military systems.	Using a civilian Linux operating system or commercial NVIDIA chips on a military radar.	Software Supply Chain / Bill of Materials (SBOM) vulnerabilities.
	4. Operational Interaction / Multi-User (User-Level Hybrid) The same digital platform is used simultaneously by civilian and military operators for different objectives.	Air or port traffic management system, used by civilian controllers and military officers.	Identity and access management based on strict Zero Trust policies.

Dual-use paradigm	Description	Examples	Focus Argoritm cybersecurity
Dual-Production / Industrial Surge Flexible Capacity is not about the product itself, but about the production line.	Civilian industrial infrastructures that can quickly switch production ("toggle") from commercial goods to military goods in the event of a crisis, without fundamentally changing technology.	an automobile factory switching to light armored vehicle production.	Here, the audit is not on the final product, but on the conversion capacity (Surge Capacity). The algorithm must check: "How quickly can this civilian factory become a secure military supplier and does it have protected digital plans (CAD files)?
Latent Dual-Use Inadvertent Dual-Use / Hidden Risk	Purely civilian technologies, developed without any military intent, but which have a hidden military potential or can be diverted (misused).	A biological synthesizer legitimately used for vaccines, but which can be reprogrammed to create pathogens. Or a hyper-realistic video game whose graphics engine is used by terrorist groups to simulate attacks (training).	This is the most dangerous category for compliance and export control. Here the algorithm works like an anomaly detector. The company doesn't know it has a problem. The algorithm has to scan the technical specifications and say, "Attention!
Co-Development / Deep Tech Integration Common Development from Scratch	Projects where the civil-military distinction is impossible because the technology is too early (TRL 1-3). Funding and research are shared in a mixed consortium (University + Army + Private Company).	Quantum computing or meta-materials. There is no "civilian quantum chip" vs. "military quantum chip" in the research phase; there is only quantum physics	The algorithm's challenge is managing intellectual property (IP) and access for foreign researchers. The algorithm must establish digital Chinese Walls within the same laboratory.

5.1.2. Emerging paradigms

In the cutting-edge literature and strategic reports (NATO / Chatham House 2026), 3 new emerging hybrid categories of dual-use technologies are already emerging

Table 3 - The focus of the cyber algorithm according to emerging dual-use paradigms

Dual-use paradigm	Description	Examples	Focus Argoritm cybersecurity
Cloud-Native Sovereign Dual-Use (Dual-Use Suveran in the Cloud)	In the future, we are talking about gigantic shared cloud infrastructures.	The same commercial cloud infrastructure (e.g. Microsoft Azure, Amazon AWS or sovereign European clouds) runs in separate enclaves civilian data (banks, hospitals) and operational military data.	This is a revolutionary category for the algorithm. It no longer audits a product, but audits the dynamic isolation of the cloud (Hypervisor & Tenant isolation). The algorithm will have to verify that the "logical walls" in the cloud are strong enough that a cyber attack on the civilian side cannot pass into the military enclave.

Dual-use paradigm	Description	Examples	Focus Argoritm cybersecurity
Algoritm-as-a-Service (GenAI / Foundation Models Dual-Use)	The emergence of Large Language Models (LLMs) and Artificial General Intelligence (AGI) creates a category where the basic mathematical model (the Foundation Model) is identical, but the usage differs by a simple prompt or API.	A civilian AI model trained to program software or analyze legal contracts can be instantly transformed, through a few specific commands (fine-tuning), into a tool that searches for vulnerabilities in enemy systems or writes malicious code.	In this future category, compliance can no longer be done at the source code level (because the model is huge and black-box). The dynamic algorithm will have to audit "guardrails" and prompt filters (Prompt Engineering Compliance) to prevent the civilian model from being hijacked for lethal purposes.
Open-Source Dual-Use Dual-Use through Open Ecosystems	The transition from private intellectual property to decentralized ecosystems (open-source software, open-weight AI models such as those from Meta).	The technology is no longer owned by a civilian company (as is the case with Transfer or Hybrid), but is available on public platforms (e.g. GitHub). The global civilian community improves it daily, and armies take it for free and integrate it into their combat systems (as is already happening with open-source drone navigation software).	The hardest to audit. The algorithm will have to assess the "hygiene of the open-source supply chain" (Software Supply Chain Security). It must verify that vulnerabilities have not been introduced into the open civilian code by hostile state actors (poisoning attacks), before the military downloads that software.

If we analyze the evolution from the five current paradigms (Transfer, Hybrid, Dual-Production, Latent, Co-Development) toward the three future paradigms (Sovereign Cloud, Algorithm-as-a-Service, Open-Source), the global actions undertaken during the last two years (2024–2026) have shifted radically from simple checklists toward dynamic governance mechanisms.

However, based on the analysis of concrete actions implemented within the EU–NATO area and the associated progress matrices, we observe that the majority of actions and results have been achieved within the Transfer Spin-in/out, Hybrid (Convergent), and Co-Development / Deep Tech Integration models.

5.2 Concrete Actions Implemented (2024–2026)

5.2.1 Standardization and Reciprocity of Controls (Regulatory Pillar)

Harmonization of the CRA (Cyber Resilience Act) with CMMC 2.0: The European Commission and the U.S. Department of Defense (DoD) established working groups within the framework of the Trade and Technology Council (TTC) for the automated mapping of compliance evidence. If a civilian startup complies with CRA requirements regarding vulnerability reporting and patch management, this data is automatically processed by GRC (Governance, Risk, and Compliance) algorithms in order to partially satisfy CMMC Level 2 requirements.

Introduction of the SBOM (Software Bill of Materials) as a Mandatory Standard: Both under the NIS2 Directive (fully entered into force) and within NATO military procurement processes, suppliers of hybrid or embedded dual-use technologies are required to provide a digital passport of components (SBOM). This enables the automatic scanning of vulnerabilities within civilian code prior to military integration.

Open-Source Standards and Modular Architectures: Military institutions are increasingly exploring and adopting modular design principles and open-source standards in order to reduce dependency on single vendors and facilitate the integration of new technologies.

Consensus on Regulatory Interoperability: Within the EU–U.S. Trade and Technology Council (TTC), working groups were initiated for the mutual recognition of certain security standards (for example in IoT and cryptography), thereby reducing the duplication of compliance efforts for transatlantic companies.

Update of Export Regulations (EU & U.S.): A distinct category for "cyber-surveillance items" (cyber surveillance and intrusion systems) was introduced, establishing strict rules intended to prevent their use in human rights violations. In addition, the European Commission published strict compliance guidelines for exporters.

Public-Private Partnerships (PPP): Governments collaborate with private companies in research and development projects. **Accelerated Procurement Systems:** Many governments have simplified and accelerated procurement processes for innovative technologies.

5.2.2 Secure Testing and Acceleration Infrastructures (Operational Pillar)

NATO DIANA Testing Centre Network (TEVV): More than 180 testing centers equipped with cyber ranges have become operational. Startups developing dual-use technologies can execute their civilian code within simulated environments replicating military-grade attacks (e.g., EW jamming, advanced state-sponsored cyberattacks).

Cross-Border Regulatory Sandboxes: The EU launched controlled testing environments in which companies developing dual-use AI solutions may experiment simultaneously with compliance under the EU AI Act and Export Control regulations, while receiving technical assistance from national cybersecurity agencies (such as the National Cyber Security Directorate – DNSC in Romania).

Defense-Level Innovation Units (e.g., DIU in the U.S., DASA in the UK): These are probably among the most visible and effective solutions. They act as intermediaries between the Pentagon/Ministries of Defense and Silicon Valley/startups through simplified procurement processes and dedicated investment funds.

Technology Exercises and Demonstrations: Joint exercises directly integrating emerging commercial technologies in order to test them under relevant operational conditions. Example: NATO exercises involving startups.

5.2.3 Compliance Automation (Compliance-as-Code)

Transition Toward Continuous Auditing: Major agencies (such as ENISA and NCIA) financed pilot projects aimed at transitioning from annual document-based audits toward automated scripting systems. These systems verify in real time whether the APIs and cloud infrastructures of hybrid projects comply with data isolation policies (Zero Trust architecture).

5.2.4 Hybrid Funding Programs

European Defence Fund (EDF) and NATO Initiatives (such as DIANA – Defence Innovation Accelerator for the North Atlantic): These programs finance civilian startups developing deep-tech solutions (AI, quantum security), requiring them from the design phase onward to comply with cybersecurity standards compatible with the military environment.

Defense Venture Capital Funds (e.g., NATO Innovation Fund): These funds invest directly in startups with dual-use potential in order to support the development of products capable of serving defense purposes.

Small Business Innovation Research (SBIR/STTR) Programs in the United States: These programs allocate part of federal R&D budgets to small businesses and startups for the development of innovative technologies, many of which possess strong dual-use potential.

5.3 Results Following Implementation

Progress Metrics: Data and Indicators

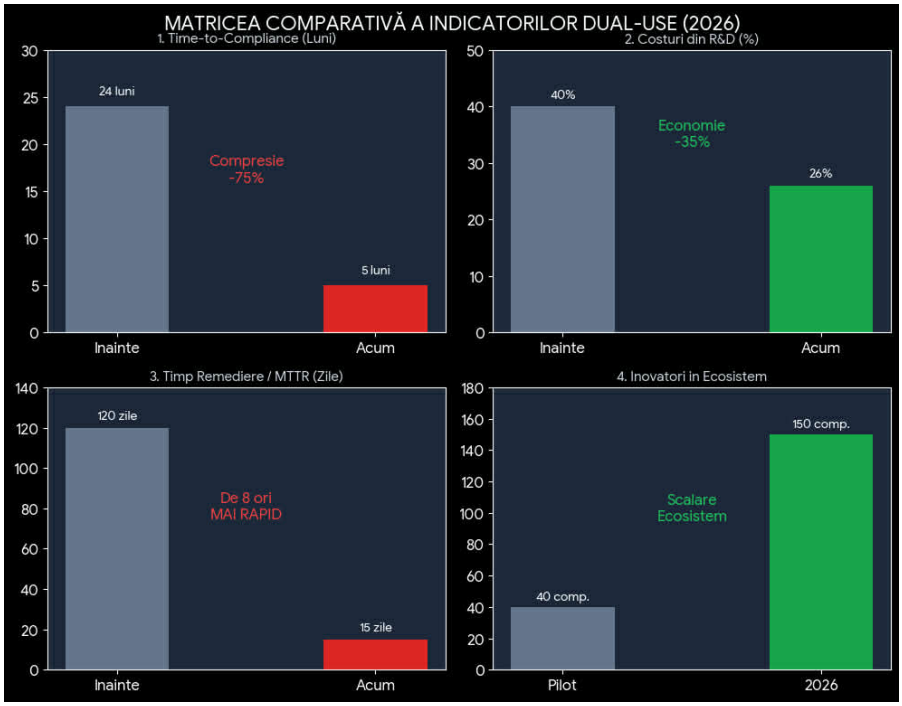

FIG.2 Correlated analysis of progress indicators in hybrid dual-use ecosystems.

Quadrant 1 & 3 (Risk/Time Contraction - Red): Highlights the reduction in compliance time from 24 to 5 months and the collapse of the mean time to remediate (MTTR) from 120 days to under 15 days.

Quadrant 2 & 4 (Efficiency and Scalability - Green): Illustrates the release of R&D budget previously absorbed by bureaucracy and the increase in the volume of companies attracted in Phase 2 to 150 innovative entities.

IBM, PwC and Research Gate reports report the following progress indicators in the area of dual-use, hubrid and emerging projects:

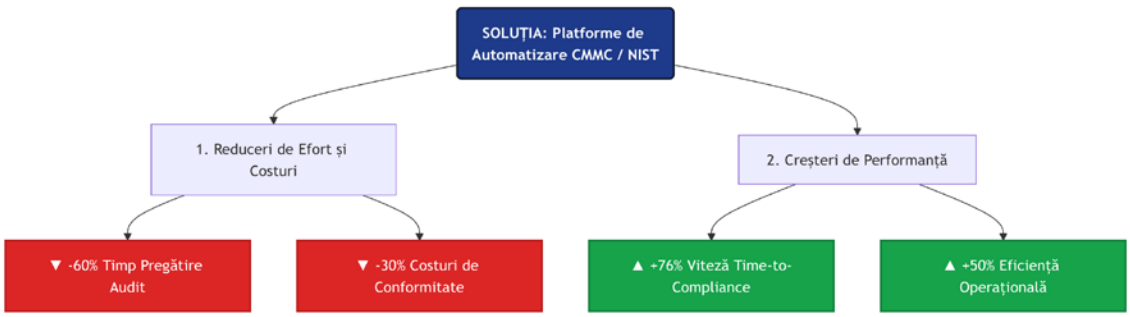

FIG.3 Binary matrix of efficiency in compliance automation (Source: PwC)

FIG.4 Time compression diagram of the initial audit in Cloud environments (Source: ResearchGate Data)

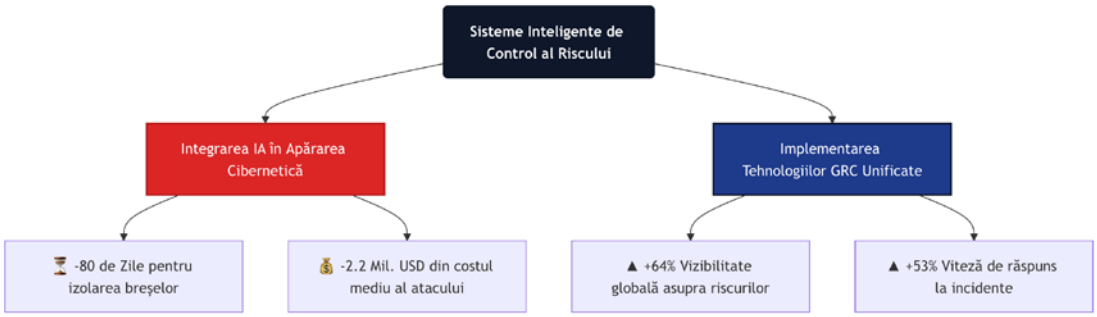

FIG.5 The correlated model of AI-based resilience and unified risk governance (Source: IBM Data)

6. DISCUSSIONS

In the effort to define a dynamic algorithm that is as efficient and useful as possible, after scanning dual-use models with cybersecurity requirements, implemented actions, and results already achieved in the process of harmonizing dual-use cybersecurity compliance, we also analyzed:

6.1 What Has Not Yet Been Implemented, but Could Be Considered?

For rapid (or even automated) transfer and integration in the future, the focus should be placed on:

Development of Common Interfaces and Open APIs: Military systems should be designed from the outset using modular architectures and open APIs, enabling any civilian developer to create applications or components that can be easily integrated while complying with strict security standards.

Impact: Just as a smartphone can run thousands of applications, a military system could rapidly integrate verified civilian solutions.

A "Dual-Use by Design" Culture: Research and development funding should require, whenever possible, the consideration of dual-use applications from the very beginning of any project, whether civilian or military.

Impact: This reduces subsequent adaptation efforts and stimulates innovation in a more sustainable manner.

Unification of Cybersecurity Standards: The development of tier-based cybersecurity standards recognized by both the civilian and military sectors. A technology certified at a certain security level would require only minor adaptation for higher-level use.

Impact: This would significantly simplify the validation and integration process, even though a "military-grade" level will always remain stricter.

Interdisciplinary Education and Training: University and specialization programs combining expertise in military and civilian engineering, addressing both design and operational perspectives.

Impact: This creates a workforce capable of understanding and navigating between the two worlds.

Flexible and Continuous Funding Mechanisms: Dedicated funds capable of rapidly financing the testing and scaling of dual-use technologies, with minimal bureaucracy and rapid review cycles.

Impact: This enables innovations to move quickly from the laboratory/startup phase to practical application.

Laws and Policies Encouraging Civil-Military Partnerships: Legislative frameworks simplifying intellectual property transfer, reducing legal risks for public-private partnerships, and stimulating investment in dual-use innovation.

Impact: This provides clarity and motivates companies to become involved. By implementing these measures, a closer symbiosis between civilian innovation and military needs can be achieved, transforming the current fragmentation into a rapid innovation cycle.

6.2 How Are All These Data and Information Integrated into the Foundation of the Algorithm?

For the auditing algorithm to be valid, it must integrate performance metrics extracted from these initiatives. Therefore, the algorithm will use these indicators as benchmarks throughout its development, testing, and implementation processes.

CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

The scientific investigation conducted within this work highlights that, in the current geopolitical and geoeconomic landscape of the European Union and the North Atlantic Alliance, dual-use technologies no longer represent a secondary option, but rather the fundamental axis of innovation and resilience in defense.

The historical fracture between the restrictive military ecosystem and the commercial civilian one—driven by asymmetries in costs, development cycles (time-to-market), and rigid national security standards (such as MIL-STD or export control regimes)—can no longer be managed through traditional, sequential technology transfer mechanisms (spin-in / spin-out).

The factual analysis demonstrates that prioritizing an integrated, dynamic, and convergent approach to cybersecurity compliance represents the optimal solution for overcoming this structural gap.

The current dynamics of cyber threats and the accelerated iteration rate of civilian algorithms (as observed in modern operational theaters) require a shift from static, document-based audits toward automated models of continuous risk assessment.

Tools such as the Cyber Resilience Act (CRA) in the civilian space and CMMC 2.0 in the defense sector highlight the need for a normative translator capable of unifying cross-sector requirements.

The academic and applied response to this structural challenge is materialized through the development of a dynamic cybersecurity auditing algorithm for dual-use SMEs and deep-tech startups, grounded within the doctoral thesis.

The empirical data analyzed indicate that the internalization of a framework based on the principle of “Control Inheritance” can generate a massive reduction of up to 75% in Time-to-Compliance, while also reducing by more than one third the financial barriers that hinder early-stage commercial innovation. Furthermore, through the use of Software Bill of Materials (SBOM), the algorithm directly optimizes the speed of vulnerability remediation (MTTR) within integrated hybrid systems.

In conclusion, securing and rapidly scaling dual-use technologies requires a reconfiguration of cybersecurity governance.

The algorithm under development provides an essential predictive and dynamic tool for enabling secure technological collaboration, directly contributing to the strengthening of technological sovereignty and the collective resilience of the Euro-Atlantic defense ecosystem.

ACKNOWLEDGMENT

The following contributors participated synergistically in the realization of this study:

1. **PhD Candidate Adriana NIȚESCU** | UPB - FAIMA
   - author of the doctoral thesis and of the dynamic dual-use compliance algorithm architecture dedicated to SMEs and deep-tech startups;
2. **Lecturer Dr. Tiberiu TĂNASE** | Secretary of DIS - CRIFST | Romanian Academy
   - a prominent figure who defined and articulated the evolution of dual-use technologies from a historical perspective;
3. **The Octogon Hub Team** | start-up business ecosystem
   - the entity that provided the empirical datasets and specific indicators from the startup and business innovation ecosystem.

The authors hereby declare that this paper represents an original research contribution, has not been previously published in any specialized journal or conference volume, and is not currently under review or peer evaluation in any other publication.

This material constitutes an intermediate and exploratory stage of research within the doctoral thesis, being submitted exclusively to the present military conference for evaluation and potential inclusion in its official proceedings volume.

REFERENCES

[1] J.A. Alic, L.M. Branscomb, H. Brooks, A.B. Carter & G.L. Epstein, *Beyond spinoff: Military and commercial technologies in a changing world.* Boston, MA: Harvard Business School Press, 1992;

[2] A.D. Little, *Unlocking the strategic power of dual-use technologies: Models and best practices for success*, Brussels, Belgium: Arthur D. Little Global Defense & Aerospace Practice, 2025;

[3] Aspen Digital, *A security symphony: Harmonizing global cybersecurity regulations*. Washington, D.C.: The Aspen Institute, 2024;

[4] M. Baldwin, *Dual-use technologies (Report 051 ESC*). Brussels, Belgium: NATO Parliamentary Assembly, Economics and Security Committee, 2024;

[5] E. Commission, *White paper on options for enhancing support for research and development involving technologies with dual-use potential. Brussels*, Belgium: European Commission, Directorate-General for Research and Innovation, 2024;

[6] M. Draghi, *The future of European competitiveness: A competitiveness strategy for the European Union*. Brussels, Belgium: European Commission Publications Office, 2024;

[7] European Parliament and Council of the European Union, *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.* Official Journal of the European Union, L 206, Luxembourg: Publications Office of the European Union, 2021;

[8] European Parliament and Council of the European Union, *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 (NIS2 Directive).* Official Journal of the European Union, L 333, Luxembourg: Publications Office of the European Union, 2021;

[9] European Parliament and Council of the European Union, *Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).* Official Journal of the European Union, Luxembourg: Publications Office of the European Union, 2024;

[10]IBM Security. (2024). *Cost of a data breach report 2024.* Cambridge, MA: IBM Corporation Security Division, International Journal of Information Technologies and Security. (2025). *The role of dual-use technologies in hybrid warfare*. IJITS Journal, 17(1), 105-118. Sofia, Bulgaria: Union of Scientists in Bulgaria;
[11]Joint Research Centre, *Strategic dependencies and dual-use technology supply chains in the European Union*. Seville, Spain: European Commission Joint Research Centre (JRC), 2024;
[12] J. Molas-Gallart, *Which dual-use? Framing the history of military-commercial technology transfer*. Research Policy, 26(3), 321-337, 1997;
[13] NATO, *Hybrid threats and hybrid warfare reference curriculum* (Volume I). Brussels, Belgium: NATO Academic Affairs / Defence Education Enhancement Programme (DEEP), 2024;
[14] NATO DIANA, *DIANA pilot challenge programmes: Sourcing future capabilities from dual-use innovators*. London, UK: NATO Defence Innovation Accelerator for the North Atlantic Operations Center, 2025;
[15] PricewaterhouseCoopers, *Global compliance insights: Transforming compliance from a cost center to a value driver*. New York, NY: PwC Global Risk & Regulatory Platform, 2025;
[16] ResearchGate, *Compliance as code: Automating compliance and continuous auditing in cloud systems*. Berlin, Germany: ResearchGate Engineering & Security Analytics Publishing, 2025;
[17] T. Tănase, *Inteligența artificială în securitatea digitală.* Arad, România: Editura Concordia, 2024;
[18]U.S. Department of Defense, *Cybersecurity maturity model certification (CMMC) 2.0: Program guidance and assessment frameworks.* Washington, D.C.: Office of the Under Secretary of Defense for Acquisition & Sustainment, 2024;
[19] Wassenaar Arrangement, *Guidelines & procedures, including the plenary agreements*. Vienna, Austria: Secretariat of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 2024.