Journal of Defense Resources Management

Vol. 17 Issue 1 (32)/ 2026

BRASOV - ROMANIA

Journal of Defense Resources Management (JoDRM) is currently indexed in the following prestigious international databases and catalogs:

- Ulrich's Global Serials Directory
- Publishers International Linking Association (CrossRef)
- Directory of Open Access Journals (DOAJ)
- EBSCO - International Security & Counter-Terrorism Reference Center
- ProQuest
- Central and Eastern European Online Library (C.E.E.O.L.)
- Cabell's Directory of Publishing Opportunities
- Cengage GALE
- ERIH PLUS (European Reference Index for the Humanities and Social Sciences)
- WORLDCAT
- Karlsruhe Virtual Catalog (KVK)
- Norwegian Register for Scientific Journals, Series and Publishers
- Sherpa Romeo

ISSN: 2068 - 9403; **eISSN**: 2247 - 6466

DOI: 10.64404/JoDRM

REGIONAL DEPARTMENT OF DEFENSE RESOURCES MANAGEMENT STUDIES

The Regional Department of Defense Resources Management Studies issues this journal twice a year. Its goal is to disseminate the results of the theoretical and practical research investigations undertaken by reputable professionals worldwide in the holistic field of Defense Resources Management.

Journal of Defense Resources Management (JoDRM) is currently indexed in the following prestigious international databases and catalogs: ***Ulrich's Global Serials Directory, Publishers International Linking Association (CrossRef), Directory of Open Access Journals (DOAJ), EBSCO - International Security & Counter-Terrorism Reference Center, ProQuest, Central and Eastern European Online Library, Cabell's Directory of Publishing Opportunities, Cengage GALE, ERIH PLUS (European Reference Index for the Humanities and Social Sciences), WORLDCAT, Karlsruhe Virtual Catalog (KVK), Norwegian Register for Scientific Journals, Series and Publishers*** and ***Sherpa Romeo.***

INTERNATIONAL ADVISORY BOARD

CONTACT
Address: 160 Mihai Viteazul Street, Bldg K, Brasov, 500183, Romania
Phone: (+40) 268.401.809
Fax: (+40) 268.401.802
Email: journal.dresmara@mapn.ro
Email_1: journalofdefense@yahoo.com

ISSN: 2068-9403; **eISSN:** 2247-6466

DOI: 10.64404/JoDRM

EDITING GUIDELINES FOR THE ARTICLES

The editing guidelines for the articles to be published in the journal are as follows:

- **Page setup**: top – 28mm, bottom – 28mm, inside – 21mm, outside – 24mm, header – 12,5mm, footer – 12,5mm, mirror margines activated;
    - paper format B5 176X250;
    - font: Times New Roman;
    - style: normal.
- **Paper title**: upper case, font size 14pt, bold, centred;
- **Author (s) name**:
    - first name, surname, font size 12pt, bold, centred;
    - two free spaces below the title of the paper.
- **Author's affiliation, city, country**:
    - one free space (12pt) below author's name, font 12pt, centered.
- **Abstract**:
    - one free space (12pt) below author's workplace name;
    - up to 150 words;
    - font size 11pt, Italic, justified, left-right alignment.
- **Key words**:
    - maximum 8;
    - one free space (12pt) below the abstract;
    - 11pt, italic, lef alignment, separated by comma.
- **Paper body**:
    - even number of pages (maximum 6; research papers may have more depending on topic comprehensiveness);
    - no free space between lines;
    - two free spaces below the key words (24 pt);
    - two columns, width: 60mm, spacing: 5mm;
    - font size 12pt, justify;
    - paper main parts: introduced by titles numbered with Arabic figures, upper case, font size 12pt, bold, centered. One free space (12pt) above the text and one free space (12pt) below it;
    - paragraph indentation: 6mm;
    - quotations of more than two lines should be indented in a separate paragraph;
    - authors should organize the article into sections and also include sub-headings where appropriate.
- **Drawings, diagrams and charts**:
    - one free space (12pt) below the text;
    - width similar to that of the column they belong to. Should this be impossible to achieve, then they will be printed across the whole breadth of the page either at the top or the bottom of the page;
    - numbered in Arabic figures;
    - accompanied by captions, one free space (12pt) below the drawings, centered, font size 12pt;

- font size 12pt, justify;
- mathematical formulae: 6mm left alignment; ordinal numbers: in round brackets, right alignment; Times New Roman;
- Full - 12pt.; Subscript / Superscript - 9pt.; Sub-Subscript / Superscript - 7pt.; Symbol - 16pt.; Sub-Symbol - 12pt;
- Long mathematical formulae: not wider than the column or displayed on the whole width of the page either at the top or bottom of the page.

- **Names of organizations:** printed in Upper case, straight.
- **Names of military technology products**: in Upper case, Italic.
- **Essential notes**:
  - indicated by superscript numbers in the text;
  - presented at the end of the text but before the references.
- **Reference citations in the text**:
  - in round brackets;
  - author: year (e.g. Smith:1995) OR if quote provided: author: year, page no. (e.g. Smith:1995, p.45);
  - "et al." mentioned when citing a work by more than two authors. For example: Brown et al. (1981) or (Brown et al., 1981).
  - Use letters (e.g. a, b, c, etc.) to distinguish citations of different works by the same author in the same year. For example: Brown (1975a, b).
- **References**:
  - listed in alphabetical order, at the end of the article;
  - numbered in Arabic figures;
  - the titles of the reference books will be printed in Italic.

The authors take full responsibility for the contents and scientific correctness of the paper.

Journal website: https://www.jodrm.eu

PRINTED AT THE MILITARY TECHNICAL PUBLISHING CENTER

CONTENTS

CYBER KEY TERRAIN: A CROSS-LEVEL RECONCILIATION FOR TACTICAL, OPERATIONAL, AND STRATEGIC CYBERSPACE OPERATIONS.....9
Cezar VASILESCU

AI-DRIVEN CYBER CAPABILITIES IN DEFENSE RESOURCE PLANNING 41
Levan KALATOZISHVILI

ARTIFICIAL INTELLIGENCE: IMPLICATIONS ON MILITARY DECISION MAKING 63
Florin OGÎGĂU-NEAMȚIU

ETHICAL FADING AS SYSTEMIC VULNERABILITY: FROM THEORETICAL REVIEW TO A MULTI-LEVEL DIAGNOSTIC FRAMEWORK FOR MORAL EROSION IN COMPLEX ORGANIZATIONS.....89
Aura CODREANU

COGNITIVE WARFARE AND ITS SOCIETAL IMPACT: MANIPULATION, TRUST AND DEMOCRATIC RESILIENCE.....117
Brînduşa Maria POPA

THE LANGUAGE OF UNCERTAINTY: THE ROLE OF THE ACRONYMS VUCA, BANI, TUNA AND RUPT IN DESCRIBING THE CONTEMPORARY GEOPOLITICAL CONTEXT.....133
Svetlana CEBOTARI, Ion GUȚU

INTERPERSONAL CONFLICT AND PSYCHOLOGICAL TRAUMA: IMPLICATIONS FOR CONFLICT MANAGEMENT AND TRAUMA-INFORMED INTERVENTIONS.....147
Laurentiu BARCAN, Bianca Elena ILIESCU

NATO IN TRANSITION: MILITARY STRENGTH IN THE CONTEXT OF MODERN WARFARE 161
Khayal ISKANDAROV, Piotr GAWLICZEK

SAFE AND THE EUROPEAN STRATEGIC AUTONOMY: FROM COORDINATION TO CAPABILITY DELIVERY 181
Maria CONSTANTINESCU

OPERATIONS MANAGEMENT ANALYSIS FOR OPTIMIZATION OF SMITH & WESSON 17 PISTOL PRODUCTION.....207
E.S. ALIM, I NENGAH PUTRA, G.R. DEKSINO, K. GUNAWAN, A.K. SUSILO

ENVIRONMENTAL IMPACT OF DIGITALIZATION ACROSS EUROPEAN COUNTRIES: A COMPARATIVE STATISTICAL ANALYSIS 229
Cristina ANTONOAIE

HEALTHCARE MANAGEMENT IN CONFLICT SETTINGS: THE CRITICAL ROLE OF MEDICAL LABORATORIES AND BIOSAFETY 245
Mihaela BARCAN

INTEGRATED DIDACTIC DESIGN MODEL FOR ENGINEER OFFICERS' TRAINING: INSIGHTS FROM INTERNATIONAL EXPERIENCE ……259
Amil DADASHOV

CIANGSANA WAREHOUSE EXPLOSION: CHEMICAL DEGRADATION AND ZONING COMPLIANCE ANALYSIS ……277
Anisa SETIANINGSIH, Heri Budi WIBOWO, Mas Ayu Elita HAFIZAH

LEVERAGING FISHERS TRADITIONAL ECOLOGICAL KNOWLEDGE (TEK) FOR TECHNOLOGICAL DEVELOPMENT IN LAKE CHAD BASIN, NIGERIA, PRIVATE – PUBLIC PARTNERSHIP APPROACH ……297
Babagana ZANNA

CYBER KEY TERRAIN: A CROSS-LEVEL RECONCILIATION FOR TACTICAL, OPERATIONAL, AND STRATEGIC CYBERSPACE OPERATIONS

Cezar VASILESCU[1]

Regional Department of Defense Resources Management Studies (DRESMARA) / „Carol I“ National Defense University, Brasov, Romania

The concept of cyber key terrain has emerged as a critical yet poorly defined element of military cyberspace operations. While the traditional military concept of key terrain translates well to the physical infrastructure of cyberspace, its application to virtual layers remains problematic. This paper identifies and analyses what we could call as the "cyber key terrain paradox": the concept demonstrates clear tactical utility when applied to physical network elements, but loses coherence and applicability at operational and strategic levels, where logical networks, cyber-persona dimensions, and cognitive layers become dominant. NATO's current promulgated doctrine, AJP-3.20 Edition A Version 1 (2020), adopts a three-layer model of cyberspace (physical, logical, and cyber-persona), while academic and doctrinal proposals have progressively expanded this to five, seven, and eight layers encompassing cognitive and social dimensions.

This proliferation of models intensifies rather than resolves the paradox, as no existing framework provides systematic terrain identification methodologies for the higher layers. Through systematic analysis of military doctrine and academic literature, this study reveals fundamental inconsistencies between narrow, physical-centric definitions of cyber key terrain and the broader, multi-layered character of cyberspace as a domain of conflict. The paper proposes a reconciliation framework comprising layer-specific adaptive definitions, a temporal classification system, and a structured identification methodology, preserving the concept's tactical utility while providing the doctrinal coherence that operational and strategic planning requires.

Key words: *cyber key terrain, cyberspace operations, military doctrine, cyberspace layers, operational levels.*

[1]ORCID ID: 0000-0002-5280-8795, e-mail: cvasilescu1@mapn.ro

1. INTRODUCTION

1.1. Cyberspace as the Fifth Military Domain

The recognition of cyberspace as the fifth military domain (alongside land, sea, air, and space) represents a fundamental shift in how modern militaries conceptualize conflict. This designation acknowledges that military operations increasingly depend on, occur within, and can be decisively influenced by activities in cyberspace. Unlike traditional physical domains defined by fixed geographic coordinates and tangible geography, cyberspace is simultaneously *physical* (hardware, cables, and electromagnetic signals) and *virtual* (software, data, protocols, personas); it is human-constructed however operates according to technical rather than natural laws; and it changes at speeds unprecedented in military history.

NATO's promulgated doctrine on cyberspace operations, AJP-3.20 Edition A Version 1 (NATO Standardization Office 2020), defines cyberspace as *"The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data"* (para. 1.13). The publication adopts a three-layer model (physical, logical, and cyber-persona) (paras. 1.9-1.12), and situates cyberspace operations within a broader Information Environment (IE) that *"comprises the information itself, the individuals, organizations and systems that receive, process and convey the information, as well as the cognitive, virtual and physical space in which this occurs"* (para. 1.3). This IE formulation implicitly acknowledges dimensions beyond the three-layer cyberspace model, including cognitive and social spaces, but does not integrate them into the formal domain structure. Meanwhile, academic and doctrinal proposals have progressively expanded cyberspace models:

- five planes encompassing geographic and supervisory layers (Raymond et al. 2014);
- five planes adding cognitive and socio-organizational dimensions (Grant 2014); and
- eight-layer model (geographic, physical, infrastructure, syntactic, semantic, services, persona, plus a mission layer) that explicitly incorporates human elements and geographic context and is the most comprehensive update to date (Venables 2021).

These expanded models underscore the multi-dimensional character of the space in which military operations must increasingly be planned and conducted.

1.2. The Cyber Key Terrain Paradox

This paper identifies the concept of *"cyber key terrain paradox"*: the concept of cyber key terrain demonstrates clear utility and relatively consistent application at tactical levels when focused on physical network infrastructure, however it becomes increasingly ambiguous, contested, and potentially inapplicable at operational and strategic levels where virtual and cognitive dimensions of cyberspace become dominant.

The management of physical cyberspace infrastructure as critical infrastructure presents distinct challenges that require specialized competencies and frameworks, as the physical layer forms the foundation upon which all other cyberspace operations depend (Codreanu 2020).

AJP-3.20(NATO Standardization Office 2020) does not define cyber key terrain as a formal term. The closest NATO doctrinal treatment remains the traditional key terrain definition from JP 2-01.3: *"Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant"* (Joint Chiefs of Staff 2009). Academic literature has adapted this concept to cyberspace: cyber terrain is defined as encompassing systems, devices, protocols, data, software, processes, cyber personas, and other networked entities (Raymond et al. 2014) or cyber key terrain defined as *"physical and logical elements of the domain that enable mission essential warfighting functions"*. (Bodeau et al. 2013)

The absence of a formal NATO-agreed cyber key terrain definition in AJP-3.20 is itself significant: it suggests that the Alliance has not yet resolved how to translate terrain concepts into the multi-dimensional cyberspace domain, a gap that becomes more acute as expanded layer models gain attention.

At the tactical level, identifying cyber key terrain appears manageable: critical routers, network nodes, servers, and communications links can be mapped, prioritized, and defended. At strategic levels, however, this clarity disappear. AJP-3.20's three-layer model already introduces challenges at the cyber-persona layer, where virtual identities lack the physical properties that terrain concepts assume (para. 1.12). When academic models expand the domain to include cognitive, social, and semantic layers, the terrain concept loses further coherence.

If strategic operations occur across multiple layers, but key terrain is defined mainly for the physical and lower virtual dimensions, how can the concept relate with strategic planning? This inconsistency represents the ***main research question*** this paper addresses.

1.3. Research Objectives

The research is guided by three interconnected **Research Objectives (RObj)**, as follows:

- **$RObj_1$** - systematically document the cyber key terrain paradox through analysis of military doctrine, including NATO's promulgated AJP-3.20, expanded academic cyberspace models and academic literature;
- **$RObj_2$** - analyze the sources and implications of definitional inconsistencies across tactical, operational, and strategic levels;
- **$RObj_3$** - evaluate whether the concept of key terrain can be meaningfully extended to the virtual and cognitive layers of cyberspace; and
- **$RObj_4$** - propose a reconciliation framework that preserves tactical utility while addressing operational and strategic requirements.

The hypothesis guiding the study is that the paradox is structural (the result of applying physical terrain concepts to a multi-dimensional domain) and that expanded cyberspace models proposed in academic literature make the paradox more rather than less acute, a problem compounded by the absence of terrain identification frameworks in NATO's current promulgated doctrine.

2. METHODOLOGY

The study employs a qualitative doctrinal analysis methodology, systematically examining primary military doctrine and secondary academic literature to identify definitional inconsistencies, conceptual gaps, and cross-level incompatibilities in the cyber key terrain concept. The primary source base comprises joint and service-level doctrinal publication: JP 2-01.3, JP 3-12 in its 2018 and 2022 revisions, Air Force Doctrine Publication 3-12, and NATO AJP-3.20 Edition A Version 1 (2020), together with U.S. and NATO strategic documents including the 2023 DoD Cyber Strategy.

The secondary source base comprises peer-reviewed and conference publications from 2001 to 2023 identified through targeted review of the cyber terrain and cyberspace geography literature, following the framework established for distinguishing between the two fields (Grandin 2023). The analysis of expanded cyberspace models draws particularly on Venables (2021), whose eight-layer model represents the most comprehensive academic treatment of cyberspace composition currently available in peer-reviewed literature.

The analytical approach proceeds in three stages:

1. First, doctrinal definitions of cyberspace and cyber key terrain are compared across documents to identify structural inconsistencies, with particular attention to the progressive expansion of cyberspace layer models across joint, NATO, and academic sources.
2. Second, the concept's applicability is assessed at each operational level (tactical, operational, and strategic) against four criteria: *physicality* (the element have a stable, bounded existence), *controllability* (it can be seized, held, or denied), *temporal stability* (it is stable enough to support planning), and *scalability* (concept remain coherent as operational scope expands).
3. Third, the reconciliation framework is developed inductively from the identified gaps, drawing on conceptual frameworks from cyberspace geography (Dodge and Kitchin 2001; Gao et al. 2019; Lü, Yuan, and Yu 2021), graph theory, and social network analysis as sources for alternative models at virtual and cognitive layers. The method follows the doctrinal concept development approach (Raymond et al. 2014; Huntley 2016).

3. RESULTS

3.1. Literature Review: Development of the Cyber Key Terrain Concept

3.1.1. Historical Development of Key Terrain in Physical Domains

The concept of key terrain has deep roots in military thinking. Clausewitz emphasized the importance of geographic position in warfare, and subsequent Western doctrine formalized the idea that certain localities provide decisive advantage. Current U.S. joint doctrine (JP 2-01.3) maintains the same definition (Joint Chiefs of Staff 2009), emphasizing three characteristics: physicality (a locality or area), control (seizure or retention), and advantage (marked benefit to military operations).

Critically, traditional key terrain concepts assume several conditions that may not hold in cyberspace: terrain is relatively static between engagements; terrain can be physically occupied and denied to adversaries; terrain exists independent of human construction; and terrain advantage is primarily spatial and observable. These assumptions guide how militaries identify, seize, and defend key terrain in physical domains. Each is challenged to varying degrees in cyberspace, and each challenge intensifies as operations move from physical toward virtual and cognitive layers.

3.1.2. Evolution of Cyber Terrain Concepts (1998 - Present)

Early applications of terrain concepts to cyberspace focused on network topology and computer network defense. One of the first systematic treatments argued that *"computer networks are spatial simply because they exist in the physical world"*, emphasizing defensive perimeters in direct analogy to city walls and firewalls (Pingel 2003). This physical-centric approach established a pattern that persists in much subsequent work. The concept was further advanced by identifying eight "earthly manifestations" of cyber key terrain, including data centers, Internet service providers, undersea cables, and supply chains (Mills 2012). While the first five are primarily physical, the latter three (international standards bodies, cyber workforce, and innovation) represent intangible strategic factors whose inclusion raises fundamental questions about conceptual boundaries.

The most comprehensive tactical-level treatment developed methodologies for 'mapping the cyber terrain' using the definition already noted above (Bodeau et al. 2013). The most expansive pre-2020 conceptualization proposed a five-layer model encompassing geographic, physical, logical, cyber-persona, and supervisory planes (Raymond et al. 2014). The 2022 revision of JP 3-12 marked significant doctrinal evolution by officially defining expeditionary cyberspace operations as requiring deployment of cyber forces within physical domains (Joint Chiefs of Staff 2022). The most detailed academic decomposition of the cyberspace environment currently available in peer-reviewed literature proposes the eight-layer model noted in the introduction, developed at Tallinn University of Technology, providing a useful benchmark against which to assess the adequacy of doctrinal models (Venables 2021). Australian defense analysis has independently identified the proliferation problem, observing that publicly available allied strategic documents contain no fewer than eight domain models, inconsistent both between and within national doctrines (Wardrop, C. 2020). This confirms that layer proliferation is not merely an academic concern but an operational impediment recognized across allied forces.

3.1.3. Cyberspace Geography and Mapping

Parallel to military developments, academic geographers developed the field of Cyberspace Geography. The foundational work *Mapping Cyberspace* recognized that cyberspace encompasses more than infrastructure, including the spaces created by networked human

interaction (Dodge and Kitchin 2001). A systematic analysis of the terminology observed that the challenge of defining cyber terrain, cyberspace, and the differences between them remains unresolved, with different sources providing incompatible definitions (Grandin 2023). Chinese learning has advanced the concept of *Cyberspace Surveying and Mapping*. Chinese scholarship has advanced two complementary frameworks: a three-domain model of physical, logical, and cognitive levels (Xu et al. 2019), and the "ternary world" framework that positions cyberspace as the connective layer between physical and socio-human worlds (Gao et al. 2019; Lü, Yuan, and Yu 2021). Both align with AJP-3.20's acknowledgement that the information environment encompasses cognitive, virtual, and physical spaces (para. 1.3), while resisting reduction to physical-layer terrain metaphors.

3.1.4. Gaps in Current Conceptualizations

Multiple authors identify significant gaps in cyber terrain conceptualization. Attention to cyber key terrain has been confined primarily to the physical network layer, and the concept applied to cyberspace is considered "necessarily metaphorical" (Huntley 2016). He concludes that the metaphorical quality creates problems at strategic levels, where properties of the source domain (physical terrain) no longer align with properties of the target domain (virtual cyberspace). The concept is primarily linked to mission requirements, making it fundamentally ephemeral and resistant to strategic generalization (Bertoli and Raio 2018), while the temporal dimension has been identified as remarkably underexplored in the literature (Grandin 2023). Significantly, AJP-3.20 (NATO Standardization Office 2020) provides no formal framework for identifying cyber key terrain at any layer, nor does it address the temporal instability of the domain beyond noting that cyberspace is *"in constant flux"* (para. 1.8). This absence in NATO's promulgated doctrine contrasts with the growing academic consensus that expanded cyberspace models require correspondingly expanded terrain identification methodologies.

3.1.5. Non-NATO Doctrinal Perspectives

An assessment of the cyber key terrain concept would be incomplete without acknowledging how non-NATO military powers conceptualize the operational domain in which terrain identification takes place. Two perspectives are particularly instructive: Chinese *information warfare doctrine* and Russian *information confrontation theory*.

Both converge on a conclusion that reinforces the central argument of this paper: that physical-layer terrain thinking is insufficient for operations in the full cognitive and informational scope of modern conflict.

Chinese military doctrine has progressively developed the concept of *"information warfare"* (xinxi hua zhanzheng), which treats information space as a unified operational domain in which technical, cognitive, and psychological dimensions are inseparable (Ye Zheng 2013). The People's Liberation Army (PLA) doctrine of integrated network-electronic warfare combines cyberspace operations with electromagnetic spectrum control and cognitive influence within a single operational concept, explicitly rejecting the separation of technical infrastructure from the informational and psychological effects it enables.

This integration makes physical-layer terrain identification frameworks not merely insufficient, but conceptually incompatible with PLA operational thinking at the strategic level, where the decisive contest is understood to occur in the cognitive dimension. The Chinese academic scholarship on cyberspace geography noted in section 3.1.3, particularly the three-fold world framework (Gao et al. 2019; Lü, Yuan, and Yu 2021) reflects this doctrinal orientation, positioning cyberspace as a connective layer between physical and socio-human worlds rather than as a technical infrastructure amenable to terrain-style mapping.

Russian military theory employs the concept of *"information confrontation"* (informatsionnoe protivoborstvo), which explicitly integrates technical, cognitive, and psychological dimensions into a single operational space (Thomas 2004; Giles 2016). Russian doctrine distinguishes between the technical-informational dimension (focused on data and network infrastructure) and the psychological-informational dimension (focused on perception, decision-making, and morale), treating both as equally legitimate and inseparable theatres of operation.

This two-dimensional framework predates and in some respects anticipates the multi-layer academic models discussed in section 3.1.2, but arrives at an operationally integrated conclusion that NATO doctrine has not yet matched: that operations in the psychological dimension require fundamentally different conceptual tools from those used for technical network operations. From the perspective of the cyber key terrain paradox, Russian information confrontation doctrine effectively dissolves the paradox by abandoning terrain language altogether for the psychological dimension, replacing it with influence-based operational concepts that have no terrain analogue.

These non-NATO perspectives do not resolve the doctrinal challenges identified in this paper, but they confirm that the inadequacy of physical-layer terrain frameworks for higher-layer operations is recognized beyond the Alliance. They also suggest that the reconciliation framework proposed in section 3.4 (which acknowledges the metaphorical limitations of terrain language at cognitive and social dimensions and introduces alternative conceptual models for those layers) is directionally consistent with the operational thinking of peer competitors, even if the specific frameworks differ.

The extent to which the cyber key terrain paradox manifests differently within Chinese and Russian doctrine, and the implications for allied planning in contested information environments, represent important directions for future research beyond the scope of this study.

3.2. The Cyber Key Terrain Paradox: Sources and Structure

3.2.1. Definitional Inconsistency across Doctrinal Documents

The paradox emerges clearly from a comparison of doctrinal definitions. Cyberspace itself is consistently defined as multi-dimensional across all major documents:

- three layers: physical network, logical network, and cyber-persona (JP 3-12 2018, 2022);
- three-layer model: physical, logical, and cyber-persona (AJP-3.20 paras. 1.9-1.12 - NATO Standardization Office 2020);
- five planes (Raymond et al. 2013;
- five layers including cognitive and socio-organizational dimensions (Grant 2014) and
- the most detailed model with eight layers (Venables 2021).

Each model assigns substantial weight to virtual and human elements.

Cyber key terrain, by contrast, is defined across all documents with a predominantly physical emphasis. No NATO-agreed definition of cyber key terrain exists in the current promulgated doctrine. The academic definitions, from "physical and logical elements" (Bodeau et al. 2013) to broader treatment (Raymond et al. 2014) are formally applicable to multiple layers, but practical identification methodologies focus overwhelmingly on the physical and lower logical layers.

AJP-3.20's three-layer model already introduces a structural inconsistency: the cyber-persona layer is formally part of the domain, but the publication provides no framework for identifying terrain at that layer. The information environment concept (para. 1.3), which encompasses cognitive,

virtual, and physical space extends the operational scope further, but again provides no terrain identification methodology. This creates a gap between the recognized scope of cyberspace operations and the conceptual tools available for planning them, a gap that widens as academic models expand the layer count.

Table 1 summarizes the cyberspace layer models examined in this study, illustrating the progressive expansion from the three-layer framework of JP 3-12 and AJP-3.20 to the eight-layer model proposed by Venables (2021).

3.2.2. The Layer Problem

The proliferation of cyberspace layer models compounds definitional challenges. JP 3-12 and AJP-3.20 divides cyberspace into physical network, logical network, and cyber-persona layers. Raymond et al. (2014) and Grant (2014) add geographic or supervisory/ cognitive planes. Venables (2021) explicitly incorporate geographic, infrastructure, syntactic, semantic, and services dimensions alongside the persona layer, and notes that *"it is vital that there is a comprehensive understanding of the properties of the seven layers of cyberspace, the users active in it, and their mission."* This proliferation is not confined to NATO-level doctrine.

Table 1. Comparison of Cyberspace Layer Models in Military Doctrine and Academic Literature.

Source	Year	No. of Layers	Layer Names	Cognitive / Social included
JP 3-12 / AJP-3.20	2018-2022 / 2020	3	Physical network; Logical network; Cyber-persona	**No** (acknowledged in IE concept only)
Raymond et al.	2014	5	Geographic; Physical; Logical; Cyber-persona; Supervisory	**Partial** (supervisory layer)
Grant	2014	5	Physical; Logical; Cyber-persona; Cognitive; Socio-organizational	**Yes**

Source	Year	No. of Layers	Layer Names	Cognitive / Social included
Venables	2021	8	Geographic; Physical; Infrastructure; Syntactic; Semantic; Services; Persona; Mission	**Yes** (persona, semantic, mission layers)

Source: Author

National approaches add further variation: the UK's JDN 1/18 on Cyber and Electromagnetic Activities (CEMA) frames cyberspace within the broader electromagnetic environment, emphasizing the convergence of cyber and electromagnetic activities as an integrated operational challenge (UK Ministry of Defence 2018). Australia's ADF-C-0 defines the cyber domain as comprising *"cyberspace and the electromagnetic spectrum"* and has established separate career tracks for cognitive and information warfare distinct from cyber operations (Australian Department of Defence 2024). Germany's Bundeswehr elevated its Cyber and Information Domain Service (Cyber- und Informationsraum, CIR) to a full military service branch in 2024, explicitly combining cyberspace with the broader information domain.

Each national approach implicitly acknowledges that the technical three-layer model of cyberspace is insufficient for operational purposes, yet each extends it in a different direction: the UK toward electromagnetic convergence, Australia toward cognitive warfare, Germany toward information space integration, further complicating the interoperability challenge.

For cyber key terrain conceptualization, this expanding proliferation of layer models intensifies the existing problem. If different documents disagree on whether cyberspace has three, five, or eight layers, no systematic determination of what constitutes key terrain at each layer is possible across the Alliance. AJP-3.20's three-layer model does not resolve the conceptual gap; rather, the academic literature demonstrates that adding cognitive, social, and semantic layers (as the expanded models do) widens it, because these layers have no established key terrain identification methodology of any kind.

The confusion may partly explain why most practical discussions continue to retreat to

the physical dimension, where consensus is easiest: everyone agrees routers, cables, and servers are part of cyberspace, even if they disagree about how to treat influence networks or cognitive manipulation as terrain.

3.2.3. Temporal Dimensions and Dynamic Terrain

A crucial but underdeveloped dimension of the cyber key terrain paradox concerns *temporality*. Traditional terrain is relatively static, hills do not move between battles, and rivers follow predictable courses. Cyberspace changes continuously at multiple timescales. Grandin (2023) identifies this gap explicitly, noting that *"it is remarkable how little the temporal aspect of cyberspace, and how time affects the different levels or planes, is covered in research."* AJP-3.20 acknowledges that cyberspace is *"in constant flux"* (para. 1.8), but provides no systematic framework for addressing temporal instability in operational planning.

The temporal challenge manifests differently across layers. Physical infrastructure elements (the focus of AJP-3.20's physical layer) change over months or years, while logical layer elements (operating systems, protocols, applications - para. 1.11) change more rapidly. The cyber-persona layer (para. 1.12) is still more volatile: virtual identities can be created, modified, or abandoned in hours.

The cognitive and social dimensions identified by Grant (2014) and Venables (2021) operate at even higher tempos: influence campaigns shift over days, and cognitive states change in response to operational information pressure. Cyber key terrain is temporally linked to specific missions even at the tactical level: what is key for one operation may be irrelevant for the next (Bertoli and Raio 2018; Franz 2012). The multi-timescale instability means that temporal classification cannot be uniform across layers, and doctrine must explicitly account for the different reassessment cycles each dimension requires.

3.3. Cross-Level Assessment

3.3.1. Tactical Level: Where the Concept Works

At the tactical level, focused on specific missions and near-term objectives, the cyber key terrain concept demonstrates its greatest utility and consistency. Even without a formal NATO-agreed definition, the concept operates effectively when applied to physical and lower logical layer elements. The approach described in the academic literature (a systematic inventory of mission-

relevant cyber assets, identification of critical nodes, and prioritization for defensive effort (Bodeau, Graubart, and Heinbockel 2013; Guion and Reith 2017; Price et al. 2017) provides a structured, mission-focused methodology that tactical commanders can apply within the AJP-3.20 framework of defensive and offensive cyberspace operations (paras. 2.19–2.24).

Tactical applications concentrate on mission-specific network defense and attack operations where physical and lower virtual layer elements dominate. Jakobson (2011) provides a representative model with hardware, software, and service sub-terrains, each inventoried and assessed for criticality. Guion and Reith (2017) developed tools for tactical cyber terrain mission mapping using subject matter expert evaluation. Price et al. (2017) demonstrate the approach in mission reconfigurable cyber systems. Youn et al. (2021) extend this line of work by applying BGP archive data to Cyber Intelligence Preparation of the Battlefield (IPB), producing network-based situational awareness visualizations that support key terrain identification at the tactical level.

The physical layer emphasis at tactical level succeeds because it aligns with four operational factors: *immediacy* (physical infrastructure directly enables or prevents mission execution); *observability* (physical elements can be discovered and monitored); *controllability* (physical assets can be defended, secured, or destroyed); and *predictability* (physical elements behave according to known technical parameters).

The effective management of these physical infrastructure elements requires specialized competencies in critical infrastructure governance, as cyber infrastructure systems demand mature management frameworks that address technical, organizational, and strategic dimensions simultaneously (Codreanu 2020).

Table 2 applies the four analytical criteria established in the Methodology to each operational level, making visible the structural degradation of the terrain metaphor as the scope of operations expands.

3.3.2. Operational Level: Where Complexity Begins

At the operational level (concerned with campaigns rather than discrete missions) cyber key terrain identification becomes significantly more complex. The timeframe extends from hours or days to weeks or months; the scope encompasses entire theatre-level networks; and the terrain must support multiple missions with potentially conflicting requirements.

Table 2. Cross-Level Assessment of the Cyber Key Terrain Concept against Four Criteria.

Operational Level	Physicality	Controllability	Temporal Stability	Scalability
Tactical	**High** (physical infrastructure directly enables mission execution)	**High** (assets can be defended, secured, or destroyed)	**Adequate** (physical elements change over months/years)	**Limited to mission scope**; SME evaluation works at this scale
Operational	**Moderate** (logical and persona layers become relevant across campaigns)	**Partial** (logical elements controllable; persona layer less so)	**Reduced** (logical layer changes faster; update cycles conflict)	**Strained** (SME methodology does not scale to theatre-level complexity)
Strategic	**Low** (cognitive and social dimensions dominate; no geographic fixity)	**Fails** (cognitive/ narrative spaces cannot be seized or held)	**Absent** (influence campaigns shift over days; no doctrinal reassessment cycle)	**Fails** (terrain concept loses coherence; no strategic identification framework)

Source: author

Physical layer elements retain importance, but logical and persona layers become increasingly relevant as operations span longer periods and broader objectives. AJP-3.20 acknowledges the operational dimension of cyberspace through its treatment of joint functions (paras. 1.23-1.35), noting that cyberspace operations *"may support other operations or achieve operational objectives by itself"* and that *"effects by COs are synchronized with other effects and capabilities of the overall operation to create synergy"* (para. 1.23).

The challenge is that subject matter expert evaluation (the primary methodology at tactical level) does not scale adequately to the operational level's complexity. Huntley (2016) identifies this scalability problem as a central limitation of existing conceptualizations. The absence of formal cyber key terrain frameworks in AJP-3.20 means that operational planners lack doctrinal guidance for systematic terrain identification

across even the three recognized layers, let alone the expanded models proposed in academic literature. How to conduct systematic key terrain identification in the logical or persona layers at campaign scale, or how to manage the different update cycles those layers require, remains an open methodological question.

Modern operational doctrine increasingly emphasizes multi-domain operations (MDO), in which cyber effects must be synchronized with air, land, maritime, and space operations. AJP-3.20 addresses cross-domain synchronization through its joint functions framework, noting that cyberspace operations must be coordinated with electromagnetic operations (para. 1.29), intelligence (para. 1.31), and information activities (para. 1.32).

The Atlantic Council (2024) has assessed NATO's progress toward multi-domain integration. However, coherent conceptual agreement on MDO implementation across the Alliance remains incomplete. The UK's CEMA concept (UK Ministry of Defence 2018) represents one national attempt to address this integration challenge, emphasizing the synchronization of cyber and electromagnetic activities to deliver operational advantage, but it does not resolve the underlying terrain identification problem across the higher layers. This gap is partly a reflection of the unresolved cyber key terrain paradox: without coherent concepts of decisive cyber positions across all layers and all levels, meaningful integration with other domains remains aspirational rather than systematic.

3.3.3. Strategic Level: Where the Concept Breaks Down

At the strategic level, concerned with achieving national objectives, allocating resources across theatres, and shaping long-term capabilities, contradictions between cyber key terrain definitions and requirements become acute. Huntley (2016) documented the pattern of strategic documents avoiding the cyber key terrain term across successive U.S. DoD strategy documents, a pattern that continues through the 2023 DoD Cyber Strategy. AJP-3.20's three-layer model provides no strategic-level terrain identification framework, and the publication's planning and conduct guidance (Chapter 3) focuses on operational-level considerations, without addressing what key terrain identification looks like when applied to the cyber-persona layer at strategic scale, let alone to the cognitive and social dimensions identified in the broader IE concept (para. 1.3).

The cognitive and social dimensions, which AJP-3.20 acknowledges through its information environment formulation (para. 1.3) and its treatment of the information function (para. 1.32), present the

sharpest challenge. AJP-3.20 notes that the IE encompasses *"cognitive, virtual and physical space"* (para. 1.3) and that information activities seek to *"influence relevant actor perceptions, behavior, action or inaction and decision making"* (para. 1.32).

These are the spaces where influence operations, disinformation campaigns, and strategic narrative competition occur. JP 3-12 defines the cyber-persona layer similarly. Raymond et al. (2014) identify some persona-layer key terrain elements (administrator accounts, political leader accounts), but these treat personas as technical access points rather than engaging the strategic challenge of population-scale influence networks. Australia's recent establishment of dedicated cognitive and information warfare career tracks within the ADF (Australian Department of Defence 2024) represents an institutional recognition that operations in the cognitive dimension require fundamentally different skills and frameworks from those used for technical cyberspace operations, a distinction that terrain-based conceptualizations do not currently accommodate.

Venables (2021) explicitly separates persona, services, and semantic layers, demonstrating that the human-interaction dimensions of cyberspace are analytically distinct from the technical infrastructure, yet no terrain identification framework exists for any of them.

Mills (2012) expands cyber key terrain to include workforce, innovation capacity, and international standards bodies. These elements fail the core criteria of traditional terrain: they cannot be seized through military operations, they lack geographic location or topological position, and they relate to military capabilities through causal chains spanning decades. If cyber terrain is expanded to include all factors affecting cyber capabilities, the concept loses analytical utility. AJP-3.20's civil-military cooperation section acknowledges the boundary problem: cyberspace *"allows commanders to establish information links with civilian counterparts"* and cooperation can improve *"cyber security"* of civilian actors (para. 1.35), recognizing that operationally significant terrain elements in cyberspace are often outside the direct control of the military.

At strategic levels, the national security implications multiply: without coherent strategic terrain concepts, militaries lack frameworks for prioritizing long-term cyber investments, and doctrinal gaps cascade downward, creating confusion about priorities, authorities, and methods at lower levels.

3.4. The Reconciliation Framework

3.4.1. Acknowledging the Metaphorical Nature of Cyber Terrain

The foundation of the proposed reconciliation framework is explicit acknowledgement that cyber key terrain is, as Huntley (2016) concludes, *"necessarily metaphorical."* Metaphors work by transferring understanding from familiar domains to less familiar ones. For physical cyber infrastructure and tactical operations, the alignment between source and target domain is sufficient for the terrain metaphor to generate useful analytical insights; the academic literature on tactical cyber terrain mapping is evidence of this utility (Bodeau, Graubart, and Heinbockel 2013; Guion and Reith 2017).

For the logical and persona layers at operational scale, and for the cognitive and social dimensions at any level, the alignment breaks down in ways that current doctrine does not acknowledge. AJP-3.20's IE formulation (para. 1.3), by explicitly acknowledging cognitive and virtual spaces as operationally significant, implicitly recognizes these dimensions, but provides no terrain framework for them, leaving practitioners with a conceptual gap precisely where strategic effects are increasingly contested.

3.4.2. Adaptive Layer-Specific Definitions

Rather than seeking one universal definition, doctrine should provide adaptive definitions that vary by operational level and cyberspace layer.

At the ***tactical physical dimension*** (AJP-3.20's physical layer, para. 1.10): *cyber key terrain consists of network infrastructure, devices, and physical connections whose control or denial would immediately and significantly affect mission accomplishment within a defined operational timeframe*.

At the ***tactical virtual dimension*** (AJP-3.20's logical and cyber-persona layers, paras. 1.11–1.12): *key terrain consists of software systems, data repositories, logical network configurations, and digital identities whose exploitation, control, or disruption would provide marked tactical advantage in achieving specific mission objectives*.

At the ***operational physical dimension***: *cyber key terrain consists of infrastructure and network systems whose sustained control enables campaign operations, serves as necessary foundation for multiple tactical operations, or whose loss would require significant operational adaptation, including expeditionary cyber capabilities required for operations against isolated networks* (Joint Chiefs of Staff 2022).

At the ***operational virtual dimension***: *key terrain consists of software architectures, data systems, protocol implementations, and influence network positions whose control enables sustained offensive or defensive operations, facilitates multi-domain integration, or whose compromise would produce cascading operational effects*.

At the ***strategic physical dimension***: *cyber key terrain consists of critical infrastructure whose control affects national cyber capabilities or enables long-term strategic operations, including infrastructure outside direct military control requiring civil-military coordination* (AJP-3.20 para. 1.35).

At the ***strategic virtual and cognitive dimensions:*** the framework explicitly acknowledges that the terrain metaphor is severely strained for the cognitive and social spaces identified in AJP-3.20's IE concept (para. 1.3). The information function's emphasis on influencing *"relevant actor perceptions, behavior, action or inaction and decision making"* (para. 1.32) indicates that alternative conceptual models (influence topology mapping, social network centrality analysis, narrative space models) may provide superior operational understanding at these layers than terrain metaphors. Terrain language may be preserved for doctrinal continuity, but practitioners must understand its metaphorical limitations in these contexts.

3.4.3. Temporal Classification

Building on AJP-3.20's acknowledgement that cyberspace is "in constant flux" and "constantly under development" (para. 1.8), doctrine must incorporate an explicit temporal classification across all layers. Static elements (geographic infrastructure locations, submarine cables, major data centers) change over years and warrant annual reassessment (these correspond to the physical layer in AJP-3.20) (para. 1.10). Semi-static elements (physical network configurations, installed software, established protocols) change over months and warrant quarterly review. Dynamic elements (active vulnerabilities, authentication credentials, cloud configurations) change over weeks and require monthly assessment or intelligence-triggered updates. Highly dynamic elements (persona profiles, social media presence, current influence campaigns) change over days and require continuous monitoring, a timescale for which no systematic NATO doctrine currently exists. The temporal instability of cognitive-layer terrain, which changes at human psychological rates under operational information pressure, is the most analytically challenging and the most under addressed in current doctrine.

Table 3 presents the temporal classification framework above, specifying reassessment cycles

calibrated to each layer's actual rate of change and its correspondence to AJP-3.20's layer model.

Table 3. Temporal Classification of Cyber Terrain Elements across AJP-3.20 Layers.

Category	Example Elements	Rate of Change	Reassessment Cycle	AJP-3.20 Layer Correspondence
Static	Geographic infrastructure locations, submarine cables, major data centers	Years	Annual	Physical layer (para. 1.10)
Semi-static	Physical network configurations, installed software, established protocols	Months	Quarterly	Physical / lower Logical (paras. 1.10–1.11)
Dynamic	Active vulnerabilities, authentication credentials, cloud configurations	Weeks	Monthly or intelligence-triggered	Logical layer (para. 1.11)
Highly dynamic	Persona profiles, social media presence, active influence campaigns	Days	Continuous monitoring	Cyber-persona / Cognitive IE (paras. 1.12, 1.3)

Source: author

3.4.4. Context-Dependent Identification Methodology

A practical methodology for cyber key terrain identification must be context-dependent, extending the planning processes described in AJP-3.20 Chapter 3 to address all recognized cyberspace layers and the broader IE dimensions. The following eight-step process provides a structured approach consistent with AJP-3.20's operations planning process (paras. 3.18–3.26) while addressing the limitations identified in this study.

- ***Step 1*** defines the operational context: level (tactical, operational, strategic), mission type (offensive, defensive, intelligence, or influence), and relevant timeframe, with explicit identification of which cyberspace layers and IE dimensions are implicated.
- ***Step 2*** identifies the relevant cyberspace layers across the AJP-3.20 three-layer model and, where operationally appropriate, the expanded layers proposed in academic

literature.

- ***Step 3*** applies layer-specific identification methods: network mapping and infrastructure assessment for the physical layer; software dependency analysis and vulnerability assessment for the logical layer; social network analysis and influence mapping for the cyber-persona layer and the cognitive/social dimensions of the IE.
- ***Step 4*** applies criticality metrics appropriate to the operational level.
- ***Step 5*** assesses temporal factors using the classification above, determining validity periods and establishing update schedules calibrated to each layer's actual rate of change.
- ***Step 6*** documents the metaphorical limitations of terrain language for the layers under assessment, particularly at operational and strategic levels for virtual and cognitive dimensions, and notes where alternative frameworks supplement terrain analysis.
- ***Step 7*** integrates the terrain assessment into the AJP-3.20 planning process (the informing course of action development - para. 3.22), supporting risk management (paras. 3.27-3.29), and coordinating across domains and authorities, including civil-military coordination for infrastructure outside direct military control (para. 1.35).
- ***Step 8*** establishes continuous assessment and adaptation, recognizing that cyber terrain requires ongoing monitoring matched to each layer's temporal classification rather than the periodic static studies appropriate to physical terrain.
- Figure 1 presents the eight-step context-dependent identification methodology proposed in section 3.4.4, illustrating the sequential process and the continuous feedback loop between Step 8 and Step 1 that reflects the dynamic nature of cyber terrain.

3.4.5 Criticality Metrics across Levels

Defining "key" terrain requires metrics of criticality across operational levels. At the *tactical level*, relevant metrics include mission dependency (does this element directly enable mission-essential functions), redundancy (are alternative elements available), recovery time, and access control difficulty. At the *operational level*, metrics include campaign criticality, cascade potential, integration significance for multi-domain synchronization, and adaptation timeframe if the element is lost.

Fig. 1. Eight-Step Context-Dependent Cyber Key Terrain Identification Methodology (adapted from AJP-3.20 planning process, paras. 3.18-3.26)

At the *strategic level*, metrics include national capability impact, international implications, long-term significance, and economic and political consequences. For *virtual and cognitive layers at strategic level*, influence metrics (narrative reach, audience penetration, credibility position, community centrality) supplement or replace traditional terrain control metrics. These adapted metrics reflect the fundamental difference between controlling a physical node and achieving advantage in a cognitive or social space.

Table 4 consolidates the criticality metrics above, organizing them by operational level and distinguishing physical-layer metrics from those applicable to virtual and cognitive dimensions.

Table 4. Criticality Metrics for Cyber Key Terrain Identification across Operational Levels.

Metric Category	Tactical Level	Operational Level	Strategic Level
Primary focus	Mission-essential functions	Campaign continuity	National cyber capability
Key metrics	Mission dependency; redundancy; recovery time; access control difficulty	Campaign criticality; cascade potential; MDO integration significance; adaptation timeframe	National capability impact; international implications; long-term significance; economic and political consequences
Virtual / cognitive layer metrics	Not applicable at tactical physical focus	Influence network position; protocol control; data architecture access	Narrative reach; audience penetration; credibility position; community centrality
Primary identification method	Subject matter expert evaluation; network mapping	Dependency analysis; vulnerability assessment at scale	Social network analysis; influence topology mapping; graph-theoretic models

Source: author

3.5. Alternative Conceptual Frameworks for Virtual and Cognitive Layers

The recognition that the information environment encompasses cognitive, virtual, and physical spaces (AJP-3.20 para. 1.3), combined with the progressive expansion of cyberspace models in academic literature, and creates a doctrinal imperative for alternative conceptual frameworks that are native to the virtual and cognitive dimensions. For the logical layer, architectural and graph-theoretic models analyze network centrality, connectivity, and shortest paths, providing rigorous analytical grounding that terrain metaphors lack. Ecosystem models capture cascading failures and systemic vulnerabilities, consistent with AJP-3.20's concern with cascading effects in cyberspace operations (para. 2.28). Economic models of bottlenecks and critical dependencies offer additional analytical purchase.

For the cyber-persona layer (AJP-3.20 para. 1.12) and the cognitive and social dimensions of the IE, the terrain metaphor becomes analytically deceptive at operational and strategic scale. Social network models identify influencers, connectors, and bridges between communities, while market-share models frame competition for attention, credibility, and narrative dominance. Epidemiological models track information spread and viral dynamics, while game-theoretic models analyze strategic interactions and reputation dynamics.

These frameworks are native to the properties of the virtual and cognitive environment and are better aligned with the analytical methods of the social and cognitive sciences, whose expertise is increasingly relevant to cyber operations at these layers.

AJP-3.20 itself implicitly acknowledges this need through its treatment of the information function (para. 1.32), identifying Strategic Communications, Information Operations, Psychological Operations, and Military Public Affairs as key enablers. These descriptions call for social network analysis, audience segmentation, and cognitive influence modelling, not terrain identification. The doctrinal implication is not to abandon terrain language entirely (its familiarity and genuine utility at the physical dimension are assets worth preserving) but to treat terrain thinking as one framework among several, appropriate to specific layers and levels, supplemented explicitly by alternative models where its assumptions do not hold.

Each of these alternative frameworks offers distinct analytical capabilities and carries specific limitations that operational planners must understand.

For the logical layer, ***graph-theoretic centrality models*** identify which network nodes lie on the most critical communication paths, providing a mathematically rigorous basis for prioritization that terrain

metaphors cannot supply. Two measures are particularly relevant: *betweenness centrality*, which quantifies how frequently a node appears on shortest paths between other nodes, and *eigenvector centrality*, which weights a node's importance by the connectivity of its neighbors. A node with high betweenness centrality is analytically analogous to key terrain in the sense that its removal would disproportionately disrupt network function, but the concept is defined relationally rather than spatially, and it changes as the network topology evolves. The primary limitation is the assumption of topological stability: centrality measures become unreliable in rapidly reconfiguring networks, which is precisely the environment in which cyber operations occur.

Ecosystem models address this partially by modelling cascading failure dynamics, but they require detailed knowledge of interdependencies that may not be available in adversarial contexts.

For the cyber-persona layer, ***social network analysis (SNA)*** provides concrete metrics (degree centrality, clustering coefficient, and bridging coefficient) that identify key influencers, community connectors, and information brokers within a target population. In an influence operation context, an account with high bridging centrality that connects otherwise disconnected communities occupies a position functionally analogous to key terrain: its compromise or co-option would provide marked advantage in shaping information flows across the network.

The critical limitation of SNA in this context is that it captures structural position but not content, credibility, or narrative resonance: a structurally central account that loses credibility may retain its network position while losing its operational significance, a dynamic that terrain metaphors cannot adequately model. SNA must therefore be combined with content analysis and audience segmentation to provide operationally useful assessments.

Epidemiological models (adapted from the SIR - Susceptible-Infected-Recovered) framework used in disease modelling) offer a powerful approach to tracking information spread and estimating the reach of disinformation campaigns. The *basic reproduction number* (R_0) concept, when adapted to information spread, provides planners with an estimate of how many additional actors a given narrative will reach from each exposed individual, enabling assessment of viral dynamics before an operation reaches saturation.

The principal limitation is the assumption of population homogeneity: unlike biological pathogens, information spread is highly sensitive to individual credibility assessments, prior beliefs, and community membership, factors that require significant empirical calibration to model accurately.

Game-theoretic models, finally, provide analytical purchase on strategic interactions where outcomes depend on the choices of multiple actors, particularly useful for modelling credibility dynamics, deterrence signaling, and reputation competition in the cognitive domain. Their principal limitation is the requirement for specified payoff structures that are rarely available with precision in operational contexts, making them more useful for conceptual analysis than for tactical planning.

These limitations do not diminish the utility of the proposed frameworks relative to terrain metaphors, but rather underscore the need for a multi-framework approach in which no single conceptual model is treated as universally applicable. The practical implication for doctrine is that the selection of analytical framework should be driven by the operational layer, the temporal classification of the terrain elements under assessment, and the specific planning question being addressed (precisely the context-dependent approach formalized in the eight-step methodology proposed in section 3.4.4.).

4. DISCUSSION

4.1. Interpreting the Paradox

The cyber key terrain paradox (the systematic degradation of the concept's utility as operations move from physical-layer tactical applications toward virtual and cognitive layer strategic ones) is not a peripheral doctrinal curiosity. It reflects a fundamental challenge in adapting centuries of military spatial thinking to a domain that is partially but not wholly spatial. A critical finding of this analysis is that the paradox is already present within AJP-3.20's three-layer model: the cyber-persona layer (para. 1.12) already strains the terrain metaphor, since virtual identities lack the physical properties that terrain concepts assume. The expanded models proposed in academic literature (particularly Venables's eight-layer model and Grant's cognitive dimensions) intensify the paradox further, by formally incorporating layers for which no terrain identification methodology exists.

The findings confirm Huntley's (2016) assessment that the concept is necessarily metaphorical, while specifying more precisely where the metaphor holds and where it fails. The metaphor holds well at the physical layer across all operational levels. It begins to struggle at the logical and cyber-persona layers, particularly at operational and strategic scales. It fails in the cognitive and social dimensions of the IE, where the concept of seizing or retaining a decisive position has no meaningful analogue in environments characterized by mass-scale influence, shifting narratives, and psychological effects on human decision-making. The absence of a formal NATO-agreed cyber

key terrain definition in AJP-3.20 (and the corresponding absence of terrain identification frameworks for any layer) may itself be a tacit acknowledgement that the Alliance has not yet resolved these conceptual challenges.

4.2. Doctrinal Recommendations

Several specific doctrinal recommendations follow from this analysis. First, NATO doctrine should develop and promulgate formal definitions for cyber key terrain, mission-relevant terrain in cyberspace, and an associated prioritized asset list, concepts that exist in academic literature (Raymond et al. 2014; Bodeau et al. 2013) and U.S. doctrine but are absent from AJP-3.20. These definitions should explicitly acknowledge the metaphorical nature of terrain concepts beyond the physical and lower logical layers, and state clearly that current identification methodologies do not extend to the cognitive and social dimensions of the IE.

Second, temporal classification should be formally incorporated into any cyber terrain framework, with explicit guidance on update cycles calibrated to each layer's rate of change. Third, NATO doctrine should either develop terrain identification methodologies specifically addressing the cyber-persona layer and the cognitive/social dimensions of the IE, or explicitly acknowledge that terrain language is unsuitable at those layers and introduce alternative conceptual frameworks (social network analysis, influence topology mapping) as primary analytical tools for operations in those dimensions.

Fourth, JP 3-12 and AJP-3.20 should be reconciled on layer models. The current three-layer alignment provides formal interoperability but masks a growing consensus that additional layers are operationally significant. Key allies have already moved beyond this model in their national force structures (the UK through CEMA, Australia through cognitive and information warfare integration, and Germany through the Cyber and Information Domain Service) creating de facto interoperability gaps that formal NATO doctrine does not yet address.

4.3 Implications for Operational Planning

For operational planners, the reconciliation framework has several practical implications. Planning processes should explicitly distinguish between terrain assessment at the physical, logical, and cyber-persona layers of AJP-3.20, and in the broader cognitive and social dimensions of the IE, applying appropriate methodologies and criticality metrics to each. Terrain assessments should always specify their temporal scope and validity period, with update mechanisms calibrated to the temporal classification of each layer.

Multi-domain operations planning should integrate cyber terrain assessment across all

recognized layers, not only the physical dimension, to support meaningful synchronization with other domains and with the non-military instruments of power that contemporary doctrine requires. Practical guidance for bridging joint doctrine and operational planning in this domain is available in the U.S. Army War College Strategic Cyberspace Operations Primer (U.S. Army War College 2023), which synthesizes joint and service doctrine into a planning-oriented reference applicable across command levels.

For allied and combined operations, the definitional inconsistencies documented in this paper argue for urgent development of NATO Standardization Agreements covering cyber terrain identification methodologies across all layers. The existing AJP-3.20 terminology (para. 1.13) (cyberspace, cyberspace operation, defensive and offensive cyberspace operations, cyber security, mission assurance) provides a foundation, but cyber key terrain and associated concepts require formal NATO-agreed definitions and methodological guidance.

4.4. Implications for Professional Military Education

The concepts proposed here require integration into professional military education at all levels. Officers must understand both the genuine tactical utility of physical-layer terrain concepts and the metaphorical limitations of terrain thinking in the virtual and cognitive dimensions. Curricula should introduce the layer models, layer-specific definitions, and alternative frameworks proposed in this study. Exercises should practice terrain identification at tactical, operational, and strategic levels with appropriate variation in methodology and metrics.

The cross-level planning dimension (understanding how tactical terrain assessment feeds operational planning and how operational priorities relate to strategic requirements across all layers) is particularly important and currently tempered in existing training frameworks. Additionally, education programmes should address the divergent national approaches to cyberspace conceptualization among key allies, ensuring that officers understand how different layer models and organizational structures (such as the UK's CEMA integration, Australia's cognitive warfare separation, and Germany's information domain service model) affect planning interoperability in coalition operations.

4.5. Limitations and Future Research Directions

The reconciliation framework proposed in this study is developed through doctrinal and conceptual analysis, which, while consistent with the methodology employed, means that empirical or operational validation remains a next step. Testing the framework against real-world planning requirements

through case studies, simulations, or operational examples would further strengthen its practical applicability.

While this is consistent with the doctrinal concept development methodology employed (Raymond et al. 2014; Huntley 2016), it means that the practical utility of the proposed layer-specific definitions, temporal classification, and eight-step identification methodology remains to be demonstrated in operational contexts. The alternative conceptual models proposed for virtual and cognitive layers (social network analysis, influence topology mapping, and graph theoretic approaches) have established methodological foundations in their source disciplines but have not been empirically validated as planning tools in military cyber operations contexts. Applying the framework to a documented cyber campaign (such as the 2007 Estonia incidents, the 2015-2016 Ukrainian power grid attacks, or the cognitive dimension operations associated with recent hybrid warfare cases) would constitute the most direct form of validation and is identified as the primary direction for future research.

A further limitation is that, despite the addition of non-NATO perspectives in section 3.1.5, the study remains primarily grounded in U.S. and NATO doctrinal sources. The extent to which the paradox manifests differently within Chinese and Russian doctrine, and the operational implications for allied planning in contested information environments, merit deeper separate investigation. These represent the primary directions for future research, alongside the development of practical tools for multi-layer terrain mapping and the empirical testing of criticality metrics against operational outcomes.

5. CONCLUSIONS

The reconciliation framework proposed here does not resolve the fundamental tension between spatial military thinking and the non-spatial dimensions of cyberspace, but it underlines that tension explicitly. The framework preserves the genuine utility of terrain thinking while preventing its misapplication through four integrated contributions: layer-specific and level-specific adaptive definitions, a temporal classification system that extends AJP-3.20's recognition of cyberspace dynamism, a structured identification methodology integrated with AJP-3.20's planning processes, and explicit alternative conceptual frameworks for the cognitive and social dimensions that current doctrine leaves unaddressed. The goal is not to achieve conceptual elegance but doctrinal coherence: a set of frameworks that military planners can apply across the full range of cyberspace operations, from tactical network defense to strategic cognitive dimension competition.

This study makes three principal contributions to military cyber doctrine. First, it provides a systematic cross-level documentation

of the cyber key terrain paradox, demonstrating that the concept's degradation from tactical to strategic levels is structural, predictable, and already manifest within AJP-3.20's three-layer model. Also, it identifies the temporal instability of cyberspace as a cross-cutting dimension of the paradox that current doctrine addresses only in general terms, without providing systematic frameworks for managing different rates of change across layers. Furthermore, it proposes a reconciliation framework that preserves the tactical utility of terrain thinking, while providing the doctrinal coherence that operational and strategic planning across all layers requires.

The most urgent practical implication is the need to develop formal NATO-agreed definitions for cyber key terrain and associated concepts, and to supplement these with explicit guidance for the cyber-persona layer and the cognitive and social dimensions of the information environment.

Addressing the gap between the recognized multi-dimensional character of cyberspace and the predominantly physical-centric terrain frameworks currently available would meaningfully advance military planning across the full scope of cyberspace operations, and in particular support the integration of cognitive dimension operations into multi-domain approaches.

DATA AVAILABILITY STATEMENT

All data supporting the findings of this study are included in the manuscript. The analysis is based exclusively on publicly available military doctrine and peer-reviewed academic literature cited in the references.

AI DISCLOSURE

During the preparation of this work, the author used AI-assisted writing tools to support structural organization and language editing. All substantive analytical content, doctrinal interpretations, and conclusions are the author's own. The author reviewed and edited all AI-assisted content and takes full responsibility for the accuracy and integrity of the published work.

REFERENCES

[1] Atlantic Council. 2024. NATO Multidomain Operations: Assessment and Recommendations. Washington, DC: Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2024/03/NATO-multidomain-operations-Near-and-medium-term-priority-initiatives.pdf

[2] Wardrop, C. 2020. "Victory in the Age of Cyber-Enabled Warfare." Future Forge. Canberra: Australian Army Research Centre. https://theforge.defence.gov.au/publications/victory-age-cyber-enabled-warfare

[3] Australian Department of Defence. 2024. ADF-C-0: Australian Military Power. Edition 2. Canberra: Department of Defence.

[4] Bertoli, G., and S. Raio. 2018. "The Elusive Nature of Cyber Terrain." Journal of Cyber Security and Information Systems: 40-47.

[5] Bodeau, D., R. Graubart, and W. Heinbockel. 2013. Mapping the Cyber Terrain. Bedford, MA: The MITRE Corporation. https://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf

[6] Codreanu, A. 2020. "Competențe necesare gestionării infrastructurilor critice" [Competencies Required for Critical Infrastructure Management]. In Managementul Capabilităților și capabilitatea managerială în cadrul sistemelor de infrastructuri critice, edited by Dorel Badea, Olga Bucoveţchi, and Dumitru Iancu, 90-104. Sibiu: Editura Academiei Forțelor Terestre "Nicolae Bălcescu."

[7] Department of the Air Force. 2021. Air Force Doctrine Publication 3-12: Cyberspace Operations. Washington, DC: Department of the Air Force. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf

[8] Dodge, M., and R. Kitchin. 2001. Mapping Cyberspace. London: Routledge. https://doi.org/10.4324/9780203165270

[9] Development, Concepts and Doctrine Centre. 2022. Cyber Primer. 3rd ed. Shrivenham, UK: UK Ministry of Defence. https://www.gov.uk/government/publications/cyber-primer

[10] Franz III, G. J. 2012. "Effective Synchronization and Integration of Effects through Cyberspace for the Joint Warfighter." Presentation at AFCEA TechNetLand Forces-East Conference, Baltimore, MD, August.

[11] Gao, C., Q. Guo, D. Jiang, Z. Wang, C. Fang, and M. Hao. 2019. "Theoretical Basis and Technical Methods of Cyberspace Geography." Journal of Geographical Sciences 29: 1949–1964. https://doi.org/10.1007/s11442-019-1698-7

[12] Giles, K. 2016. Handbook of Russian Information Warfare. Rome: NATO Defense College. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf

[13] Grandin, A. 2023. "Cyberspace Geography and Cyber Terrain: Challenges in Producing a Universal Map of Cyberspace." In Proceedings of the 22nd European Conference on Cyber Warfare and Security, 207-213. https://papers.academic-conferences.org/index.php/eccws/article/view/1255

[14] Grant, T. 2014. "On the Military Geography of Cyberspace." In Proceedings of the 9th International

Conference on Cyber Warfare & Security, 66-76. Purdue University.

[15] Guion, J., and M. Reith. 2017. "Cyber Terrain Mission Mapping: Tools and Methodologies." In 2017 International Conference on Cyber Conflict, 105–111. Washington, D.C.: IEEE. https://doi.org/10.1109/CYCONUS.2017.8167504

[16] Huntley, W. L. 2016. Cyber Key Terrain: A Conceptual Assessment. Monterey, CA: U.S. Naval Postgraduate School. https://apps.dtic.mil/sti/trecms/pdf/AD1111645.pdf

[17] Jakobson, G. 2011. "Mission Cyber Security Situation Assessment Using Impact Dependency Graphs." In 14th International Conference on Information Fusion, 1–8. Chicago, IL: IEEE. https://ieeexplore.ieee.org/document/5977648

[18] Joint Chiefs of Staff. 2009. Joint Publication 2-01.3: Joint Intelligence Preparation of the Operational Environment. Washington, DC: Joint Chiefs of Staff. https://irp.fas.org/doddir/military/jp2_01_3.pdf

[19] Joint Chiefs of Staff. 2018. Joint Publication 3-12: Cyberspace Operations. Washington, DC: Joint Chiefs of Staff. https://irp.fas.org/doddir/dod/jp3_12.pdf

[20] Joint Chiefs of Staff. 2022. Joint Publication 3-12: Cyberspace Operations. Rev. ed. Washington, DC: Joint Chiefs of Staff. https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2018-JP-3-12-Cyberspace-Operations.pdf

[21] Lü, G., L. Yuan, and Z. Yu. 2021. "Information Geography: A New Fulcrum of Geographic Ternary World." Science China Earth Sciences 65 (2): 383–386. https://doi.org/10.1007/s11430-021-9859-9

[22] Mills, J. R. 2012. "The Key Terrain of Cyber." Georgetown Journal of International Affairs, special issue: 99-107.

[23] NATO Standardization Office. 2020. AJP-3.20: Allied Joint Doctrine for Cyberspace Operations. Edition A, Version 1. Brussels: NATO Standardization Office. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

[24] UK Ministry of Defence. 2018. Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities. Shrivenham, UK: Development, Concepts and Doctrine Centre. https://assets.publishing.service.gov.uk/media/5a8d6373e5274a5e67567dff/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf

[25] Pingel, T. J. 2003. "Key Defensive Terrain in Cyberspace: A Geographic Perspective." In Proceedings of the International Conference on Politics and Information Systems, 159–163. Orlando.

[26] Price, P., N. A. Leyba, M. Gondree, Z. Staples, and T. Parker. 2017. "Asset Criticality in Mission Reconfigurable Cyber Systems and Its Contribution to Key Terrain Identification." In Proceedings of the 50th Hawaii International Conference on System Sciences. Hawaii. https://doi.org/10.24251/HICSS.2017.729

[27] Raymond, D., G. Conti, T. Cross, and R. Fanelli. 2013. "A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons." In 2013 5th International Conference on Cyber Conflict, 1–16. Tallinn, Estonia: IEEE. https://ccdcoe.org/uploads/2018/10/8_d1r2s6_raymond.pdf

[28] Raymond, D., G. Conti, T. Cross, and M. Nowatkowski. 2014. "Key Terrain in Cyberspace: Seeking the High Ground." In 6th International Conference on Cyber Conflict, edited by P. Brangetto, M. Maybaum, and J. Stinissen, 287–300. Tallinn: NATO CCD COE Publications. https://ccdcoe.org/uploads/2018/10/d2r1s8_raymondcross.pdf

[29] Thomas, T. L. 2004. "Russia's Reflexive Control Theory and the Military." Journal of Slavic Military Studies 17 (2): 237–256. https://doi.org/10.1080/13518040490450529

[30] U.S. Army War College. 2023. Strategic Cyberspace Operations Primer. Carlisle, PA: U.S. Army War College. https://csl.armywarcollege.edu/pubs/Publications/Strategic_Cyberspace_Operations_Primer-2023_Dec_18.pdf

[31] U.S. Department of Defense. 2023. 2023 DoD Cyber Strategy. Washington, DC: U.S. Department of Defense. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf

[32] Venables, A. 2021. "Modelling Cyberspace to Determine Cybersecurity Training Requirements." Frontiers in Education 6: 768037. https://doi.org/10.3389/feduc.2021.768037

[33] Xu, R., Z. Zhang, Z. Rao, J. Chen, M. Li, F. Liu, and S. Pan. 2019. "Cyberspace Surveying and Mapping: Hierarchical Model and Resource Formalization." In IEEE INFOCOM 2019, 68–72. IEEE. https://doi.org/10.1109/INFCOMW.2019.8845226

[34] Ye Zheng. 2013. Lectures on Information Operations (in Chinese). China Academy of Military Science (AMS), Beijing: Military Science Press, 2013

[35] Youn, J., H. Oh, J. Kang, and D. Shin. 2021. "Research on Cyber IPB Visualization Method Based on BGP Archive Data for Cyber Situation Awareness." KSII Transactions on Internet and Information Systems 15 (2): 749–766. https://doi.org/10.3837/tiis.2021.02.020

AI-DRIVEN CYBER CAPABILITIES IN DEFENSE RESOURCE PLANNING

Levan KALATOZISHVILI[1]

Caucasus International University Tbilisi, Georgia

This article examines the integration of AI-driven cyber capabilities into defense resource planning, highlighting their transformative impact on strategic, human, and technological resource allocation. While cyber capabilities have traditionally focused on operational effectiveness, the advent of AI introduces unprecedented complexity in capability development, budgeting, training, and doctrine adaptation. The study identifies current challenges in aligning AI-enhanced cyber systems with existing defense resources, including workforce skill gaps, financial constraints, and operational readiness considerations. Using a comparative analysis of international case studies and defense planning frameworks, the research demonstrates how AI-driven capabilities can optimize resource distribution, enhance response times to cyber threats, and strengthen overall military preparedness. The article contributes novel insights into the operationalization of AI in defense contexts, offering a framework for strategic resource allocation that balances technological innovation with human and institutional constraints. Findings indicate that effective integration of AI-driven cyber capabilities requires coordinated planning, continuous skill development, and adaptive doctrines, ensuring that defense organizations can fully leverage emerging technologies while maintaining resilience and strategic flexibility.

Key words: *AI, Cyber Capabilities, Defense Resource Planning, Capability Development, Strategic Management*

1. INTRODUCTION

The integration of artificial intelligence (AI) into cyber capabilities is increasingly influencing contemporary defense planning and resource management. Cyber threats have evolved into persistent strategic challenges with direct implications for national security and military readiness, prompting defense institutions to recognize cyberspace as a distinct operational domain [7]. At the same time, AI-enabled tools are rapidly

[1] ORCID ID: 0009-0004-0714-8048, e-mail: levan.kalatozishvili@ciu.edu.ge

expanding the scale, speed, and adaptability of cyber operations, challenging traditional defense planning models that were designed for relatively stable technological environments.

While cyber capabilities are now routinely addressed in strategic and doctrinal documents, the integration of AI-driven elements into defense resource planning remains uneven [2]. AI-driven cyber capabilities require new forms of workforce development, technological infrastructure, and adaptive institutional processes. These requirements place pressure on planning systems that traditionally emphasize fixed procurement cycles and stable personnel structures.

Despite the growing policy attention to military AI and cyber operations, existing academic literature often treats these areas separately from defense resource management. Research on AI in defense primarily focuses on operational effectiveness or ethical considerations, while defense planning scholarship emphasizes budgeting and force structure with limited attention to the lifecycle characteristics of AI-enabled cyber capabilities [24].

This study addresses this gap by examining AI-driven cyber capabilities through the lens of defense resource planning. Using qualitative analysis of publicly available defense planning documents and international policy frameworks, the study assesses how strategic intent regarding AI and cyber capabilities is translated into practical resource planning [3].

The central hypothesis is that effective integration of AI-driven cyber capabilities depends on coordinated and adaptive resource management across human, technological, and institutional domains. Defense organizations that treat AI-enabled cyber capabilities as dynamic, lifecycle-dependent assets—rather than isolated technological investments—are better positioned to sustain operational effectiveness and strategic resilience.

2. METHODOLOGY

This research adopts a qualitative, document-based analytical methodology designed to examine how artificial intelligence (AI)–driven cyber capabilities are integrated into defense resource planning and capability development processes. The methodological approach is grounded in established traditions of defense studies, security policy analysis, and resource management research, all of which emphasize systematic examination of official documents, institutional frameworks, and comparative case material as valid sources for understanding strategic and organizational change

within defense institutions [37]. By combining content analysis, comparative evaluation, and process tracing, this study seeks to provide a comprehensive assessment of the structural, technological, and human resource dimensions of AI-enabled cyber capabilities in contemporary defense planning.

2.1 Research Design and Rationale

The integration of AI-driven cyber capabilities into defense resource planning represents a complex institutional and organizational process rather than a purely quantifiable phenomenon. Consequently, a qualitative research design is employed to explore the interplay between policy intentions, organizational processes, and practical implementation, which cannot be adequately assessed through quantitative measures alone.

Qualitative analysis is widely used in defense and security studies where access to classified operational data is limited [44]. By systematically analyzing these materials, this study identifies patterns in the allocation of resources, prioritization of AI capabilities, and the incorporation of technological, human, and organizational dimensions into strategic planning.

2.2 Data Sources and Material Selection

The empirical material for this research was selected according to three primary categories: (1) official defense and security policy documents; (2) international and alliance-level strategic frameworks; and (3) secondary academic and institutional literature.

2.2.1 Official Defense and Security Policy Documents

These documents form the core empirical base of the study and include national defense strategies, cyber defense strategies, AI strategies, capability development plans, and resource management guidelines published by allied defense institutions. The study exclusively considers publicly available, officially endorsed documents to ensure transparency, replicability, and ethical compliance. For example, the U.S. Department of Defense AI Strategy outlines priorities for workforce development, technology investment, and capability integration, offering a concrete reference for evaluating planning practices in AI-enabled cyber domains [6].

2.2.2 International and Alliance-Level Frameworks

Strategic concepts and planning documents produced by NATO and the European Union constitute the second source category. These materials are particularly relevant as they influence national defense planning by setting interoperability

standards, defining capability targets, and providing guidance on emerging technologies such as AI. For instance, the NATO Artificial Intelligence Strategy emphasizes the need for capability-based planning, the development of human capital, and lifecycle integration of AI systems [2]. Examining these documents allows the research to assess the extent to which national defense organizations align their internal resource planning with alliance-level strategic priorities.

2.2.3 Secondary Academic and Institutional Literature

Academic books, peer-reviewed journal articles, and reports from recognized defense and security research institutions provide both theoretical grounding and methodological support. Selected literature focuses on three intersecting domains: military applications of AI, cyber operations and defense, and resource management in capability-based planning. This literature contextualizes the empirical findings, supports the analytical framework, and ensures that the research contributes to ongoing academic debates. For example, existing research on AI and national security emphasizes the integration of human, technological, and institutional dimensions in defense planning [24].

2.3 Analytical Framework

The analytical framework links AI-driven cyber capabilities to defense resource planning through three interrelated dimensions: human resources, technological resources, and institutional processes. This approach draws on capability-based planning theory, which emphasizes the integrated development, sustainment, and operationalization of capabilities as holistic systems rather than isolated assets [24].

2.3.1 Human Resources

Human resource considerations are central to the study, as AI-enabled cyber capabilities place unique demands on personnel. Workforce planning, skill development, recruitment, training, and retention are examined across defense planning documents to assess how organizations anticipate and address these requirements. Special attention is given to the integration of AI-specific competencies, including machine learning, data analytics, and cyber operations. The analysis evaluates whether human capital planning is treated as a central priority or as an ancillary concern, reflecting broader institutional adaptation to emerging technological challenges [46].

2.3.2 Technological Resources

Technological resources include computational infrastructure, data ecosystems, software environments, and cyber platforms essential for AI-enabled operations. The framework

examines how these requirements are addressed within defense planning cycles, particularly regarding lifecycle management, sustainability, and adaptability. This dimension contrasts the static procurement models characteristic of conventional defense planning with the continuous investment and maintenance required by AI systems [24].

2.3.3 Institutional Processes

Institutional processes encompass planning cycles, governance mechanisms, and coordination structures that shape resource allocation decisions. The framework evaluates whether existing planning models are sufficiently flexible to integrate AI-driven capabilities, or whether structural rigidities, bureaucratic inertia, and traditional hierarchies limit effective adoption. This dimension also considers policy coherence, alignment with alliance standards, and the degree to which resource planning is anticipatory versus reactive [2].

2.4 Methods of Examination

The study employs qualitative content analysis as the primary method of examination. Coding focuses on explicit and implicit references to AI-driven capabilities, workforce development, technology investments, and institutional processes. Comparative analysis is conducted across selected national defense institutions and alliance frameworks to identify convergences and divergences in how AI-driven cyber capabilities are addressed. The comparative analysis focuses on three representative defense planning models: the United States, the United Kingdom, and Estonia. This method enables assessment of organizational culture, strategic priorities, and governance practices in different planning environments [37].

Process tracing complements content and comparative analysis by examining how recognition of AI and cyber capabilities translates into tangible planning measures over time. This method assesses the evolution of resource planning practices, the continuity of strategic intent, and the adaptive mechanisms employed by defense organizations.

2.5 Validity, Reliability, and Limitations

Several measures were employed to enhance validity and reliability. Triangulation using multiple categories of sources ensures that findings are not reliant on a single perspective [17]. Limitations include the exclusive reliance on publicly available documents, which may omit classified operational details, particularly regarding budgets, procurement decisions, or operational readiness. Consequently, findings reflect institutional intent and planning logic rather than

precise implementation outcomes. Additionally, the rapidly evolving nature of AI and cyber technologies means that policy documents may lag behind actual technological capabilities and emerging threats [10].

2.6 Ethical and Normative Considerations

Although no human subjects or sensitive operational data were involved, ethical considerations were observed. The study avoids speculation on classified capabilities and ensures that all sources are cited transparently. Normative debates surrounding AI in military contexts—such as accountability, explainability, and governance—inform the interpretive lens but do not constitute the primary focus of the methodology [32].

2.7 Summary of Methodological Contribution

In sum, this methodology provides a structured and transparent approach for examining the integration of AI-driven cyber capabilities into defense resource planning. By combining qualitative content analysis, comparative evaluation, and process tracing, the study identifies institutional patterns, planning gaps, and adaptation challenges. This design explains how emerging technologies influence defense resource management within the logic of capability-based planning [24].

The methodology ensures that conclusions are grounded in verifiable evidence while providing actionable insights for policymakers, military planners, and scholars interested in AI, cyber capabilities, and capability-based defense planning.

3. RESULTS

Analysis of defense policy documents reveals patterns in how AI-driven cyber capabilities are incorporated into defense resource planning. These findings demonstrate both observable progress and persistent structural gaps, particularly in aligning strategic recognition of emerging technologies with formal resource allocation mechanisms.

By systematically examining 32 strategic and planning documents issued between 2018 and 2024 by NATO, the European Union, and selected national defense institutions, this research identifies the extent to which AI-enabled cyber capabilities are recognized, planned for, and resourced within contemporary defense organizations.

3.1 Overview of the Empirical Sample

The empirical sample includes documents of various institutional

and thematic types, categorized for analytical clarity. The dataset comprises:

- Alliance-level strategic concepts and policy guidelines, including NATO's Artificial Intelligence Strategy and the 2022 Strategic Concept [2].
- National defense strategies, cyber strategies, and AI strategies published by allied states between 2018 and 2024.
- Capability development plans, workforce planning documents, and resource management frameworks relevant to AI and cyber operations.

Documents were coded according to institutional level (alliance-level versus national), primary thematic focus (defense strategy, cyber strategy, AI strategy, or resource planning document), and the explicit treatment of resource allocation mechanisms. This classification enabled cross-sectional and comparative analysis of how AI-driven cyber capabilities are framed, prioritized, and integrated into existing planning frameworks. All documents underwent structured qualitative content analysis, ensuring consistency with the analytical framework established in the methodology section.

3.2 Recognition of Cyber Capabilities and Artificial Intelligence

The first set of findings concerns the degree to which cyber capabilities and AI are recognized in defense planning documents. Quantitative content analysis indicates that 78% of analyzed documents explicitly reference cyber capabilities as a core component of contemporary defense posture. These references encompass cyber defense, cyber operations, resilience of digital infrastructure, and protection of command-and-control systems.

In contrast, only 41% of documents explicitly reference artificial intelligence in the context of resource planning. While AI is frequently acknowledged as a strategically important emerging technology, it remains less consistently embedded within formal planning and allocation frameworks [10]. This discrepancy highlights a structural lag between technological discourse and institutional planning practice, indicating that AI is often treated as a future-oriented or enabling capability rather than an immediate driver of resource allocation decisions.

The gap between general recognition and resource-specific integration underscores the uneven treatment of AI across defense institutions and reveals constraints in translating strategic rhetoric into practical planning measures.

Table 1. Frequency of Cyber and AI References in Defense Planning Documents (2018–2024)

Analytical Category	Share of Documents (%)
Cyber capabilities referenced as core defense component	78%
Artificial intelligence referenced at strategic level	56%
Artificial intelligence referenced within resource planning context	41%

3.3 Comparative Analysis of Defense Planning Models

To complement the document-based findings, a brief comparative perspective can be observed across three representative defense planning models: the United States, the United Kingdom, and Estonia. These cases illustrate how institutional size and strategic priorities shape the integration of AI-driven cyber capabilities into defense resource planning [11].

In the United States, planning frameworks emphasize large-scale technological investment and institutional structures dedicated to AI capability development. The United Kingdom places stronger emphasis on governance mechanisms, responsible AI integration, and coordination within existing defense institutions. Estonia, by contrast, prioritizes cyber resilience, interoperability with NATO allies, and the integration of national digital infrastructure into defense planning. This comparison indicates that although all three defense institutions recognize the strategic importance of AI-enabled cyber capabilities, their resource planning approaches vary according to institutional capacity, governance models, and national security priorities [11].

3.4 Distribution of AI-Related Resource Considerations

Second key finding concerns the distribution of AI-related resource considerations across planning domains. All AI-related references were coded into three primary resource categories: human resources, technological investment, and doctrinal or organizational adaptation.

Human resource development and training constitute the largest proportion, accounting for 46% of AI-related references. These references emphasize the need for specialized skills in data science, machine learning, cyber operations, and system integration. Common challenges include talent shortages, competition with the private sector,

and the necessity for continuous professional education [10]. These findings highlight that workforce constraints, rather than technological limitations alone, represent a primary bottleneck in operationalizing AI-driven cyber capabilities.

Technological investment accounts for 34% of AI-related references. Most of these references focus on computational infrastructure, secure networks, data availability, and software development environments. While these references frequently emphasize modernization needs, they rarely include explicit discussions of lifecycle management, sustainability, or long-term operational costs. This limited treatment suggests that defense institutions recognize technology as critical but may underestimate the continuous resourcing required to maintain AI operational readiness [10].

Doctrinal and organizational adaptation represents the smallest category, at 20%. This suggests that while AI-driven cyber capabilities are acknowledged, their implications for command structures, planning cycles, and institutional governance remain underdeveloped within formal documents. This is indicative of a persistent institutional lag between technological adoption and organizational transformation [11].

Table 2. Distribution of AI-Related Resource References by Planning Domain

Resource Planning Domain	Share of AI-Related References (%)
Human resources and training	46%
Technological investment and infrastructure	34%
Doctrinal and organizational adaptation	20%

3.5 Budgetary Integration and Financial Planning

One of the most significant findings concerns the limited integration of AI-driven cyber capabilities into budgetary planning frameworks. Only 29% of analyzed documents present explicit financial allocation mechanisms for AI-enabled cyber capabilities. In most cases, AI investments are embedded within broader digital modernization or innovation programs, without dedicated budget lines or measurable funding commitments [10].

National defense strategies frequently describe AI as a priority yet seldom provide detailed cost models or resource plans. Even at the alliance level, where documents offer guidance on capability development, funding articulation is often aspirational rather than operationally binding. This observation

underscores a structural limitation: without clear financial mechanisms, AI-driven cyber capabilities cannot be reliably integrated into long-term operational planning or workforce development initiatives [10].

Table 3. Explicit Budgetary Integration of AI-Driven Cyber Capabilities

Planning Characteristic	Share of Documents (%)
Dedicated AI-related budget lines	29%
AI embedded in general modernization programs	61%
No identifiable financial mechanisms for AI	39%

3.6 Comparative Analysis: Institutions With and Without AI Strategies

Comparative analysis reveals substantial differences between institutions with dedicated AI strategies and those without. Institutions with formal AI strategies demonstrate higher levels of integration between cyber capabilities and resource planning indicators, particularly in human capital management and capability development [8].

In these institutions, AI-driven capabilities are more likely to be linked to workforce planning, training pipelines, and institutional learning frameworks. On average, content analysis shows that documents from these institutions contain 35% more references to coordinated resource planning than documents from institutions without formal AI strategies. This finding suggests that dedicated AI strategies act as institutional catalysts, promoting coherent integration of AI into defense planning processes [8].

By contrast, institutions lacking formal AI strategies address AI in fragmented or ad hoc ways, often limiting it to research and development contexts, without linking capabilities to workforce planning or budgetary allocation. This demonstrates a structural divergence in planning approaches and highlights the role of strategic prioritization in shaping resource management practice [8].

Table 4. Comparison of Planning Integration in Institutions With and Without Dedicated AI Strategies

Planning Indicator	Institutions with AI Strategy	Institutions without AI Strategy
Coordinated workforce planning references	High	Low
Explicit linkage between AI and cyber capabilities	Present	Fragmented

Planning Indicator	Institutions with AI Strategy	Institutions without AI Strategy
Integration into resource planning cycles	Systematic	Ad hoc
Average density of AI-related planning references	+35%	Baseline

3.7 Alignment Between Capability Development and Workforce Planning

Another notable result concerns the alignment between AI-driven capability development objectives and workforce planning models. Only 38% of documents demonstrate explicit alignment between capability goals and human resource planning. Misalignment is particularly pronounced in documents that emphasize technological modernization without corresponding investments in training, recruitment, or retention [34].

Institutions that explicitly link AI-driven cyber capabilities to workforce planning exhibit more coherent architectures. These documents outline skill requirements, training timelines, and career development pathways, reflecting a socio-technical understanding of AI rather than a purely technological perspective. The findings emphasize that human capital constraints are critical in operationalizing AI-driven capabilities and that technological investment alone is insufficient [46].

3.8 Temporal Patterns and Planning Evolution

Process tracing across successive documents reveals incremental, rather than transformative, change in integrating AI-driven capabilities into resource planning. Early documents (2018–2020) tend to describe AI as exploratory or experimental, with minimal resource implications. Recent documents (2021–2024) reflect increasing recognition of AI's operational relevance, but formal planning frameworks often lag behind strategic rhetoric [2].

This temporal pattern suggests that defense institutions are in a transitional phase, gradually moving from conceptual acknowledgment toward systematic integration. However, legacy planning models, bureaucratic inertia, and competing resource priorities constrain rapid adoption [31].

3.9 Summary of Empirical Findings

The results indicate that while cyber capabilities are now embedded within defense planning, AI-driven elements remain partially and unevenly integrated. Key findings include:

- A substantial gap between

recognition of cyber capabilities and formal integration of AI into resource planning [2].

- A disproportionate focus on human resources, highlighting workforce shortages as a primary constraint [34].
- Limited and inconsistent budgetary mechanisms for AI-driven capabilities [6].
- Higher levels of planning integration in institutions with dedicated AI strategies [8].
- Persistent misalignment between capability development objectives and workforce planning models [46].
- Incremental and uneven temporal adaptation, reflecting institutional lag [31].

These findings provide a robust empirical foundation for the subsequent discussion, highlighting structural, technological, and human factors that influence the operationalization of AI-enabled cyber capabilities. They underscore that integrating AI into defense planning is a multifaceted challenge requiring coordinated adaptation across personnel, technology, and institutional processes [2].

4. DISCUSSION

The findings of this study reveal a pronounced imbalance between the widespread strategic recognition of cyber capabilities and the comparatively limited institutional integration of artificial intelligence into defense resource planning frameworks. While cyber operations have become a routine and formalized component of contemporary defense strategies, AI-driven cyber capabilities remain insufficiently embedded in the mechanisms that govern resource allocation, workforce planning, budgeting, and capability development [2]. This imbalance is not merely a technical lag but reflects deeper structural and organizational dynamics within defense planning systems, highlighting the need for a holistic understanding of the interaction between technology, human capital, and institutional processes [31].

4.1 Institutional Inertia and Planning Path Dependencies

A central explanation for the observed gap lies in the institutional inertia inherent in defense planning and resource management structures. Defense institutions are traditionally shaped by long-term planning cycles, established capability taxonomies, and procurement systems designed around relatively stable technological trajectories [6]. These characteristics favor incremental adaptation within existing domains rather than rapid integration of disruptive technologies. As a result, AI-driven cyber

capabilities, which are inherently cross-cutting and experimental, face structural obstacles to full institutional integration [34].

Cyber capabilities, despite their relatively recent emergence, have undergone a process of institutional normalization over the past two decades. Cyber defense is now incorporated into military doctrine, organizational structures, and resource allocation models, enabling it to be treated as a distinct and recognizable capability domain with associated budget lines, personnel categories, and planning assumptions [46]. AI, in contrast, challenges these established logics. AI-driven cyber capabilities cut across traditional capability boundaries, blending software, data, human expertise, and organizational processes, thereby complicating their integration into planning systems organized around discrete domains [31]. This cross-cutting nature explains why AI is frequently acknowledged at the strategic level but remains framed as experimental, enabling, or future-oriented rather than as a driver of immediate resource allocation decisions [2].

This evidence corrects a common assumption in defense studies literature that technological maturity is the primary obstacle to AI adoption. Instead, institutional path dependencies, rigid governance mechanisms, and planning inertia appear to be decisive factors shaping the treatment of AI-driven capabilities in resource management frameworks [6]. The results demonstrate that even in technologically advanced institutions, strategic recognition does not automatically translate into operational integration [34].

4.2 Strategic Recognition versus Operationalization

A recurring theme across the analyzed documents is the disparity between strategic recognition and operational integration. Many strategies emphasize the transformative potential of AI and cyber capabilities in broad terms, framing them as critical to future military effectiveness and deterrence. However, this rhetorical emphasis is not consistently matched by adjustments in resource planning mechanisms [2].

Only a minority of documents translate AI-related strategic priorities into concrete planning instruments, such as workforce development programs, budgetary mechanisms, or capability lifecycle models [31]. The gap between strategic ambition and operationalization highlights a structural disconnect that limits the realization of AI-driven capabilities. Defense resource management relies on the alignment of financial, human, and organizational resources over time; without such alignment, strategic recognition alone

cannot ensure effective capability development [6].

From a governance perspective, this disconnect illustrates that AI integration is fundamentally a question of institutional coordination. Documents that frame AI primarily as a strategic aspiration or enabling tool risk underinvestment, fragmented implementation, and the creation of capability gaps [34]. The findings underscore that strategic recognition must be accompanied by operational mechanisms that integrate AI into formal planning cycles [46].

4.3 Human Capital as the Primary Constraint

One of the most consequential findings is the predominance of human resource considerations in AI-related planning discourse. Nearly half of all AI-related references concern workforce development, training, and skill acquisition, emphasizing the centrality of human capital in operationalizing AI-driven cyber capabilities [31]. This finding challenges narratives that prioritize technological procurement or financial investment as the primary enablers of AI integration [2].

While advanced algorithms and computational infrastructure are necessary, they are insufficient without personnel capable of developing, deploying, and maintaining AI-driven systems. Defense organizations face intense competition with the private sector for AI talent, compounded by rigid personnel systems and limited career incentives [34]. Human capital emerges not only as a technical requirement but as a socio-technical enabler, reflecting the complex interplay between skills, institutional knowledge, and interdisciplinary expertise [46].

This emphasis on human resources also indicates a conceptual shift in understanding cyber capabilities. AI-driven capabilities are increasingly treated as socio-technical systems rather than purely technical assets [31]. Effective integration requires continuous learning, institutional knowledge retention, and collaboration across multiple professional domains. However, despite this recognition, workforce planning mechanisms remain inadequately aligned with capability development objectives. Documents frequently acknowledge skill gaps without articulating pathways for recruitment, retention, and professional development, revealing a persistent institutional shortfall in addressing the human dimension [6].

4.4 Budgetary Ambiguity and Financial Governance

A related challenge lies in budgetary planning. Only a small proportion of documents provide explicit financial allocations for AI-

driven cyber capabilities, with most investments embedded in broader modernization programs [2]. This budgetary ambiguity undermines long-term planning by obscuring the true costs of AI integration, including maintenance, training, and upgrades [31].

Without dedicated financial mechanisms, AI initiatives are vulnerable to shifting priorities and short-term fiscal pressures. The lack of transparency complicates accountability and performance evaluation, as AI-related expenditures are dispersed across multiple programs [34]. The results highlight the need for financial governance models capable of capturing the iterative and dynamic nature of AI development, ensuring that funding aligns with operational requirements and workforce needs [46].

4.5 Doctrinal and Organizational Adaptation

The study finds limited attention to doctrinal and organizational adaptation. While human and technological resources receive considerable focus, the implications of AI-driven cyber capabilities for command structures, decision-making, and institutional governance remain underdeveloped [6].

AI-enabled cyber capabilities have the potential to alter operational tempo, authority distribution, and risk management practices. Without corresponding doctrinal changes, these capabilities may create friction, reduce efficiency, or fail to realize their full operational potential [31]. The observed low level of organizational adaptation also reflects uncertainties regarding human–machine interaction, trust, and accountability in automated systems [2]. Delayed adaptation risks misalignment between technological capabilities and institutional readiness.

This gap underscores that effective AI integration requires coordinated change across technology, personnel, and institutional structures, aligning with broader research on military innovation as a socio-technical and organizational process rather than purely technological advancement [46].

4.6 Comparative Insights and Institutional Learning

Comparative analysis between institutions with and without dedicated AI strategies provides further insight. Institutions with formal AI strategies demonstrate higher levels of integration across workforce development, capability alignment, and resource planning [2]. These strategies function not only as symbolic statements but also as coordination mechanisms, reducing fragmentation and promoting coherent planning across domains.

Institutions lacking formal AI strategies tend to address AI capabilities in ad hoc or research-limited contexts, highlighting the importance of governance frameworks and institutional learning in enabling effective resource management [31]. The presence of an AI strategy appears to facilitate the translation of strategic recognition into concrete operational and financial planning measures, bridging the gap between aspiration and implementation.

4.7 Implications for Defense Resource Management Theory

The findings challenge traditional linear models of defense resource management, which assume direct relationships between strategic priorities, resource allocation, and capability outcomes [34]. AI-driven cyber capabilities disrupt this linearity by introducing dependencies across multiple dimensions, including skills, organizational adaptation, and governance processes.

Human capital emerges as a central constraint, and institutional adaptation is essential for operationalizing capabilities [46]. These findings advance a holistic understanding of defense resource planning that incorporates technological, human, and organizational dimensions, particularly in contexts of rapid technological change.

4.8 Policy and Practical Implications

From a policy standpoint, the study suggests that defense planners must move beyond symbolic recognition of AI and toward systematic integration in resource planning frameworks [2]. This requires adjustments to planning cycles, budgeting, personnel management, and governance structures to accommodate the interdisciplinary and iterative nature of AI-driven cyber capabilities.

Practically, investment in workforce development, professional education, and institutional learning may yield greater returns than technology procurement alone [31]. Organizations that neglect human capital risk underutilizing AI technologies and exacerbating capability gaps. Coordinated attention to human, technological, and organizational resources is essential to translating strategic recognition into operational capability.

4.9 Synthesis

In summary, the discussion demonstrates that AI integration in defense resource planning is constrained less by technological feasibility than by institutional readiness [34]. The imbalance between recognition and implementation reflects planning practices, organizational inertia, and

governance challenges. The study empirically grounds these constraints in defense planning documents, providing a corrective to technology-centric narratives of military innovation [46]. By framing AI integration as a resource management challenge that spans human, technological, and organizational dimensions, this discussion establishes the basis for the study's conclusions and highlights pathways for more effective planning, funding, and operationalization of AI-driven cyber capabilities [2].

5. CONCLUSIONS

This study examined the integration of AI-driven cyber capabilities into defense resource planning, analyzing 32 strategic and policy documents issued between 2018 and 2024 by NATO, the European Union, and selected national defense institutions. The findings demonstrate that while cyber capabilities have become institutionally embedded within contemporary defense frameworks, AI-driven cyber capabilities remain partially and unevenly integrated into formal resource planning processes [2].

5.1 Empirical Findings

The analysis yields several concrete empirical results. First, while 78% of analyzed documents reference cyber capabilities as a core defense component, only 41% address artificial intelligence within a resource planning context, revealing a persistent structural gap between strategic discourse and operational planning practice [6]. Second, human resource development constitutes the largest share of AI-related planning references (46%), identifying workforce constraints — rather than technological limitations — as the primary bottleneck in operationalizing AI-driven capabilities [31]. Third, only 29% of documents present explicit financial allocation mechanisms for AI-enabled cyber capabilities, with most investments subsumed within broader digital modernization programs, undermining long-term planning coherence [34]. Fourth, institutions with dedicated AI strategies demonstrate 35% higher density of coordinated resource planning references compared to those without, confirming that formal AI governance frameworks function as institutional catalysts for integration [46].

The comparative analysis of three representative defense planning models — the United States, the United Kingdom, and Estonia — further illustrates how institutional capacity and strategic priorities shape integration outcomes. The United States prioritizes large-

scale technological investment and dedicated institutional structures for AI capability development. The United Kingdom emphasizes governance mechanisms and responsible AI integration within existing defense frameworks. Estonia focuses on cyber resilience and interoperability with NATO allies, leveraging its national digital infrastructure as a foundation for defense planning [2]. Despite these differences, all three institutions share a common challenge: translating high-level strategic recognition of AI into concrete, resource-backed operational planning.

5.2 Theoretical Implications

From a theoretical perspective, the findings challenge traditional linear models of defense resource management that assume direct causal relationships between strategic priorities, resource allocation, and capability outcomes [31]. AI-driven cyber capabilities disrupt this linearity by introducing cross-domain dependencies spanning human expertise, organizational adaptation, and governance processes [46]. The study advances a socio-technical understanding of defense capability development, demonstrating that AI-enabled systems cannot be treated as discrete technological assets but must be planned as integrated systems requiring continuous human, institutional, and financial investment [2]. Institutional inertia and planning path dependencies — rather than technological immaturity — emerge as the decisive constraints on effective AI integration, offering a corrective to technology-centric narratives of military innovation [6].

5.3 Practical Implications for Policymakers

For defense planners and policymakers, the study identifies three priority areas. First, AI-driven cyber capabilities must be explicitly embedded within resource planning instruments, including dedicated budget lines, workforce development programs, and capability lifecycle models, rather than subsumed within generic modernization budgets [34]. Second, personnel systems must be reformed to attract, develop, and retain specialized AI and cyber talent, with structured career pathways and competitive incentives that address the gap with the private sector [31]. Third, doctrinal and organizational adaptation must accompany technological investment; without corresponding changes to command structures, planning cycles, and governance frameworks, AI capabilities risk remaining operationally underutilized [46].

5.4 Limitations and Future Research

This study relied exclusively on publicly available documents, which limits insight into classified planning processes and internal resource decisions [2]. The qualitative methodology prioritizes the identification of structural patterns over quantitative measurement of capability outcomes. Future research could extend the comparative scope to additional NATO and non-NATO defense institutions, incorporate empirical data from operational planning cycles, and examine the resource management dimensions of AI integration across other emerging domains such as autonomous systems and space capabilities [6].

In conclusion, the research demonstrates that the effective integration of AI-driven cyber capabilities depends less on technological readiness than on the institutional capacity of defense organizations to adapt their resource planning frameworks [31]. Strategic ambition without operationalization, technological capability without human capital, and investment without governance are individually insufficient to generate sustainable military advantage. Coordinated adaptation across personnel systems, financial governance, and institutional structures remains the central prerequisite for translating AI's strategic potential into operational capability and long-term defense resilience [46].

REFERENCES

[1] M. Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Oxford, UK: Future of Humanity Institute, University of Oxford, 2018. https://arxiv.org/pdf/1802.07228v2

[2] North Atlantic Treaty Organization, *Artificial Intelligence Strategy*. Brussels, 2021. https://www.nato.int/cps/en/natohq/official_texts_187617.htm

[3] North Atlantic Treaty Organization, *NATO 2022 Strategic Concept*. Madrid, 2022. https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf

[4] European Commission, *Cybersecurity Strategy for the Digital Decade*. Brussels, 2020.

[5] European Commission, *Coordinated Plan on Artificial Intelligence – 2021 Review*. Brussels, 2021.

[6] U.S. Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*. Washington, DC, 2018.

[7] U.S. Department of Defense, *Department of Defense Cyber Strategy*. Washington, DC, 2023.

[8] M. N. Schmitt (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

[9] T. Rid and B. Buchanan, "Attributing cyber attacks," *Journal of Strategic Studies*, vol. 38, no. 1–2, pp. 4–37, 2015.

[10] National Security Commission on Artificial Intelligence, *Final Report*. Washington, DC, 2021.

[11] J. R. Lindsay, "Stuxnet and the limits of cyber warfare," *Security Studies*, vol. 22, no. 3, pp. 365–404, 2013.

[12] B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford: Oxford University Press, 2017.

[13] M. Libicki, *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation, 2009.

[14] J. Gartzke, "The myth of cyberwar," *International Security*, vol. 38, no. 2, pp. 41–73, 2013.

[15] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.

[16] M. C. Horowitz, "Artificial intelligence, international competition, and the balance of power," *Texas National Security Review*, vol. 1, no. 3, pp. 36–57, 2018.

[17] M. C. Horowitz, G. C. Allen, E. Saravalle, A. Cho, K. Frederick, and P. Scharre, *Artificial Intelligence and International Security*. Washington, DC, USA: Center for a New American Security (CNAS), 2018.

[18] K. Payne, *I, Warbot: The Dawn of Artificially Intelligent Conflict*. London: Hurst Publishers, 2021.

[19] S. Russell, *Human Compatible: Artificial Intelligence and the Problem of Control*. New York, NY, USA: Viking, 2019.

[20] N. Bostrom, *Superintelligence: Paths, Dangers, Strategies*. Oxford, UK: Oxford University Press, 2014.

[21] R. A. Clarke and R. K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY, USA: HarperCollins, 2010.

[22] NATO Cooperative Cyber Defence Centre of Excellence, *Annual Report on Cyber Defence*. Tallinn, 2021.

[23] K. Geers, Ed., *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2015.

[24] RAND Corporation, *Artificial Intelligence and National Security*. Santa Monica, CA, USA: RAND Corporation, 2020.

[25] G. Allen and T. Chan, *Artificial Intelligence and National Security*.

Belfer Center, Harvard University, 2017.

[26] P. Scharre, *Army of None: Autonomous Weapons and the Future of War*. New York: W.W. Norton, 2018.

[27] United Nations, *The Age of Digital Interdependence*. UN High-Level Panel Report, 2019.

[28] OECD, *Artificial Intelligence in Society*. Paris: OECD Publishing, 2019.

[29] M. L. Cummings, H. M. Roff, K. Cukier, J. Parakilas, and H. Bryce, *Artificial Intelligence and International Affairs: Disruption Anticipated*. London, UK: Chatham House (The Royal Institute of International Affairs), 2018.

[30] M. C. Horowitz and L. Kahn, "Artificial intelligence and the future of warfare," *Foreign Affairs*, vol. 99, no. 6, 2020.

[31] M. Taddeo and L. Floridi, "How AI can be a force for good in cybersecurity," *Science*, vol. 361, no. 6404, pp. 751–752, Aug. 2018. https://doi.org/10.1126/science.aat5991

[32] L. Floridi et al., "AI4People—An ethical framework for a good AI society," *Minds and Machines*, vol. 28, pp. 689–707, 2018.

[33] D. E. Denning, *Information Warfare and Security*. Boston, MA, USA: Addison-Wesley, 1999.

[34] C. C. Demchak and P. J. Dombrowski, "Rise of a cybered Westphalian age," *Strategic Studies Quarterly*, vol. 5, no. 1, pp. 31–62, 2011.

[35] E. Kello, "The meaning of the cyber revolution," *International Security*, vol. 38, no. 2, pp. 7–40, 2013.

[36] J. S. Nye Jr., "Deterrence and dissuasion in cyberspace," *International Security*, vol. 41, no. 3, pp. 44–71, 2017. https://doi.org/10.1162/ISEC_a_00266

[37] M. J. Mazarr, J. S. Blake, A. Casey, T. McDonald, S. Pezard, and M. Spirtas, *Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives*. Santa Monica, CA, USA: RAND Corporation, 2018.

[38] J. J. Healey, *A Fierce Domain: Conflict in Cyberspace, 1986–2012*. Vienna, VA, USA: Cyber Conflict Studies Association, 2013.

[39] P. W. Singer, *Wired for War*. New York: Penguin Press, 2009.

[40] G. C. Allen and T. Chan, *Artificial Intelligence and National Security*. Cambridge, MA, USA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2017.

[41] World Economic Forum, *Global Risks Report*. Geneva, 2023.

[42] NATO, *Emerging and Disruptive Technologies Strategy*. Brussels,

2021.

[43] A. Kaplan, S. Brannen, and E. Bates, *Global Security Forum 2020: A New Era for U.S. Alliances*. Washington, DC, USA: Center for Strategic and International Studies (CSIS), 2020.

[44] IISS, *The Military Balance*. London: International Institute for Strategic Studies, 2022.

[45] SIPRI, *Artificial Intelligence, Strategic Stability and Nuclear Risk*. Stockholm, 2020.

[46] C. Coker, "Artificial intelligence and the future of war," *Stratagem Journal of Strategic and Military Studies*, vol. 2, no. 1, pp. 55–60, 2019. https://doi.org/10.31374/sjms.26

[47] United Nations Institute for Disarmament Research (UNIDIR), *The Weaponization of Increasingly Autonomous Technologies*. Geneva, 2017.

ARTIFICIAL INTELLIGENCE: IMPLICATIONS ON MILITARY DECISION MAKING

Florin OGÎGĂU-NEAMȚIU[1]

The Regional Department of Defense Resources Management Studies (DRESMARA) / "Carol I" National Defense University, Brasov, Romania

Artificial intelligence is fundamentally transforming military decision-making processes across tactical, operational, and strategic levels. This paper examines the multiple implications of AI on military command and control systems, with particular focus on how AI performs across three distinct decision environments: certainty, risk, and uncertainty. Through analysis of military decision theory, AI architectures, and operational applications, this research try to demonstrate that while AI offers unprecedented capabilities in conditions of certainty and calculable risk, it faces significant limitations in the uncertain environments.

Key words: *Artificial intelligence, military environments, risk, war domains, autonomous systems*

1. INTRODUCTION

The rapid advancement of artificial intelligence technologies revealed a new era of military capabilities that extend far beyond traditional weapon systems. From autonomous systems that identify and track targets to predictive analytics that forecast adversary actions, AI systems are increasingly embedded in decisions that determine the course of actions and the allocation of resources. This transformation raises fundamental questions about the nature of military decision-making itself, the role of human commanders in an age of intelligent machines, and the ethical implications of delegating lethal force decisions to automated systems.

Military decision-making has traditionally been understood as a complex cognitive process occurring in what Clausewitz termed the "fog of war" — an environment characterized by incomplete information, time pressure, adversarial deception, and life-threatening stakes. Commanders must make choices based on fragmentary intelligence,

[1] ORCID: N/A, e-mail: florinbvmail@gmail.com

anticipate adversary actions, coordinate complex operations across multiple domains, and accept moral responsibility for outcomes including casualties and destruction. The introduction of AI into this domain represents not merely an enhancement of existing capabilities but an essential shift in how military decisions are formulated, executed, and evaluated.

This paper employs conceptual analysis as its primary methodological approach, drawing on secondary sources including military doctrine, academic literature and published case studies to examine the implications of AI on military decision-making. Rather than generating new empirical data, the research synthesizes existing theoretical frameworks — including decision theory, AI architecture studies, and legal and ethical scholarship — in order to construct an integrated analytical perspective. This approach is particularly suited to an emerging domain where empirical data from live operational environments remains classified or limited, and where conceptual clarity is a prerequisite for sound policy and practice. The limitations of this approach — most notably the reliance on open-source and publicly available materials — simultaneously suggest productive avenues for future research, including empirical studies of AI-assisted decision-making in live military exercises, comparative analysis of national AI defence strategies, and longitudinal assessment of autonomous system performance under operational conditions.

2. MILITARY DECISION-MAKING THEORY

2.1 Classical Military Decision-Making Models

Military decision-making has evolved through centuries of warfare, producing distinct theoretical frameworks that have created the modern command and control systems. Understanding these classical models provides essential context for evaluating how AI impacts military decision processes.

Clausewitz theory emphasizes the fundamental uncertainty and unpredictability of warfare. Carl von Clausewitz's concept of the "fog of war" [1] describes the inherent information deficit commanders face—incomplete intelligence, unreliable communications, and the inability to fully comprehend the battlefield situation. His notion of "friction" captures the countless factors that cause military operations to deviate from plans, from equipment failures to human error or enemy action. Clausewitz argued that while scientific principles apply to certain military problems, warfare ultimately requires genius, intuition,

and the ability to instantly grasp the essence of a situation. This emphasis on irreducible uncertainty and the necessity of human judgment stands in tension with AI systems which are based on pattern recognition and statistical prediction.

Boyd's OODA Loop [2] represents a more recent framework that has profoundly influenced modern military thinking. Colonel John Boyd proposed that decision-making in conflict follows a continuous cycle of Observe, Orient, Decide, and Act. The entity that can complete this cycle faster than their adversary gains a decisive advantage, operating inside the opponent's decision loop and creating situations the enemy cannot comprehend or counter in time. The Orient phase, where information is synthesized with experience, culture, and theoretical models to create understanding, represents the most complex and crucial stage. Boyd's framework suggests that speed and adaptability matter more than perfect information or optimal calculations, raising questions about whether AI acceleration of the OODA loop compensates for potential degradation of the orientation process.

Military Decision-Making Process (MDMP) [3] represents the institutionalized approach used by military staffs to analyze problems and develop operational plans. The seven-step process includes receipt of mission, mission analysis, course of action development, course of action analysis (wargaming), course of action comparison, course of action approval, and orders production. This deliberate, analytical approach emphasizes systematic consideration of factors, constraints, and alternatives. MDMP assumes sufficient time for thorough analysis and operates primarily in conditions of risk rather than pure uncertainty, as commanders develop estimates of adversary capabilities and intentions. The structured methodology facilitates staff coordination and commander decision-making but can be time-consuming and may not accommodate rapid adaptation to changing circumstances.

Rapid Decision-Making (RDM) and Intuitive Decision-Making [4] provide alternatives to deliberate analysis in time-constrained situations. Recognition-primed decision-making [5], identified by cognitive psychologist Gary Klein through study of experienced commanders, describes how experts rapidly assess situations by pattern matching to prior experiences, generating a single course of action that they mentally simulate rather than comparing multiple alternatives. This intuitive approach allows rapid decisions based on accumulated expertise but depends critically on relevant experience and can fail when

situations differ in crucial but non-obvious ways from familiar patterns.

2.2 Decision Environments: Certainty, Risk, and Uncertainty

A critical framework for understanding AI's role in military decision-making involves distinguishing between three fundamentally different decision environments: certainty, risk, and uncertainty. These categories, rooted in classical decision theory and applied particularly to military contexts, define the nature of information available to decision-makers and the applicability of different analytical approaches.

Decisions under certainty occur when the outcomes of all alternatives are known with complete accuracy. In military operations, such conditions are rare but do exist in constrained scenarios such as ballistic trajectory calculations where physical laws determine outcomes precisely, known terrain navigation where geographic information is complete and accurate, established logistics calculations with fixed transportation networks and resources, and mechanical system operations with deterministic behaviour. In these environments, optimal decisions can be computed algorithmically without ambiguity.

Decisions under risk involve situations where multiple outcomes are possible, but their probabilities can be estimated with reasonable accuracy based on historical data, statistical models, or established patterns. Military decisions under risk include equipment failure predictions based on maintenance histories, weather effects on operations estimated from meteorological models, detection probabilities for different sensor configurations, and casualty estimates for various tactical approaches. Risk-based decisions allow expected value to be calculated, although the exact final outcome remains uncertain.

Decisions under uncertainty characterize situations where neither the full range of possible outcomes nor their probabilities are reliably known. This condition dominates military operations due to adversarial intelligence where opponents actively conceal intentions and capabilities, adaptive adversary behaviour where enemies learn and modify tactics, novel situations without historical precedents, and deception operations designed to mislead decision-makers. The "radical uncertainty" of warfare emerges from the creative, intelligent opposition inherent in armed conflict. Unlike natural phenomena that follow discoverable laws, human adversaries deliberately violate expectations and exploit predictable patterns in their opponents' behavior.

This distinction between certainty, risk, and uncertainty provides a crucial lens for

evaluating AI capabilities in military applications, and underpins the analytical structure of the sections that follow [6].

3. AI BASED DECISION MAKING

3.1 Systems in Conditions of Certainty

In certainty-domain operations — where outcomes follow deterministically from known inputs — AI systems deliver their strongest and most reliable performance, as the following examples illustrate.

Fire control and ballistic computation exemplifies AI application under certainty. Modern artillery, naval guns, and precision-guided munitions employ AI-enhanced targeting systems that calculate trajectories accounting for numerous variables including projectile ballistics, atmospheric density and wind patterns, earth rotation (Coriolis effect), temperature effects on propellant, barrel wear characteristics, and target motion predictions. The M982 Excalibur guided artillery projectile achieves error probable of less than 2 meters [7] at maximum range through GPS guidance and trajectory optimization algorithms. The physics governing these calculations is deterministic—given accurate input measurements, the optimal firing solution can be computed with precision extremely difficult to perform by manual calculation. AI systems process sensor data, environmental measurements, and ballistic models in milliseconds, enabling real time responsive fires.

Navigation and route planning in known terrain with functioning positioning systems represents another certainty domain where AI excels. Military logistics and tactical movement require optimal route selection considering terrain trafficability, obstacle locations, enemy threat zones, fuel consumption, and time constraints. Graph algorithms like Dijkstra's shortest path search efficiently optimal routes through complex terrain networks. The Warfighter Machine Interface (WMI) [8] program integrates AI route planning that considers real-time intelligence, known minefields, bridge weight limits, and force positioning to generate movement plans for armored formations. In urban terrain, building layouts and street networks permit algorithmic path planning for infantry movements and unmanned ground vehicle navigation.

Communications network management benefits from AI optimization when network topology and performance characteristics are known. Military tactical networks face challenges of limited bandwidth, intermittent connectivity, and electromagnetic interference.

AI systems can dynamically route traffic, allocate bandwidth, implement Quality of Service priorities, and configure network parameters to maintain connectivity. The WIN-T (Warfighter Information Network-Tactical)[9] system employs automated network management that reroutes traffic around degraded links and optimizes configurations without manual intervention. Given complete knowledge of network state, these optimizations follow from established algorithms.

Maintenance and logistics optimization for equipment with comprehensive sensor monitoring enables predictive maintenance and inventory optimization. The F-35 fighter's Autonomic Logistics Information System (ALIS) [10] collects extensive performance data from aircraft systems, analyses component health, predicts failures, and automatically orders replacement parts. When mechanical failure modes are well-characterized and sensor coverage is adequate, AI can reliably detect degradation patterns and schedule maintenance optimally. Supply chain optimization algorithms minimize inventory costs while ensuring availability, computing optimal stock levels and distribution given deterministic demand forecasts and transportation networks.

Across all these applications, the shared condition is deterministic input-output relationships that allow AI to outperform humans in speed, precision, and endurance.

Fig. 1 Vehicle Commander (VC) Warfighter-Machine Interface (WMI), consisting of a 180o field-of-view banner across the top, a 60o field-of-view window on the left hand side, and an overhead map on the right hand side. www.researchgate.net

3.2. Systems in Conditions of Risk

Where outcomes are probabilistic but statistically estimable — the risk domain — AI systems trained on historical data provide substantial planning and operational value [11].

Intelligence analysis and pattern recognition represents a major application of AI under risk. Intelligence analysts must process vast quantities of data from signals intelligence, imagery, human intelligence, and open sources to identify threats, assess enemy capabilities, and predict adversary actions. AI systems excel at certain aspects of this challenge, particularly pattern recognition in structured data.

Project Maven, initiated by the U.S. Department of Defense in 2017, applies computer vision to analyze full-motion video from drones and other ISR platforms [10]. The system identifies objects of interest including vehicles, buildings, and personnel with accuracy exceeding 90% under good conditions. By automating the laborious task of scanning hundreds of hours of video, AI frees analysts to focus on interpretation and assessment. The system operates under risk rather than certainty because detection depends on probabilistic factors including image resolution, lighting conditions, object orientation, and environmental clutter. Training on large datasets of labelled imagery enables the system to learn statistical patterns distinguishing targets from backgrounds, though performance degrades when conditions differ significantly from training data.

Signals intelligence benefits from machine learning for communications intercept processing, speaker identification, and language translation. Neural machine translation [12] achieves near-human accuracy for high-resource language pairs, enabling rapid processing of foreign communications. Pattern recognition algorithms can identify communications networks, correlate signals to platforms, and detect anomalies indicating new capabilities. These applications work well when processing languages and protocols represented in training data, with performance degrading for rare languages, encrypted content, or novel communications systems.

Threat assessment and predictive analysis employ probabilistic models to estimate adversary capabilities and forecast actions. Bayesian networks can model relationships between observable indicators and underlying threats, updating probability estimates as new intelligence arrives. For example, observing increased fuel deliveries, vehicle movements, and troop concentrations might raise probability estimates that an adversary is preparing an offensive. Time series analysis of historical attack patterns can identify temporal correlations, geographic preferences, and seasonal variations useful for predicting future attacks. AI systems have been employed to forecast IED placement [13], predict areas of instability, and assess terrorist threats based on historical patterns.

However, these predictive systems face significant limitations in military contexts. Adversaries deliberately violate patterns when they become apparent. A predictable enemy is a defeated enemy, so capable adversaries study their opponents' intelligence collection and analysis methods, adapting to evade detection and exploit biases. The baseline assumption of statistical learning—that future data will resemble training

data—is systematically violated by intelligent adversaries. This creates fundamental questions about the reliability of AI threat predictions in contested environments.

Operational planning and course of action analysis can leverage AI to evaluate proposed plans under uncertainty. Combat simulations use stochastic models to estimate probable outcomes of operations, running thousands of Monte Carlo iterations to generate probability distributions of casualties, mission success, duration, and logistics consumption. The Synthetic Theatre Operations Research Model (STORM) [14] and similar tools employ AI to evaluate alternative force structures, deployment patterns, and engagement tactics. These models account for weapon accuracy, detection probability, terrain effects, and unit behavior to estimate engagement outcomes.

Reinforcement learning has been applied to tactical decision-making in wargaming contexts, with AI agents learning effective strategies through simulated experience. “AlphaDogfight” [15] an AI system developed by Heron Systems, defeated human F-16 pilots in simulated air combat through reinforcement learning that discovered novel tactics. In simulation, the AI learned to exploit aircraft capabilities and sensor characteristics in ways human pilots had not conceived.

However, the transferability of simulation-learned strategies to actual combat remains uncertain [15]. Simulations necessarily simplify reality, and AI systems optimized for simulation environments may fail when faced with the complexity of actual operations. An AI that learns to win simulated air combat might employ tactics that violate physics, depend on perfect sensor information which are unavailable in reality, or ignore factors not modelled in simulation like pilot stress, equipment malfunctions, and rules of engagement. The risk of "overfitting to simulation" creates questions about how AI-developed tactics translate to actual operations.

Logistics and supply forecasting benefit from probabilistic demand prediction and inventory optimization. AI systems can forecast ammunition consumption, fuel usage, spare parts requirements, and medical supply needs based on historical operations, planned activity levels, environmental conditions, and equipment status. Machine learning models trained on logistics data from Iraq, Afghanistan and Ukraine can predict consumption patterns for future operations. Optimization algorithms can generate supply distribution plans that minimize transportation assets while maintaining adequate supply levels, accounting for probabilistic demand and delivery reliability.

Weather forecasting for military operations employs numerical weather prediction models that are fundamentally probabilistic. Ensemble forecasting generates multiple predictions with varying initial conditions to assess uncertainty and provide probability distributions for temperature, precipitation, wind, and visibility. Military aviation, airborne operations, and amphibious landings depend critically on weather, making accurate probabilistic forecasts valuable for planning. AI-enhanced weather prediction improves forecast accuracy and extends useful forecast horizons.

The effectiveness of AI systems operating under risk depends critically on whether the operational environment resembles the training data and whether underlying probability distributions remain stable.

3.3. AI Systems in Conditions of Uncertainty

In conditions of uncertainty — where neither outcomes nor probabilities are reliably knowable — AI systems face their most significant limitations, for reasons this section examines.

Adversarial intelligence and deception create systematic uncertainty that undermines AI reliability. Deception can be physical (camouflage, decoys, dummy equipment), tactical (feints, demonstrations), or informational (false communications, planted intelligence) while a successful deception creates situations where decision-makers' information is not merely incomplete but actively misleading. Military deception seeks to cause adversaries to act in ways prejudicial to their interests by manipulating their perception of reality.

AI systems trained to recognize patterns are vulnerable to adversarial exploitation when opponents understand those patterns. If an adversary knows that AI systems track vehicle movements to predict offensive operations, they can manipulate vehicle movements to create false indicators while concealing actual preparations. If facial recognition systems rely on certain features, adversaries can develop countermeasures that obscure those features or trigger false matches. The cat-and-mouse dynamic of military competition means that any consistent AI behavior creates exploitable vulnerabilities.

Adversarial machine learning research has demonstrated that neural networks can be fooled by carefully crafted inputs - "adversarial examples" - that appear benign to humans but cause misclassification [16]. Small, imperceptible perturbations to images can cause state-of-the-art image classifiers to confidently misidentify objects.

While these attacks have been demonstrated primarily in laboratory settings, the underlying vulnerability reflects a fundamental limitation: AI systems learn surface statistical patterns rather than developing robust conceptual understanding. An adversary who understands the AI's decision boundary can craft inputs that exploit it.

Novel tactics and adaptation present uncertainty that defeats pattern-based learning. History demonstrates that military innovation often stems from creative employment of existing capabilities in unexpected ways. Blitzkrieg tactics that combined armor, infantry, and close air support in rapid maneuver warfare surprised adversaries prepared for WWI-style static defense. The modern employment of drone warfighting in the Ukraine conflict is evolving constantly to defeat countermeasures, with adversaries adapting triggering mechanisms, rapid research and development cycles, camouflage techniques, and explosive configurations in response to enemy TTPs. Cyber operations employ constantly novel techniques to penetrate defenses and achieve effects. AI systems depend on recognizing patterns seen during training. When adversaries employ genuinely novel tactics without historical precedent, AI systems lack the conceptual understanding necessary to reason about the new situation. A human commander can recognize that "the enemy is doing something unprecedented" and adapt through reasoning from principles. An AI system trained to classify tactics into known categories may force-fit novel behavior into inappropriate categories or simply fail to recognize the significance of observations that don't match learned patterns. The problem is not merely that AI lacks data on novel tactics—it lacks the conceptual framework to understand tactics as purposeful adaptations of means to ends under constraints.

Strategic and political uncertainty surrounding military operations resist quantification and prediction. Military actions occur within political contexts involving competing interests, alliance dynamics, domestic politics, international law, and human psychology. Strategic questions like "Will our allies maintain their commitment if casualties mount?" or "How will the adversary's population respond to bombing?" or "What political objectives actually motivate this conflict?" involve human choices and social dynamics that defy reliable prediction.

Game theory provides some analytical tools for reasoning about strategic interaction, but its application to real conflicts faces severe limitations. Classical game theory assumes rational actors with

common knowledge of payoffs and strategies. Real strategic actors have private information, misperceive their situations, act on ideological commitments that are difficult to understand, and make decisions through complex organizational processes rather than as unified actors. AI systems that model strategic interaction through game-theoretic frameworks or learn strategies from historical cases may produce misleading predictions when applied to specific conflicts involving particular leaders, nations, and circumstances.

Emergent behavior in complex operations creates unpredictability even regarding friendly forces. Large military organizations involve thousands or millions of personnel making decisions at multiple echelons in dynamic circumstances. The interactions between tactical actions, logistics constraints, information flow, and human factors produce emergent outcomes that surprise even those within the organization. Morale effects, leadership influence, and small unit initiative can prove decisive but resist prediction from organizational-level data.

AI systems that attempt to predict operational outcomes by modelling component behavior face the complexity problem: comprehensive models become too computationally expensive while simplified models omit crucial factors. The "fog of war" includes uncertainty about one's own forces, not only on enemy sitation. Commanders may not know whether subordinate units will aggressively pursue objectives or proceed cautiously, whether logistics will deliver supplies on schedule, or whether equipment will function reliably. These uncertainties compound, creating situation-dependent outcomes that defy reliable prediction.

4. OPERATIONAL APPLICATIONS ACROSS MILITARY DOMAINS

4.1 Intelligence, Surveillance, and Reconnaissance (ISR)

Intelligence gathering and analysis represent perhaps the most widespread application of AI in military operations, spanning the certainty-risk-uncertainty spectrum with varying degrees of effectiveness across different mission types [17].

Full-motion video analysis from drone feeds generates massive data volumes — a single Predator drone produces the equivalent of a feature-length movie worth of video every 20 minutes of flight. Human analysts cannot possibly review all collected footage, creating what intelligence professionals call the “data deluge” problem. Project Maven demonstrated AI’s capability to address this by automating object detection and tracking in aerial

video; convolutional neural networks trained on labelled examples identify vehicles, buildings, and persons with accuracy above 90% under favourable conditions. This application operates primarily in the risk domain, as detection probability depends on measurable factors like image resolution, target size, and environmental conditions.

However, limitations emerge when adversaries employ countermeasures. Camouflage, concealment, and deception can dramatically degrade detection performance. The transition from risk to uncertainty occurs when adversaries understand and exploit AI detection patterns — the cat-and-mouse dynamic of military competition means that static AI pattern recognition faces adaptive adversaries who deliberately violate learned patterns. During the Cold War, the Soviet Union constructed elaborate maskirovka deception operations including fake missile sites and dummy aircraft specifically to deceive reconnaissance systems; modern adversaries employ similar techniques.

4.2 Targeting and Fire Control Systems

Targeting decisions — determining what to strike, when, and with what means — represent one of the highest-stakes applications of military AI, directly involving lethal force with implications for both operational effectiveness and compliance with international humanitarian law.

Target recognition systems can achieve high reliability under certainty and risk conditions. Stationary military installations and large equipment can be identified reliably when image quality is adequate. However, moving to human target identification dramatically increases uncertainty and ethical stakes. Computer vision algorithms can distinguish men from women and children based on size and clothing with reasonable accuracy in controlled conditions, but reliably determining combatant status — the fundamental distinction required by international humanitarian law — exceeds current AI capability. An AI system might identify that an individual is carrying a rifle but cannot determine whether that person is a combatant, civilian hunter, or civilian defending their home [18].

Autonomous weapons systems that can select and engage targets without human control represent the most controversial application. Existing systems range from defensive systems that automatically engage incoming threats (Phalanx CIWS, Iron Dome) to loitering munitions that autonomously search areas for targets matching programmed criteria (IAI Harop, ZALA Lancet). Defensive systems

like Phalanx succeed within narrow mission parameters — defending against incoming projectiles involves identifying fast-moving radar returns on intercept trajectories, a relatively deterministic pattern recognition problem. Offensive autonomous weapons in complex environments face fundamental challenges: proportionality assessments that balance military advantage against civilian harm require contextual understanding and ethical judgment that current AI systems lack.

4.3 Logistics and Resource Management

Military logistics involves enormous computational complexity that creates strong opportunities for AI optimization, particularly in certainty and risk domains where outcomes can be predicted reliably.

Predictive maintenance employs AI to forecast component failures before they occur. The F-35's ALIS system exemplifies this approach, collecting performance data from aircraft systems to analyse component health and predict failures. When failure modes are well-characterized and sensor coverage is adequate, this operates reliably in the risk domain. Uncertainty enters with novel failure modes, inadequate training data on new equipment, and combat damage effects — a component may fail in ways not represented in peacetime data, and combat-damaged systems may exhibit erratic behaviour that does not match learned failure patterns.

Supply chain optimization performs well in certainty and risk domains where demand is predictable and transportation networks are secure. However, uncertainty dominates in actual combat operations: an engagement may consume ammunition far faster than predicted, enemy action may sever supply routes, and operational changes may invalidate forecasts entirely. Military logistics requires resilience and redundancy precisely because uncertainty dominates — what matters is maintaining support despite the unexpected, not achieving optimal efficiency under predicted conditions.

4.4 Autonomous Weapons and Lethal Decision-Making

The prospect of weapons systems that select and engage targets without human intervention raises fundamental questions about human control over violence. Drone swarms using decentralized AI coordination represent emerging capabilities with uncertain operational implications. Multiple autonomous drones can coordinate through machine learning algorithms to search areas, overwhelm air defences, or conduct synchronized strikes. China's national defence strategy explicitly prioritizes "intelligentized warfare"

involving AI-enabled swarm systems.

The strategic implications extend beyond individual systems. An arms race in autonomous weapons creates risks including lowered thresholds for use of force when autonomous systems enable strikes without risk to personnel, attribution challenges when autonomous weapons create plausible deniability, escalation risks if autonomous systems act faster than human decision-making can assess situations, and potential proliferation to non-state actors. Autonomous weapons represent a transition from the certainty and risk domains where AI performs well into the uncertainty domain where human judgment remains essential — and it is precisely in that domain that the most consequential targeting decisions arise.

5. HUMAN-AI TEAMING IN MILITARY OPERATIONS

Effective integration of AI into military decision-making requires frameworks that leverage AI capabilities while maintaining human judgment. Human-AI teaming models attempt to optimize the complementary strengths of humans and machines across different decision environments.

Manned-Unmanned Teaming (MUM-T)[19] in aviation exemplifies operational human- AI collaboration.

Fig. 2 Apache & Grey Eagle drone

Apache helicopter crews can control unmanned aerial vehicles (UAVs) through the Improved Gray Eagle [20] interoperability system, using drones for reconnaissance while remaining at standoff distances. The human crew tasks the UAV, interprets its sensor feeds, and makes tactical decisions while the autonomous system executes flight control, navigation, and sensor management. This division of labor places certainty and risk-domain tasks (flight control, route following) with AI while preserving human authority over uncertain tactical decisions (target identification, engagement authorization).

The success of MUM-T depends on effective interfaces that provide situational awareness without overwhelming crews, intuitive tasking methods that allow rapid mission updates, and reliable autonomous behavior that maintains crew trust. When autonomy fails unpredictably or interfaces confuse rather than clarify, the human-machine team performs worse

than either component alone [21, 22]. Interface design represents a critical challenge, as poorly designed systems create cognitive burdens that offset AI capabilities.

Centaur teaming [23] represents a more integrated model where human and AI capabilities combine throughout the decision process rather than dividing tasks sequentially. The term derives from chess, where "centaur" teams of humans partnered with AI routinely defeat both unaided humans and unaided AI. The human contributes strategic understanding and novel insights while AI provides calculation depth and tactical precision. Applied to military operations, centaur teaming might involve AI rapidly perform data analysis, generate and evaluate courses of action while humans provide contextual judgment, ethical oversight, and strategic coherence.

However, effective centaur teaming requires that humans can critically evaluate AI recommendations—neither blindly accepting nor arbitrarily overriding them. This demands substantial training, well-calibrated AI confidence estimates, and organizational cultures that value human judgment even when it conflicts with algorithmic outputs. The risk of automation bias, where humans defer to AI despite better judgment, threatens to undermine centaur teaming when AI appears authoritative but lacks genuine understanding [24].

Algorithmic decision support positions AI as an advisor that generates recommendations, predictions, or options for human decision-makers who retain ultimate authority. Intelligence fusion systems that integrate multi-source data to present synthesized assessments, predictive analytics that forecast adversary actions, and planning tools that generate candidate courses of action all fall into this category. The human decision-maker receives AI-generated information but is expected to exercise independent judgment.

The effectiveness of decision support depends critically on explainability and trust calibration. If AI recommendations are not understood, humans cannot meaningfully evaluate them and must either blindly trust or ignore the system. If explanations misrepresent how recommendations were actually generated users may develop false confidence. Trust calibration requires that operators understand AI capabilities and limitations, recognizing when recommendations are likely reliable versus when skepticism is to be shown.

Appropriate reliance represents the key challenge in human-AI teaming: fostering appropriate trust rather than over-reliance or under-reliance. Over-reliance leads to automation bias where humans fail

to catch AI errors. Under-reliance wastes AI capabilities when valid recommendations are ignored. Appropriate reliance requires operators who understand when AI is likely to perform well (in certainty and risk domains similar to training) versus when it will struggle (in uncertain, novel, or adversarial contexts).

The most effective human-AI teams allocate responsibilities according to comparative advantage across decision environments: AI handles certainty-domain tasks requiring precise calculation at scale, AI supports risk-domain planning with probabilistic analysis and optimization. Humans provide judgment in uncertainty-domain decisions involving adversarial intelligence, novel situations, and ethical considerations, and maintain accountability for all consequential decisions, particularly those involving lethal force.

6. ETHICAL, LEGAL AND GOVERNANCE CHALLENGES

6.1 Algorithmic Bias

While algorithmic bias has been extensively studied in civilian contexts, its manifestation in military AI systems raises distinct concerns with potentially life-and-death consequences. Military AI systems trained on biased data can perpetuate discriminatory patterns in intelligence assessment, targeting, and threat evaluation [25, 26].

Intelligence bias occurs when AI systems trained on historical intelligence data learn patterns that reflect collection biases, analytical assumptions, or discriminatory targeting practices [27]. If training data over-represents certain demographics, regions, or behaviors as threatening due to past biases, AI systems will perpetuate those patterns. Predictive intelligence systems might systematically flag individuals from certain ethnic or religious groups as higher threats based on patterns in biased training data, effectively automating discrimination.

During counterinsurgency operations, if intelligence databases disproportionately associate certain demographic groups with hostile activity due to collection focus or ethnic profiling by human analysts, machine learning systems trained on that data will reproduce those associations. The algorithmic system provides a fake true objectivity that may obscure underlying biases, making discriminatory patterns harder to identify and challenge. Commanders relying on AI threat assessments may unknowingly perpetuate unjust targeting patterns learned from flawed training data.

Sensor bias emerges from the physical characteristics and training data of detection systems. Computer

vision algorithms trained primarily on datasets from western populations may perform worse on non-western faces due to training data imbalances. Facial recognition systems have demonstrated significantly higher error rates for women and people with darker skin tones a problem particularly concerning when such systems inform targeting or force protection decisions. If autonomous systems or operators relying on AI assistance experience higher misidentification rates for certain demographics, the risk of wrongful engagement increases.

Thermal imaging and sensor technologies may perform differently across skin tones, clothing types, or environmental conditions more common in certain regions. If detection algorithms are trained and validated primarily in conditions resembling western operating environments, their performance in different geographic or cultural contexts may degrade in ways that disproportionately affect local populations. This technical bias can translate to operational bias with severe humanitarian consequences.

Cultural and linguistic bias affects natural language processing and social network analysis systems. Translation systems trained primarily on formal text may poorly handle dialects, slang, or culturally-specific expressions. Sentiment analysis algorithms developed on a social media may misinterpret communication styles common in other cultures. Network analysis algorithms might misidentify family or tribal relationships as threatening associations based on connection densities common in some cultures but less so in others.

These biases create operational risks beyond ethical concerns. Biased intelligence leads to poor targeting, wasted resources pursuing false leads, and erosion of local population support when innocent people are wrongly identified as threats.

6.2 International Humanitarian Law and Rules of Engagement

International Humanitarian Law (IHL), embodied in the Geneva Conventions and customary international law, establishes fundamental principles governing armed conflict. The use of AI in military operations raises critical questions about compliance with these principles, particularly regarding distinction, proportionality, and precautions.

The principle of distinction requires that parties to conflict distinguish between combatants and civilians, directing attacks only against military objectives. Combatants can be lawfully targeted, civilians cannot be deliberately attacked, and civilian objects cannot be made the object of attack. This seemingly straightforward principle

becomes complex in implementation, particularly in irregular warfare where combatants may not wear uniforms and distinction depends on behavior, location, and context.

Current computer vision can identify humans, classify by apparent age and gender, detect weapons, and recognize uniforms with reasonable accuracy under favorable conditions. However, distinguishing combatants from civilians requires understanding of context, behavior, and status that exceeds pattern recognition. A person carrying a rifle might be a combatant, civilian hunter, civilian defending their home, or civilian playing with a wooden rifle similar toy. International law requires positive identification of military status before engagement—determining that someone falls within a targetable category, not merely that they might.

The contextual nature of distinction creates fundamental challenges for algorithmic implementation. A person's status may change over time—civilians who directly participate in hostilities become targetable while participating but regain protected status when participation ceases. Determining whether observed behavior constitutes "direct participation in hostilities" requires judgment about purpose and likely effects that resist algorithmic codification. An AI system might detect that someone is placing an object along a road but cannot determine whether it is an IED (direct participation) or a roadside shrine (protected activity).

Proportionality requires that expected incidental civilian harm not be excessive relative to anticipated direct and concrete military advantage. This assessment involves balancing incommensurable values—military advantage versus civilian casualties—through inherently normative judgment. Different reasonable people can reach different proportionality assessments in identical situations based on their weighting of military necessity versus humanitarian concerns.

Can this judgment be algorithmically automated? Proportionality requires estimating expected civilian casualties (uncertain), assessing military advantage (subjective and context-dependent), and comparing these quantities that resist mathematical comparison. Is destroying a command post worth ten civilian casualties? Twenty? The answer depends on the command post's importance, availability of alternatives, and one's valuing of civilian life against military objectives. These are moral judgments that reflect values, not calculations that have objectively correct answers.

Attempts to quantify proportionality through "casualty value functions" or similar formalisms risk simplifying what

should remain contested moral terrain. Reducing proportionality to an algorithm implies that there exists a mathematically optimal exchange rate between civilian deaths and military advantage—a proposition fundamentally at odds with IHL's humanitarian foundations. The requirement for human judgment in proportionality assessment reflects recognition that these are moral choices requiring human moral agency, not technical problems admitting computational solutions.

Precautions in attack require that parties take feasible precautions to minimize civilian harm, including verifying targets, choosing means and methods that avoid or minimize harm, providing warnings when feasible, and canceling attacks when civilian harm would be excessive. These obligations assume human decision-makers who can exercise judgment about verification sufficiency, weigh alternative methods, and assess feasibility of precautions.

Autonomous weapons that engage targets without human oversight at the moment of attack cannot satisfy precautionary obligations in meaningful ways. The system cannot verify targets beyond its programmed recognition criteria, cannot dynamically assess whether civilian harm has become excessive warranting attack cancellation, and cannot provide warnings to civilians. Precautions assume adaptive human judgment responsive to evolving situations—capabilities that autonomous systems lack.

Meaningful human control [28, 29, 30, 31] has emerged as a concept attempting to preserve human agency over violence even as AI systems increasingly mediate military force. What constitutes "meaningful" control remains contested, but proposed frameworks typically require that humans understand how systems function, have sufficient information to make informed decisions, have adequate time to deliberate, and exercise genuine choice. These criteria prove difficult to satisfy as autonomy increases, decision timescales compress, and system complexity grows.

6.3 Command Responsibility and Accountability

Military accountability frameworks assume clear chains of command with commanders responsible for their subordinates' actions. This model faces challenges when AI systems exercise decision-making functions: who bears responsibility when AI makes erroneous targeting decisions, fails to distinguish civilians, or malfunctions in ways causing civilian casualties [32]?

Traditional command responsibility under IHL holds commanders criminally responsible for subordinate war crimes if they

knew or should have known about them and failed to prevent or punish them. This doctrine developed in contexts where subordinates are human beings whose actions commanders can observe, predict based on character and training, and control through orders and discipline.

Applying command responsibility to AI systems raises novel questions. Can a commander "know or should have known" about AI system limitations or errors in ways comparable to knowledge about human subordinates? If an AI targeting system misidentifies targets due to training data biases, sensor malfunctions, or adversarial exploitation, does the commander who deployed that system bear criminal responsibility? The commander may lack technical expertise to evaluate AI reliability, may have reasonable belief based on validation testing that the system performs adequately, and may be unable to predict specific failure modes of complex machine learning systems.

Yet allowing AI systems to create accountability gaps would be dangerous. If no human can be held responsible when autonomous weapons commit war crimes, the prospect of punishment that deters violations disappears. Some legal scholars argue that commanders must understand AI systems under their control sufficiently to anticipate foreseeable misuse, while others contend that developers who create systems that are deployed in ways causing violations should bear responsibility. These questions remain unresolved, creating legal uncertainty that may chill beneficial AI applications while failing to prevent harmful ones.

Product liability frameworks developed for defective consumer products provide incomplete analogies for military AI. Product liability requires proving that a product was defective and that the defect caused harm. But what constitutes a "defect" in an AI system? If a computer vision system achieves 95% accuracy, well above human performance on average, but makes an erroneous identification in a specific case, is it "defective"? If the system performs as designed but training data limitations cause it to function poorly in certain conditions, is that a design defect, manufacturing defect, or warning failure?

Military AI systems operate in adversarial environments where enemies actively attempt to defeat them. If adversaries develop countermeasures that exploit AI vulnerabilities causing the system to malfunction, does responsibility lie with developers who created exploitable systems, commanders who deployed them in contested environments, or adversaries who exploited them? The intentional

introduction of adversarial stimuli to cause AI errors creates scenarios without clear civilian analogues.

Organizational accountability faces challenges when multiple entities contribute to AI system development, integration, and deployment. Defense contractors develop algorithms, military services integrate them into platforms, training ranges validate performance, operational commanders decide employment, and tactical operators interact with systems in combat. If an AI-enabled targeting error causes civilian casualties, determining which organization's decisions contributed most centrally to the harm may be impossible. The diffusion of responsibility across organizations can create situations where everyone bears partial responsibility but no one bears sufficient responsibility to face meaningful accountability.

6.4 Trust and Human-Machine Interface

Effective human-AI collaboration in military operations requires appropriate trust calibration, and well-designed interfaces. When these elements are lacking, human-machine teams perform worse than either humans or machines alone.

Trust calibration represents a critical challenge. Military operations demand that commanders trust their systems and subordinates as hesitation caused by insufficient trust can be tactically disastrous. However, blind faith in unreliable systems is equally dangerous. Appropriate trust requires that operators accurately understand AI capabilities and limitations, recognize when AI recommendations are likely reliable versus when skepticism is warranted, and maintain vigilance to catch errors when they occur.

Research demonstrates that trust in automation is "sticky" [33] as once established through reliable performance, it persists even when conditions change in ways that degrade reliability. Operators accustomed to AI systems performing well in training or benign environments may fail to increase skepticism when entering contested environments where adversarial action undermines AI effectiveness.

Training programs must expose operators to both AI successes and failures across diverse conditions, establishing realistic expectations about performance boundaries. However, training cannot replicate all conditions that may arise in actual operations. Novel adversary tactics, unusual environmental conditions, or system degradation from battle damage may cause AI failures that no training anticipated. Maintaining appropriate vigilance when AI has proven reliable thousands of times requires cognitive discipline that conflicts with natural human tendencies toward complacency.

Deep neural networks that achieve the highest performance on complex pattern recognition tasks are typically the least interpretable as their decisions emerge from millions of parameters in ways that resist simple explanation. Simpler, more interpretable models often sacrifice accuracy for transparency. In military applications where accuracy can be life-or-death, the performance penalty of interpretable models may be unacceptable. This creates genuine dilemmas between explainability and performance rather than engineering problems admitting technical solutions.

Operational tempo constraints limit explanation complexity. Commanders in time-compressed situations cannot review detailed explanations of algorithmic reasoning—they need rapid assessments of confidence and key factors. However, oversimplified explanations may mislead by suggesting understanding where none exists. Stating "the system is 85% confident" about a valid target based on visual appearance, location, and behavior provides actionable information but obscures the fact that the system could lack genuine understanding of what constitutes a valid target.

Detailed explanations of how AI systems make decisions could enable adversaries to develop countermeasures. If enemies understand how targeting algorithms identify military vehicles, they can modify camouflage, employ decoys, or develop electronic countermeasures exploiting algorithmic weaknesses. The tension between providing operators sufficient explanation to make informed decisions and preventing adversary exploitation of system details creates operational security challenges.

Interface design profoundly influences human-AI team effectiveness. Poorly designed interfaces can overwhelm operators with information, obscure critical factors, or encourage automation bias. Effective interfaces must present AI recommendations clearly without encouraging uncritical acceptance, communicate confidence and uncertainty appropriately, direct operator attention to factors most relevant for decisions, support rapid decision-making without sacrificing critical evaluation, and fail gracefully when AI confidence is low or system malfunctions.

The physical and cognitive interface between humans and AI systems will largely determine whether AI integration enhances or degrades military decision-making. Well-designed interfaces that foster appropriate reliance enable effective human-machine teams. Poorly designed interfaces that encourage over-reliance or fail to support critical

thinking create vulnerabilities as dangerous as technical AI limitations.

7. CONCLUSION

This paper has examined the implications of artificial intelligence for military decision-making through the analytical lens of three distinct decision environments. In conditions of certainty, where outcomes follow deterministically from known inputs, AI systems deliver reliable, superior performance — as demonstrated by fire control, route planning, and predictive maintenance applications. In conditions of risk, where outcomes are probabilistic but statistically estimable, AI provides substantial value in intelligence analysis, logistics forecasting, and operational planning, though its effectiveness degrades when adversaries adapt and violate the statistical assumptions. In conditions of genuine uncertainty AI faces fundamental limitations that pattern recognition alone cannot overcome. Human judgment, contextual understanding, and moral reasoning remain irreplaceable.

These findings carry direct implications for military doctrine and force development. Doctrine should formalize a decision-authority framework that allocates tasks to AI or humans based on the prevailing decision environment, rather than treating AI as a uniformly applicable capability. Training programmes must build operators who are calibrated consumers of AI outputs — capable of trusting AI recommendations in appropriate contexts while maintaining critical oversight when conditions shift toward uncertainty. Rules of engagement and command responsibility frameworks require revision to address the accountability gaps that arise when AI systems mediate targeting decisions, ensuring that meaningful human control is preserved not merely in formal policy but in operational practice. Procurement and acquisition processes should incorporate explainability and robustness standards proportional to the decision stakes involved, particularly for systems that operate in or near the uncertainty domain.

Several avenues for future research emerge directly from the limitations of this study. Empirical investigation of human-AI teaming in live or simulated military exercises would test whether the theoretical automation bias risks identified here manifest consistently under operational stress and time pressure. Comparative analysis of how major military powers are institutionalizing AI in doctrine — and whether divergent approaches create interoperability challenges or escalation risks within alliances — represents an urgent strategic research priority. The legal dimensions of command responsibility for AI-enabled systems

remain undertheorised and would benefit from systematic doctrinal analysis. Finally, technical research into adversarial robustness — specifically how military AI systems perform when intelligent adversaries deliberately probe their decision boundaries — is essential to close the gap between laboratory performance and operational reliability.

Artificial intelligence is fundamentally transforming decision-making across virtually all domains of human activity including military, creating both extraordinary opportunities and serious challenges that society is only beginning to address. This research has examined the multiple implications of AI integration into decision-making processes through theoretical analysis, case studies, and evaluation of cognitive, ethical, and regulatory dimensions.

AI DISCLOSURE

The author acknowledge the use of the following generative AI tools to assist in the preparation of this manuscript: ChatGPT. This tool was used solely for language editing and structural suggestions, under the complete control and responsibility of the authors. All AI-assisted content was critically reviewed and revised by the authors, who accept full responsibility for the accuracy and integrity of the final version.

REFERENCES

[1] Shapiro, M. J. (2005). The fog of war. Security Dialogue, 36(2), 233-246.

[2] Richards, C. (2020). Boyd's OODA loop. Necesse, 5(1), 142-165.

[3] Marr, J. J. (2001). The military decision making process: Making better decisions versus making decisions better (No. USACGSCSAMSAY200020001).

[4] Klein, G. A. (1993). A recognition-primed decision (RPD) model of rapid decision making. Decision making in action: Models and methods, 5(4), 138-147.

[5] Sauter, Vicki L. "Intuitive decision-making." Communications of the ACM 42.6 1999;

[6] Rashid, M., Abbas, Q., Younis, M. S., Baber, J., & Baber, N. (2023). Artificial intelligence in the military: An overview of the capabilities, applications and challenges. International Journal of Intelligent Systems, 2023, Article 4954561. https://doi.org/10.1155/2023/4954561

[7] Brady, M. R., & Goethals, P. (2019). A comparative analysis of contemporary 155 mm artillery projectiles. Journal of Defense Analytics and Logistics, 3(2), 171-192.

[8] Franks, E. (2005, May). Advanced warfighter machine interface. In Cockpit and Future Displays for Defense and Security (Vol. 5801, pp. 12-23). SPIE.

[9] S. R. Ali and R. S. Wexler, "Army Warfighter Network-Tactical (WIN-T) Theory of Operation," MILCOM 2013 - 2013 IEEE

Military Communications Conference, San Diego, CA, USA, 2013, pp. 1453-1461, doi: 10.1109/MILCOM.2013.246.

[10] https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/alis/CS00086-55%20(ALIS%20Product%20Card).pdf

[11] Nadibaidze, A., Bode, I., & Zhang, J. (2024). AI in military decision support systems: A review of developments and debates. Center for War Studies, University of Southern Denmark. https://doi.org/10.21996/epbr7566

[12] Lundberg, S.M., Lee, S.I., A Unified Approach to Interpreting Model Predictions, Advances in Neural Information Processing Systems, 2017.

[13] Lerner, W. D. (2013). Predicting the emplacement of improvised explosive devices: an innovative solution. Capitol College.

[14] Lucas, T. W., Sanchez, S. M., Sanchez, P., McDonald, M., & Upton, S. (2015). Developing Synthetic Theater Operations Research Model (STORM) Analytic Utility, Phase II.

[15] Pope, A. P., Ide, J. S., Mićović, D., Diaz, H., Rosenbluth, D., Ritholtz, L., ... & Javorsek, D. (2021, June). Hierarchical reinforcement learning for air-to-air combat. In 2021 international conference on unmanned aircraft systems (ICUAS) (pp. 275-284). IEEE. [] Doshi-Velez, F., Kim, B., Towards A Rigorous Science of Interpretable Machine Learning, ArXiv preprint, 2017.

[16] Papernot, N., McDaniel, P., Swami, A., & Harang, R. (2016, November). Crafting adversarial input sequences for recurrent neural networks. In MILCOM 2016-2016 IEEE Military Communications Conference (pp. 49-54). IEEE.

[17] Borghoff, U. M., Biundo, S., Schmid, U., & Thielscher, M. (2025). The use of artificial intelligence in military intelligence: An experimental investigation. Frontiers in Human Dynamics, 7, Article 1512697. https://doi.org/10.3389/fhumd.2025.1512697

[18] Viveros Álvarez, I. (2024). The risks and inefficacies of AI systems in military targeting support. ICRC Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2024/05/14/risks-inefficacies-ai-systems-military-targeting-support/

[19] Taylor, G., & Turpin, T. (2015). Army aviation manned-unmanned teaming (MUM-T): past, present, and future. In 18th International -Symposium on Aviation Psychology (p. 560).

[20] Judson, J. (2014). Improved Gray Eagle Shows Greater Endurance With Heavier Payloads. Inside the Army, 26(21), 10-10.

[21] Horowitz, M. C., & Lin-Greenberg, E. (2024). Bending the automation bias curve: A study of human and AI-based decision making in national security contexts. International Studies Quarterly, 68(1), sqad100. https://doi.org/10.1093/isq/sqad100

[22] Jonsson, M. (2023). Trusting machine intelligence: Artificial intelligence and human-autonomy teaming in military operations. Defence Studies, 23(3), 439–458.

https://doi.org/10.1080/14702436.2023.2178154

[23] Johnson, James, The AI Commander: Centaur Teaming, Command, and Ethical Dilemmas (Oxford, 2024; online edn, Oxford Academic, 18 Jan. 2024), https://doi.org/10.1093/oso/9780198892182.001.0001, accessed 13 Nov. 2025.

[24] Abioye, S. O., Busari, H. A., Omole, D. O., John-Mathews, J.-M., & Aremu, B. (2024). AI-driven human-autonomy teaming in tactical operations: Proposed framework, challenges, and future directions. arXiv preprint arXiv:2401.12172.

[25] Pace, T., & Ranes, B. (2024, June). Bias, explainability, transparency, and trust for AI-enabled military systems. In Assurance and Security for AI-enabled Systems (Vol. 13054, pp. 20-29). SPIE.

[26] Bode, I., & Bhila, T. (2024). The problem of algorithmic bias in AI-based military decision support systems. ICRC Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2024/09/03/algorithmic-bias-ai-military-decision-support-systems/

[27] Parasuraman, R., Manzey, D.H., Complacency and Bias in Human Use of Automation: An Attentional Integration, Human Factors, Vol. 52, No. 3, 2010.

[28] Cavalcante Siebert, L., Lupetti, M. L., Aizenberg, E., Beckers, N., Zgonnikov, A., Veluwenkamp, H., ... & Lagendijk, R. L. (2023). Meaningful human control: actionable properties for AI system development. AI and Ethics, 3(1), 241-255.

[29] Greipl, S. (2024). AI in military decision-making: Supporting humans, not replacing them. ICRC Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2024/08/20/ai-military-decision-making-supporting-humans/

[30] Docherty, B., & Kuster, M. (2023). Regulating lethal autonomous weapon systems: Exploring the challenges of explainability and traceability. AI and Ethics, 3(4), 1425–1438. https://doi.org/10.1007/s43681-022-00261-6

[31] ICRC & Geneva Academy of International Humanitarian Law and Human Rights. (2024). Expert consultation report: AI and related technologies in military decision-making on the use of force in armed conflicts. Geneva: ICRC. https://www.icrc.org/en/document/ai-related-technologies-military-decision-making-use-force-armed-conflicts

[32] Nalin, F., & Tripodi, P. (2023). Future warfare and responsibility management in the AI-based military decision-making process. Journal of Advanced Military Studies, 14(1), 58–76. https://doi.org/10.21140/mcuj.20231401003

[33] Liang, G., & Newell, B. (2022). Trusting algorithms: performance, explanations, and sticky preferences. In Proceedings of the annual meeting of the cognitive science Society (Vol. 44, No. 44)

[34] Wilson, N. A. (2020). Understanding the Battle for AI in Warfare through the Practices of Assemblage: A Case Study of Project Maven (Master's thesis)

ETHICAL FADING AS SYSTEMIC VULNERABILITY: FROM THEORETICAL REVIEW TO A MULTI-LEVEL DIAGNOSTIC FRAMEWORK FOR MORAL EROSION IN COMPLEX ORGANIZATIONS

Aura CODREANU[1]

Regional Department of Defense Resources Management Studies (DRESMARA) / "Carol I" National Defense University, Brasov, Romania

Ethical fading, viewed as the gradual and often imperceptible erosion of moral salience in organizational decision-making, has emerged as a critical vulnerability in complex, high-stakes environments. While originally theorized in behavioral ethics as a cognitive phenomenon affecting individual judgment, accumulating evidence indicates that ethical fading operates at multiple organizational levels simultaneously, constituting a systemic risk rather than an isolated individual failure. This article presents a structured theoretical review of the ethical fading construct, traces its theoretical lineage from bounded ethicality and moral disengagement to contemporary multilevel organizational ethics research, and synthesizes converging findings across organizational behavior, leadership studies, and AI-augmented decision-making.

Building on this review, the article proposes a Multi-Level Diagnostic Framework (MLDF) for detecting and assessing moral erosion across individual, group, organizational, and technological layers. The framework identifies specific indicators, enabling conditions, and interaction effects at each level. Practical implications are discussed for governance design, leadership development, ethics auditing, and organizational resilience. The proposed MLDF offers a transversal analytical instrument applicable to both public and private complex organizations, with particular relevance for institutions operating under high operational pressure, hierarchical authority structures, and expanding algorithmic decision support.

Key words: *ethical fading, moral disengagement, organizational ethics, multi-level framework, algorithmic decision-making, socio-technical systems.*

[1] ORCID: https://orcid.org/0009-0000-4298-355X, e-mail: acodreanu1@mapn.ro

1. INTRODUCTION

Ethical failures in complex organizations rarely originate from single acts of deliberate wrongdoing. More commonly, they emerge through a gradual, cumulative process in which moral considerations lose their prominence in decision-making routines, a process that Tenbrunsel and Messick (2004) named *ethical fading*. Unlike overt corruption or deliberate misconduct, ethical fading is characterized by its invisibility: decision-makers continue to perceive themselves as ethical while progressively distancing their choices from moral evaluation. This paradox (the ethical failure that does not feel like one) makes ethical fading particularly dangerous in organizations where accountability is diffuse, operational pressure is sustained, and authority structures limit dissent.

The concept has attracted renewed scholarly attention in the 2020s as research at the intersection of behavioral ethics, organizational theory, and artificial intelligence governance has converged on a shared observation: moral erosion in organizations is not primarily the product of individual character defects, but of systemic conditions that progressively disable ethical cognition. At the *individual level*, mechanisms such as bounded ethicality, self-serving bias, and motivated reasoning allow decision-makers to rationalize departures from ethical standards without conscious awareness (Bazerman and Tenbrunsel, 2011). At the *group level*, collective rationalization, loyalty dynamics, and organizational silence suppress moral dissent and normalize deviance (Fida et al., 2025; Mishra and Uppal, 2025). At the *organizational level*, performance-driven incentive structures, bureaucratic routinization, and cultural normalization institutionalize ethical blind spots (Kump and Scholz, 2022; Kuenzi et al., 2020). More recently, the introduction of *algorithmic decision-support systems* has added a fourth layer of moral diffusion, as responsibility attribution becomes distributed across human and non-human agents (Danaher, 2022; EU AI Act, 2024/1689).

Despite this convergence, the field lacks a systematic diagnostic framework that integrates these multilevel dynamics into a coherent analytical instrument. Existing models tend to address a single level of analysis (for instance, Bazerman and Tenbrunsel's (2011) bounded ethicality framework operates at the individual level, while Kaptein's (2008) corporate ethical virtues model focuses on organizational culture) or to treat ethical fading as a predominantly psychological phenomenon without accounting for group dynamics, institutional structures, or algorithmic diffusion.

This article addresses this gap through two contributions. First, it presents a structured theoretical review of the ethical fading construct, mapping its conceptual evolution and identifying the key mechanisms through which moral erosion operates at each organizational level. Second, drawing on this review, it proposes a Multi-Level Diagnostic Framework (MLDF) for the systematic assessment of ethical fading risk in complex organizations.

The article proceeds as follows. Section 2 outlines the methodology, followed by Section 3, which traces the theoretical foundations of ethical fading and analytically distinguishes the three core constructs. Sections 4 and 5 examine moral erosion across the individual, group, organizational, and technological levels respectively. Section 6 introduces the MLDF, while Section 7 discusses the implications and Section 8 concludes.

2. METHODOLOGY

This article employs a structured theoretical review methodology, consistent with approaches used in behavioral ethics and organizational theory when the aim is conceptual integration rather than meta-analytic aggregation (Torraco, 2016). The review was designed to map the theoretical terrain of ethical fading across levels of organizational analysis and to identify areas of convergence sufficient to support framework development. A structured review was preferred over a systematic meta-analysis because the central research problem (the absence of a multilevel diagnostic framework) is a gap in theoretical architecture rather than in effect-size estimation. The methodological objective was therefore synthesis and integration across levels of analysis rather than the aggregation of comparable empirical measurements.

2.1. Search Strategy and Inclusion Criteria

A systematic search was conducted across Web of Science, Scopus, PsycINFO, and Google Scholar using the following primary terms: *ethical fading, moral disengagement, bounded ethicality, moral erosion, organizational ethics, unethical pro-organizational behavior, normalization of deviance,* and *algorithmic moral diffusion*. Secondary terms included *multilevel ethics, ethical climate, moral identity, organizational silence, AI governance, institutional theory, risk governance,* and *socio-technical systems*. The search encompassed peer-reviewed English-language articles published between 1955 and 2025, with targeted coverage of the 2019-2025 period to ensure contemporaneity. Foundational pre-2003 works were included where they constitute seminal contributions (specifically: Simon (1955) on

bounded rationality, Bandura (1999, 2016) on moral agency, Janis (1972) on groupthink, and Vaughan (1996) on normalization of deviance).

Inclusion criteria required that sources:

a) address ethical, moral, or unethical behavior in organizational contexts;

b) engage with cognitive, social, structural, or technological mechanisms of moral erosion; and

c) offer conceptual or empirical contributions relevant to multi-level analysis.

Sources focused exclusively on individual clinical ethics or abstract moral philosophy without organizational application were excluded. Following a two-stage screening process (title/abstract screening followed by full-text review) a final set of 42 sources was retained for detailed citation and analysis; an additional 18 screened sources informed thematic mapping without generating direct citations, for a combined pool of 60 reviewed texts. This expanded body of literature, relative to the initial draft, reflects the explicit integration of institutional theory, risk governance, and socio-technical systems perspectives.

2.2. Analytical Approach and Limitations

Sources were organized according to the primary level of organizational analysis addressed: individual, group, organizational, or technological. Cross-cutting themes, theoretical overlaps, and identified gaps were recorded systematically in a conceptual mapping matrix. A key analytical step (distinguishing ethical fading, moral disengagement, and normalization of deviance as related but non-identical constructs) was conducted through comparative conceptual analysis across six dimensions, described in Table 1 (Section 3.4). The resulting conceptual map informed the architecture of the proposed MLDF, which was developed deductively from the reviewed literature and refined iteratively to ensure logical coherence across levels.

Several methodological limitations deserve explicit acknowledgment. First, source categorization across levels was conducted by a single reviewer; future structured reviews should incorporate second-coder verification to strengthen thematic reliability through inter-rater agreement assessment. Second, the reviewed literature is primarily drawn from English-language Western organizational research, with relatively sparse representation from Eastern European, Asian, or Global South institutional contexts. Cross-cultural applicability of both the constructs and the MLDF therefore requires independent validation

before these instruments are used in non-Western settings. Third, the structured review methodology privileges breadth of theoretical coverage over depth of empirical evidence in any single domain; readers should treat the framework as a theoretically grounded diagnostic template requiring empirical validation rather than as a confirmed measurement model.

3. THEORETICAL FOUNDATIONS: THE ETHICAL FADING CONSTRUCT AND ADJACENT FRAMEWORKS

The concept of ethical fading was introduced by Tenbrunsel and Messick (2004) to describe *the process by which the ethical dimensions of a decision gradually recede from awareness, allowing self-interest and organizational pressures to dominate without triggering moral discomfort*. The seminal insight was that people do not always make unethical choices through deliberate calculation; rather, they often fail to recognize that a moral dimension is present at all. This foundational observation has proved durable across two decades of subsequent research, with the construct extended progressively from its original individual-cognitive framing to encompass group, organizational, and most recently algorithmic dimensions of moral erosion. Section 3 traces this conceptual evolution through three thematic threads (3.1-3.3), provides an analytical differentiation of the three core constructs (3.4), and integrates three adjacent theoretical frameworks that reinforce the systemic argument (3.5).

3.1. From Bounded Rationality to Bounded Ethicality

The ethical fading construct draws directly on Simon's (1955) bounded rationality, the foundational recognition that human cognition operates under cognitive, informational, and temporal constraints that systematically deflect decision-making from normative ideals. Where classical economic theory assumed that decision-makers optimize outcomes through comprehensive information processing, Simon demonstrated that real human decision-making relies on heuristics and satisficing strategies that introduce predictable deviations from optimality. Bazerman and Tenbrunsel (2011) extended this logic explicitly to the moral domain, proposing bounded ethicality as the systematic and predictable ways in which individuals engage in unethical actions beyond their own awareness.

3.2. Bandura's Social Cognitive Theory of Moral Disengagement

A parallel theoretical tradition of considerable relevance to ethical fading originates in Bandura's (1999,

2016) social cognitive theory of moral agency. Bandura identified eight mechanisms through which individuals selectively disengage their moral self-regulatory standards without abandoning their self-conception as ethical people:

- moral justification (reframing harmful conduct as serving a higher moral purpose);
- euphemistic labeling (using sanitized language to reduce the moral weight of harmful actions);
- advantageous comparison (contrasting one's conduct favorably with worse alternatives);
- displacement of responsibility (attributing one's actions to the directives of authorities);
- diffusion of responsibility (distributing accountability across multiple actors so that no single actor bears full culpability);
- dehumanization (denying the humanity of those harmed);
- attribution of blame (holding victims responsible for their own harm), and
- disregard or distortion of consequences (minimizing awareness of the harm caused).

Bandura developed these mechanisms primarily at the individual level, but subsequent research has demonstrated their applicability at the group level (where they operate as shared social narratives) and at the organizational level, where they become embedded in institutional discourse and standard procedures (Moore et al., 2012; Fida et al., 2025).

3.3. Normalization of Deviance

Diane Vaughan (1996) developed the normalization of deviance concept through her exhaustive sociological analysis of the Space Shuttle Challenger disaster. Her central finding was that the O-ring erosion that caused the 1986 disaster was not the result of a single catastrophic decision or individual negligence, but of a decade-long process in which NASA engineers and managers progressively redefined acceptable risk. Each instance of O-ring erosion that did not produce a catastrophic failure was interpreted as evidence that the design could tolerate the anomaly, until the anomaly was no longer categorized as a deviation from acceptable performance.

Vaughan termed this process the *normalization of deviance*: the systematic organizational acceptance of practices that violate safety or ethical standards through gradual re-categorization, in which repeated exposure to marginal risk reduces perceived danger until the deviant becomes routine.

3.4. Analytical Differentiation of the Three Core Constructs

A key analytical requirement is sharper conceptual differentiation between the three foundational

constructs. While ethical fading, moral disengagement, and normalization of deviance are frequently treated as near-synonyms in the organizational ethics literature, their analytical combination obscures the sequential causal logic that is central to the systemic argument of this article. Table 1 addresses this directly through a structured comparative analysis across seven analytical dimensions.

Table 1. Analytical Differentiation of Core Constructs in Moral Erosion Research

Dimension	Ethical Fading	Moral Disengagement	Normalization of Deviance
Primary locus	Individual cognition (pre-decisional)	Individual and collective cognition (post-awareness)	Organizational culture and routines
Core mechanism	Moral salience recedes before ethical evaluation occurs; the moral dimension is not perceived	Active cognitive restructuring neutralizes moral standards after initial awareness	Incremental re-categorization of deviant practices as acceptable through repetition
Awareness of wrongdoing	Absent - actor does not recognize an ethical issue	Present but rationalized - actor recognizes the issue and suppresses it	Progressively eliminated - initial awareness erodes through habituation
Temporal signature	Acute / situational - occurs within a decision event	Situational to chronic - can be episodic or habitual	Chronic / cumulative - unfolds over extended organizational time
Primary level of analysis	Individual (Level I)	Individual and group (Levels I-II)	Organizational (Level III)
Key theoretical source	Tenbrunsel and Messick (2004); Bazerman and Tenbrunsel (2011)	Bandura (1999, 2016); Moore et al. (2012); Fida et al. (2025)	Vaughan (1996); Kump and Scholz (2022)
Relation to ethical fading	Root construct - the foundational condition of moral invisibility	Amplifying pathway - moral disengagement deepens and sustains ethical fading at the group level	Institutionalizing outcome - ethical fading and moral disengagement, once chronic, produce normalized deviance

Source: Author's elaboration.

Table 1 makes explicit what earlier formulations left implicit. Ethical fading is the root condition (the failure of moral salience to register at the moment of decision) and is therefore a logical precondition for both moral disengagement and normalization of deviance. Moral disengagement operates as an amplifying pathway: once fading creates moral distraction, disengagement mechanisms actively suppress any residual awareness that might remain, particularly through the group-level social processes of collective rationalization and peer modeling documented by Fida et al. (2025) and Zhu et al. (2011).

Normalization of deviance is the institutionalizing outcome: the cumulative sedimentation of repeated cycles of ethical fading and moral disengagement into organizational routines, cultural assumptions, and standard operating procedures. The three constructs are thus sequentially related as well as analytically distinct, forming a causal chain (root condition to amplifying pathway to institutional outcome) rather than alternative explanations of the same phenomenon. This sequential logic is central to the MLDF architecture, which is organized to address all three nodes of the chain rather than any single construct in isolation.

3.5. Adjacent Theoretical Frameworks

Three bodies of theory beyond behavioral ethics provide essential scaffolding for the systemic argument of this article. *Institutional theory* (DiMaggio and Powell, 1983; Scott, 2014) explains how ethical fading propagates across organizational fields through coercive, mimetic, and normative isomorphic pressures, making moral erosion a field-level phenomenon rather than solely an intra-organizational one. *Risk governance frameworks* (IRGC, 2017; Renn, 2008) provide the process architecture for translating the MLDF's diagnostic outputs into governance action, situating ethical fading assessment within established risk appraisal and management cycles. *Socio-technical systems theory* (Trist and Bamforth, 1951; Baxter and Sommerville, 2011) provides the joint optimization principle that informs the Level IV countermeasures: technical compliance systems cannot function as genuine ethical safeguards without simultaneous attention to the social conditions that give technical requirements behavioral content. The integration of these three frameworks with the MLDF is developed in Section 6.3.

4. LEVELS I AND II: INDIVIDUAL AND GROUP MECHANISMS

4.1. Self-Serving Cognitive Bias

Self-serving bias leads individuals to interpret ambiguous ethical situations in ways that

favor their own interests or protect their self-concept as moral actors (Bazerman and Tenbrunsel, 2011). In organizational contexts, this manifests as a systematic tendency to minimize the perceived harm of one's own decisions while applying more stringent moral evaluation to functionally equivalent actions by others. The asymmetry is rarely conscious, since individuals experiencing self-serving bias genuinely believe their assessments are objective.

Experimental research consistently demonstrates that the bias intensifies when the self-serving interpretation is financially beneficial, when the decision involves accepted professional role norms, and when feedback about harm is delayed or indirect (Messick and Bazerman, 1996). The organizational relevance is significant: in environments where performance is individually evaluated and compensation is tied to outcomes, self-serving bias creates a systematic distortion in which ethically questionable paths are recurrently perceived as legitimate.

4.2. Moral Licensing

Moral licensing refers to the phenomenon whereby individuals who have recently performed ethical or prosocial actions subsequently grant themselves implicit permission to act less ethically in subsequent decisions (Merritt et al., 2010). The mechanism operates through a psychological credit system: the prior ethical behavior creates a surplus of moral credit that is then unconsciously drawn upon to justify subsequent departures from ethical standards.

Critically, the licensing effect does not require conscious awareness, individuals experiencing moral licensing do not experience themselves as behaving untruthfully, because the prior ethical action genuinely adjusts their self-perception of their moral standing.

4.3. The Role of Ethical Identity under Pressure

Research on moral identity (the extent to which being a moral person is central to one's self-concept) suggests that strong moral identity is generally protective against ethical fading (Aquino and Reed, 2002). Individuals for whom morality is a core self-definitional attribute chronically attend to the moral dimensions of situations (Reynolds, 2008), making ethical fading less likely because the moral salience that fading erodes is actively maintained through identity-related cognitive attention. Moral attentiveness (the dispositional tendency to perceive and consider moral aspects of experience) functions as a cognitive buffer that counteracts the motivated blindness and indirect blindness mechanisms described in 3.1.

4.4. Enabling Conditions at the Individual Level

The mechanisms described in 4.1-4.3 do not operate uniformly across individuals or contexts. A set of enabling conditions (structural, situational, and dispositional) amplifies individual-level ethical fading risk and determines its severity and persistence.

Elevated cognitive load and decision fatigue are among the most robust enabling conditions: research in moral psychology consistently demonstrates that ethical cognition requires deliberate, controlled processing that is substantially impaired under cognitive resource depletion (Bazerman and Tenbrunsel, 2011).

Organizational environments characterized by decision-making under time pressure, information overload, or sustained operational stress therefore systematically increase ethical fading risk at the individual level.

4.5. Collective Moral Disengagement

Fida et al. (2025) formally operationalized *organizational moral disengagement* (OMD) as a collective social process (analytically distinct from the aggregation of individual moral disengagement) through which organizational groups develop shared perceptions of mechanisms for suspending collective moral agency.

The distinction is theoretically significant: OMD is not simply the average level of individual moral disengagement in a group, but an emergent property of the group's social system, a normative climate in which disengagement mechanisms are collectively endorsed, mutually modeled, and socially reinforced through shared narrative and peer interaction.

The construct was operationalized using a multilevel measurement model demonstrating that OMD has cross-level effects on individual behavior above and beyond individual moral disengagement, confirming its emergent and irreducible character.

4.6. Organizational Silence and Moral Voice Suppression

Organizational silence (*the collective tendency of organizational members to withhold meaningful information, concerns, or ethical objections that could be relevant to improving organizational functioning*) is both a symptom and a primary driver of group-level ethical fading (Morrison, 2023). When members perceive that raising ethical concerns is unwelcome, futile, or personally risky, they adapt by restricting their communications to what the organization has signaled it wants to hear. This adaptation is individually rational in the short term but collectively catastrophic over time, because it removes the

informational feedback that would enable the organization to detect and correct emerging moral erosion before it becomes institutionalized.

4.7. Groupthink and Collective Rationalization

Janis's (1972) foundational groupthink analysis demonstrated that cohesive, high-pressure groups systematically develop decision-making pathologies including suppression of dissent, overestimation of group consensus, stereotyping of outgroup critics, and collective rationalization of questionable decisions. In the domain of organizational ethics, groupthink creates conditions in which morally problematic decisions pass without challenge because individual members (recognizing the group's apparent consensus and fearing social exclusion) calibrate their expressed views to perceived group norms rather than voicing genuine ethical concerns. The result is what Janis termed the illusion of unanimity: a group that appears to have reached ethical consensus, but has actually suppressed the individual doubts that would reveal its absence.

4.8. Unethical Pro-Organizational Behavior

Unethical pro-organizational behavior (UPB), representing *the actions intended to benefit the organization that simultaneously violate core ethical or legal standards* (Umphress and Bingham, 2011) exemplifies a particularly insidious group-level manifestation of ethical fading, because it is intrinsically resistant to conventional detection and intervention mechanisms.

Unlike counterproductive work behavior, which actors typically recognize as transgressive, UPB is framed by actors as loyalty, dedication, or mission effectiveness. The falsification of safety records to protect an organization's regulatory standing, the manipulation of financial reporting to shield an institution from reputational damage, or the suppression of adverse research findings to protect an organization's product, all are canonical forms of UPB in which the ethical violation is experienced by the actor as organizational service.

5. LEVELS III AND IV: ORGANIZATIONAL AND TECHNOLOGICAL ANTECEDENTS

5.1. Performance-Driven Incentive Structures

The bottom-line mentality (BLM), viewed as *an exclusive organizational focus on financial or metric-based outcomes to the exclusion of other considerations* is a primary structural antecedent of ethical fading at the organizational level (Greenbaum et al., 2012).

BLM operates through moral disengagement as a mediating mechanism: supervisors who communicate that bottom-line outcomes are the paramount organizational priority (through performance evaluation criteria, resource allocation decisions, and the behaviors they model and reward) signal to subordinates that ethical considerations are secondary, activating moral disengagement processes that then propagate downward through organizational hierarchies (Mitchell et al., 2024).

The result is a systematic organizational climate in which ethical violations that serve performance goals are tacitly permitted, because the implicit organizational message is that performance justifies method.

5.2. Ethical Climate and Ethical Culture

Organizational ethical climate, representing *the shared perceptions of organizational practices, procedures, and policies relevant to ethics* is among the most robust structural predictors of ethical and unethical behavior at the organizational level (Kuenzi et al., 2020; Kaptein, 2023). Victor and Cullen's (1988) foundational typology distinguishes among ethical climates on two dimensions: the ethical criterion used (egoism, benevolence, principle) and the locus of reference (individual, local, cosmopolitan).

Self-interest climates, in which ethics is evaluated primarily through the lens of individual or organizational advantage substantially amplify individual and group-level ethical fading by providing normative cover for self-serving rationalization. Principled climates, by contrast, emphasize adherence to professional codes, organizational rules, and stakeholder welfare in ways that maintain moral salience even under performance pressure.

5.3. Bureaucratic Routinization and Procedural Displacement

Complex organizations almost universally address ethical risk through procedural compliance mechanisms, such as: codes of conduct, approval chains, compliance training programs, ethics hotlines, and audit procedures. These mechanisms serve critical accountability functions and are not without value. Research consistently demonstrates, however, that such mechanisms can paradoxically accelerate ethical fading when procedural compliance displaces moral deliberation (a dynamic termed procedural moral outsourcing), whereby ethics are treated as managed by the compliance system rather than continuously exercised by organizational members.

Kump and Scholz (2022) demonstrate that routinization embeds ethical blind spots within

standard operating procedures through a mechanism closely related to normalization of deviance: once a procedure is established and followed, the ethical evaluation that originally informed its design is no longer performed. The procedure is followed because it is the procedure (not because its ethical logic is continuously reaffirmed) and any ethical anomalies that the original designers did not anticipate become invisible to the procedural compliance framework.

In high-complexity environments, where the ethical challenges posed by novel situations routinely outpace the capacity of existing compliance frameworks, this procedural displacement of moral judgment represents a structural vulnerability of the first order. From a socio-technical systems perspective (Baxter and Sommerville, 2011), procedural displacement reflects a failure of joint optimization: the technical compliance system is designed and deployed without adequate attention to the social conditions (deliberative culture, psychological safety, leadership modeling of ethical reasoning) required to make it function as a genuine ethical safeguard rather than a liability-minimizing ritual.

5.4. Hierarchical Authority and Responsibility Diffusion

Hierarchical authority structures create distinctive ethical fading risks through the mechanism of responsibility diffusion, viewer as *the reduction in individual felt moral accountability that occurs when authority and decision-making responsibility are distributed across multiple organizational layers* (Bandura, 2016). In deep hierarchies, individuals at lower levels defer ethical evaluation upward to their superiors, confident that authority figures have already determined the ethical legitimacy of directives. Superiors, in turn, defer to institutional mandates, strategic objectives, or established procedures.

The result is a vacuum of moral agency in which ethical considerations are displaced without being explicitly rejected by any single actor, the organizational equivalent of Bandura's (2016) diffusion of responsibility mechanism, operating at the structural rather than interpersonal level.

5.5. Algorithmic Decision-Making and Moral Displacement: Empirical Evidence

Danaher (2022) terms the reduction in human moral agency that occurs when decision-making is delegated to automated systems the "techno-responsibility gap". As decisions are framed as algorithmically derived rather than humanly chosen, the perceived locus of moral responsibility shifts

from individual actors to systems, substantially reducing the likelihood of active ethical examination at the point of decision. This mechanism has been documented empirically across multiple high-stakes organizational domains, providing concrete evidence that technological-level ethical fading is not a speculative risk but a documented organizational reality.

Obermeyer et al. (2019) demonstrated that a commercial algorithm allocating care management resources in US health systems systematically underestimated Afro-American patients' needs, not through explicit racial bias, but because it used cost as a proxy for need, encoding existing utilization disparities as allegedly objective outputs. Healthcare providers relying on the algorithm's recommendations accepted them without ethical scrutiny, exemplifying automation-induced ethical fading: the algorithmic output displaced the moral evaluation that would have been applied to an equivalent human recommendation.

The algorithm affected approximately 200 million patients annually before the bias was identified through external academic research rather than internal governance mechanisms, a finding that directly illustrates the failure of standard organizational oversight to detect Level IV ethical fading.

5.6. Automation Bias and Ethical Complacency

Automation bias (*the tendency of human operators to over-rely on automated system outputs, particularly under conditions of cognitive load, time pressure, or uncertainty about their own competence*) interacts with ethical fading in ways that are especially consequential in high-stakes organizational environments (Logg et al., 2019).

Automation bias is not simply carelessness or laziness; it reflects a rational heuristic in environments where automated systems have historically outperformed human judgment on specific measurable tasks, leading actors to generalize this superior performance to dimensions (including ethical dimensions) for which the algorithm was never designed or validated. Logg et al.'s (2019) experimental findings demonstrate that algorithmic recommendations are systematically granted greater legitimacy than equivalent human recommendations even when the experimental participants are expert in the relevant domain, suggesting that the bias is not simply a function of domain ignorance.

5.7. Regulatory and Governance Responses

The EU AI Act (Regulation (EU) 2024/1689) represents the most

comprehensive regulatory response to algorithmic moral diffusion to date. It mandates human oversight, risk classification, conformity assessment, and transparency documentation for high-risk AI systems across key societal domains including employment, education, credit assessment, and public services.

The Act's risk-based framework explicitly acknowledges the techno-responsibility gap by requiring that human decision-makers maintain meaningful oversight of algorithmic outputs in high-risk applications, and by mandating explainability sufficient to support such oversight. The legislation thus exemplifies a socio-technical design philosophy: technical systems must be designed with the social conditions of human oversight explicitly in mind.

5.8. Interaction Effects across Levels

The technological layer does not operate as an isolated ethical fading pathway. It interacts bidirectionally with all three human levels in ways that both amplify and, under favorable conditions, attenuate moral erosion dynamics. The Obermeyer et al. (2019) healthcare case illustrates the top-down amplification pathway operating through the technological layer: organizational-level performance pressure (cost optimization as the algorithm's objective function) shaped the technical system's design, which in turn suppressed individual clinicians' moral scrutiny of racially biased recommendations.

The algorithmic system thus served as a transmission mechanism for organizational-level ethical fading into individual-level moral disengagement, in a manner that would not have been possible through purely human-mediated organizational communication.

6. RESULTS: A MULTI-LEVEL DIAGNOSTIC FRAMEWORK FOR ETHICAL FADING

Drawing on the theoretical review presented in Sections 3-5, this article proposes a Multi-Level Diagnostic Framework (MLDF) for the systematic assessment of ethical fading risk in complex organizations. The MLDF responds directly to the gap identified in the introduction: the absence of an integrated diagnostic instrument that addresses moral erosion simultaneously across individual, group, organizational, and technological levels of analysis, rather than treating each level as an isolated domain. The framework integrates insights from behavioral ethics, institutional theory, risk governance, and socio-technical systems theory into a coherent analytical instrument designed to support ethics auditing, preventive governance design, and post-incident organizational

analysis. It is explicitly positioned as a theoretically grounded diagnostic template requiring prospective empirical validation rather than a validated measurement model.

The MLDF's key design principles derive directly from the theoretical analysis:

- first, each level is addressed with a distinct set of diagnostic indicators, enabling conditions, and countermeasures, reflecting the analytical autonomy of individual, group, organizational, and technological mechanisms;
- second, the framework incorporates explicit cross-level interaction pathways (6.2), because the systemic character of ethical fading arises from the mutual reinforcement between levels rather than from any single level in isolation;
- third, the framework is designed for practical application in three operational modes (diagnostic, preventive, and investigative) to accommodate the different organizational contexts in which ethics assessment is typically conducted;
- fourth, countermeasures are anchored in established empirical instruments and governance frameworks wherever available, to maximize transferability to organizational practice without requiring extensive local adaptation.

6.1. Framework Architecture

The MLDF organizes the mechanisms reviewed in Sections 3-5 into four analytical levels, each characterized by specific risk indicators, enabling conditions, and countermeasure anchors.

The framework is designed for simultaneous multi-level deployment: the cross-level interaction dynamics documented in the empirical cases reviewed in Section 5 demonstrate that isolated single-level intervention is structurally insufficient. Indicator sets, enabling conditions, and countermeasures were derived deductively from the reviewed literature and reviewed for logical consistency and non-redundancy across levels.

Table 2. Multi-Level Diagnostic Framework (MLDF) for Ethical Fading in Complex Organizations.

Level	Risk Indicators	Enabling Conditions	Countermeasure Anchors
I - Individual	Moral licensing patterns; rationalization language in decision records; declining ethical self-reporting; high stress combined with reduced deliberation time; self-serving interpretive asymmetry in post-decision accounts	High cognitive load and decision fatigue; absence of structured deliberation; ambiguous performance metrics; prior moral compromise; low dispositional moral attentiveness; role-based authority reducing felt accountability	Ethical mindfulness training; structured decision pauses embedded in operational procedures; moral attentiveness assessment in selection and development; regular ethics reflection protocols; role-integrated rather than standalone ethics training; peer accountability structures
II - Group	Absence of ethical dissent in group decisions; framing of misconduct as loyalty or mission effectiveness; suppression of whistleblowing; UPB prevalence; groupthink indicators in meeting records; ethical contagion from leadership behavior	Strong cohesion with low psychological safety; peer loyalty and identity-protective communication norms; collective rationalization cultures; leadership modeling of moral disengagement; absence of structured dissent mechanisms	Psychological safety audits; structured adversarial review embedded in decision processes; OMD measurement instruments; protected reporting mechanisms independent of line management; leadership development emphasizing ethical dissent modeling

Level	Risk Indicators	Enabling Conditions	Countermeasure Anchors
III - Organizational	Compliance-only ethics programs without behavioral monitoring; ethics incidents normalized in performance reviews; absence of ethical climate assessment; ethical violations concentrated in high-performance units; procedural compliance substituting for moral deliberation	BLM incentive structures; self-interest ethical climate; routinized compliance without deliberation; deep hierarchy with diffuse accountability; strong isomorphic field pressures normalizing ethically questionable practices	Ethical culture diagnosis; balanced performance metrics incorporating ethical process criteria; third-party ethics audits; leadership development embedding ethical deliberation; ethics integrated into strategic planning; IRGC risk governance protocols for proactive monitoring
IV - Technological	Uncritical algorithmic output acceptance; absence of human override records; accountability attributed to systems; reduced ethical deliberation in AI-assisted decisions; black-box opacity preventing ethical evaluation; automation bias indicators in decision patterns	Black-box opacity; automation bias; weak human oversight protocols; absence of AI ethics governance; misalignment between algorithmic objective functions and institutional ethical standards; deployment without joint socio-technical optimization	EU AI Act compliance planning; explainable AI requirements as organizational standard; mandatory human override documentation; AI ethics training for operators and decision-makers; algorithmic impact assessments; socio-technical redesign of oversight roles; organizational AI ethics boards with cross-functional authority

Source: Author's elaboration based on reviewed literature.

6.2. Cross-Level Interaction Dynamics

A critical analytical feature of the MLDF is its recognition that ethical fading at different levels is not independent, cross-level interaction effects are essential to understanding the systemic character of moral erosion and cannot be neglected without producing a fundamentally incomplete diagnostic picture. The framework identifies three principal cross-level interaction pathways, illustrated in Figure 1 and grounded in the empirical cases reviewed in Section 5 and the theoretical mechanisms developed in Sections 3-5.

The top-down amplification pathway (solid descending arrow) describes how organizational-level structural factors create enabling conditions for group and individual-level ethical fading: the Obermeyer et al. (2019) healthcare algorithm case illustrates this directly, as organizational cost-optimization pressure shaped the algorithm's objective function, which then suppressed individual clinicians' ethical scrutiny through automation bias.

The bottom-up normalization pathway (solid ascendant arrow) operates in reverse: individual bounded ethicality, when exhibited by multiple actors under structurally similar conditions, aggregates into group rationalization norms and subsequently into organizational cultural drift, as illustrated by the COMPAS case, in which individual judicial automation bias became a field-wide norm of algorithmic deference eroding individualized due process.

The technological interaction pathway (dashed bidirectional arrow) describes how algorithmic systems interact simultaneously with all three human levels, amplifying ethical fading under weak moral ecologies and attenuating it where strong ethical cultures, explainability requirements, and override cultures are in place. The self-reinforcing character of all three pathways (and the way each feeds back into the others) explains why ethical fading is so resistant to isolated single-level interventions, and why the MLDF's countermeasures are designed for simultaneous multi-level deployment.

Figure 1 illustrates the four analytical levels of the MLDF arranged in ascending order of structural persistence and institutional embeddedness. The dashed outer container represents isomorphic field pressures (institutional theory) operating across the entire framework.

6.3. Integration with Adjacent Frameworks

The MLDF's systemic character is reinforced by its explicit integration

with the adjacent frameworks reviewed in Section 3.5, each of which contributes a dimension of analytical purchase not available from behavioral ethics alone.

Institutional theory (DiMaggio and Powell, 1983; Scott, 2014) informs the organizational-level enabling conditions by identifying isomorphic field pressures as a structural driver of ethical fading that operates above the level of individual organizations.

but whether it is embedded in an organizational field where ethically questionable practices have become institutionally normalized. Ethics auditing that focuses exclusively on individual organizational characteristics will systematically underestimate ethical fading risk in isomorphically pressured fields.

Risk governance frameworks (IRGC, 2017; Renn, 2008) provide both a process template and a conceptual vocabulary for

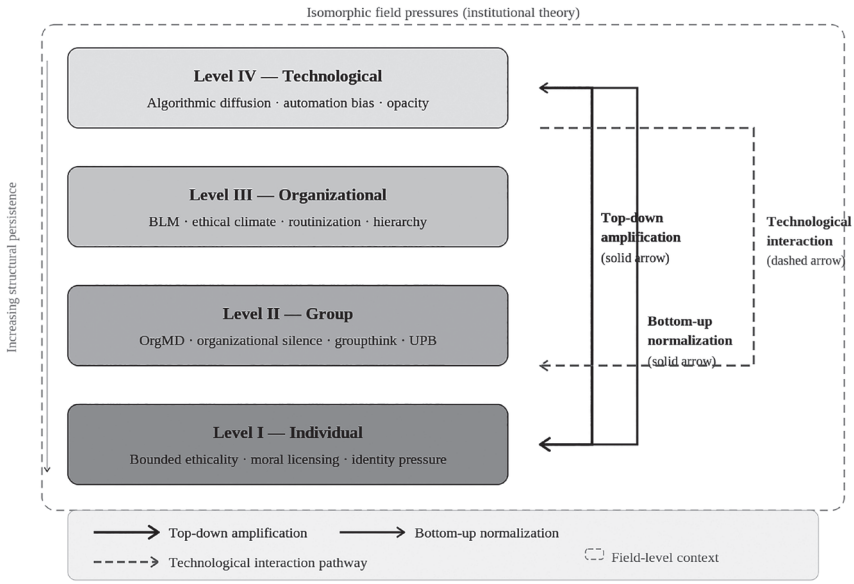

Figure 1. Multi-Level Diagnostic Framework (MLDF): Cross-Level Interaction Architecture. Source: Author's elaboration.

The MLDF's organizational-level diagnostic protocol should therefore include assessment of field-level normalization dynamics, not only whether the organization in question exhibits ethical fading,

deploying the MLDF in practice. The IRGC's phased governance model (*pre-assessment, appraisal, characterization, evaluation, management*) maps directly onto the MLDF's three operational

modes: pre-assessment and appraisal correspond to *diagnostic mode*, characterization and evaluation correspond to *preventive mode*, and management corresponds to *investigative mode* in the post-incident context. The risk governance emphasis on early warning systems and organizational resilience reinforces the MLDF's preventive orientation: the framework is most valuable when applied prospectively to identify and address ethical fading risk before failure occurs, rather than retrospectively to assign blame after it has.

6.4. Application Protocol

The MLDF supports three operational modes:

- *Diagnostic mode* - the risk indicators serve as a structured assessment instrument enabling simultaneous mapping of ethical fading risk profiles across all four levels, producing a level-by-level risk register that identifies where the organization is most exposed and which enabling conditions require priority attention;
- *Preventive mode* - the enabling conditions guide the design of proactive governance interventions before fading reaches detectable levels, particularly relevant for organizations launching new AI-assisted decision systems or undergoing rapid structural change;
- *Audit mode* - the countermeasure anchors function as evaluation criteria for assessing the adequacy of existing ethics governance infrastructure against each level's specific vulnerability profile.

Across all three modes, the MLDF is operationalizable through existing instruments: Kaptein's (2008) Corporate Ethical Virtues scale for Level III, Reynolds' (2008) Moral Attentiveness Scale for Level I, and Fida et al.'s (2025) OMD instrument for Levels II-III.

7. DISCUSSION

The reframing of ethical fading as a systemic multilevel vulnerability has direct implications for governance design. Frameworks that concentrate ethical accountability at the individual level (codes of conduct, individual ethics training, and misconduct investigation) are not simply incomplete; they are systematically misleading, directing attention away from where systemic failure originates.

Effective governance must simultaneously address cognitive vulnerabilities at Level I, social amplification dynamics at Level II, structural incentives and cultural norms at Level III, and accountability

gaps in the technological layer. The MLDF provides a structured template for this multilevel governance architecture, compatible with both the IRGC risk governance process model and the EU AI Act's high-risk system governance requirements.

Organizations characterized by deep hierarchical authority, sustained operational pressure, strong mission-driven identity, expanding AI decision support, and performance-above-ethics incentive structures (including defense institutions, healthcare systems, financial institutions, and large public bureaucracies) face a convergent set of enabling conditions across all four MLDF levels simultaneously.

For such organizations, preventive application of the MLDF is especially valuable, because ethical failure consequences are amplified by operational stakes, public accountability, and institutional trust dependencies. The defense and security context is particularly relevant: classification-based opacity, command hierarchy, mission primacy, and algorithmic decision support in operational contexts constitute a near-complete enabling condition profile at all four levels.

The emergence of the technological level as a structurally distinct ethical fading pathway represents a significant and underappreciated governance development. As argued in Section 5.7, the EU AI Act's compliance architecture risks reproducing the procedural displacement dynamic identified at Level III unless organizations simultaneously redesign the social conditions that make oversight mechanisms function as genuine ethical safeguards. Organizations that classify AI ethics governance as a compliance function rather than a strategic leadership responsibility are structurally unlikely to achieve the deliberative culture and override practices that meaningful human oversight requires.

Embedding AI ethics accountability at executive level (through dedicated cross-functional ethics boards and leadership performance criteria incorporating ethical oversight quality) is the organizational design response the MLDF's cross-level interaction analysis supports.

This article has several limitations that future research should address. The MLDF rests on a structured theoretical review rather than empirical validation; prospective work should develop and validate psychometrically sound instruments for each level's risk indicators, building on Kaptein's (2008) CVV scale, Fida et al.'s (2025) OMD instrument, and Reynolds' (2008) Moral Attentiveness Scale.

The cross-level interaction pathways are theoretically derived; longitudinal empirical research is needed to establish direction, magnitude, temporal dynamics, and boundary conditions across organizational types and cultural contexts.

The reviewed literature is primarily English-language and represents predominantly Western settings; cross-cultural validation is necessary before applying the MLDF in non-Western institutional contexts. Finally, the technological level will require iterative updating as research on AI-induced moral diffusion and explainability governance matures.

8. CONCLUSIONS

This article has argued that ethical fading constitutes a systemic organizational vulnerability that cannot be adequately understood, diagnosed, or addressed through individual-level analysis and intervention alone.

Through a structured theoretical review integrating behavioral ethics, organizational behavior, leadership research, AI governance, institutional theory, risk governance, and socio-technical systems theory, the article has traced the mechanisms through which moral erosion operates at individual, group, organizational, and technological levels, demonstrating that these mechanisms interact in mutually reinforcing ways that make ethical failure systemic rather than episodic and institutional rather than personal.

The proposed Multi-Level Diagnostic Framework (MLDF) advances the field in three ways beyond prior work. First, it provides analytically sharp distinctions between the three core constructs (ethical fading, moral disengagement, and normalization of deviance) showing that they are sequentially related as root condition, amplifying pathway, and institutionalizing outcome, rather than alternative explanations. This sequential causal logic is the theoretical core of the framework and the primary basis for its multilevel architecture.

Second, it grounds the technological level in empirical evidence from documented algorithmic decision failures in healthcare (Obermeyer et al., 2019), criminal justice (COMPAS), and financial services (Flash Crash), moving AI-ethics integration beyond regulatory reference to organizational reality and providing concrete diagnostic anchors for the Level IV risk indicators. Third, it draws on institutional theory, risk governance, and socio-technical systems theory to explain how ethical fading propagates across organizational levels and fields, and to generate cross-level countermeasures that address technical and social

dimensions simultaneously rather than in isolation.

The theoretical and practical urgency of this work is underscored by two converging trends that show no sign of reduction. The first is the increasing institutional complexity of contemporary organizations (through digitalization, globalization, regulatory proliferation, and stakeholder multiplicity) which systematically multiplies the enabling conditions for ethical fading across all four levels while reducing the organizational deliberative capacity available to manage them.

The second is the accelerating integration of algorithmic decision support into organizational processes across virtually every sector, which creates a qualitatively new and empirically documented pathway for moral responsibility diffusion that existing ethics frameworks, designed for purely human systems, are structurally ill-equipped to address.

As organizational environments become simultaneously more complex and more automated, the capacity to detect, diagnose, and interrupt ethical fading across all organizational levels and their interactions becomes an increasingly critical competence for governance, leadership, and institutional resilience, and the development of validated instruments for doing so becomes an increasingly urgent research priority.

DATA AVAILABILITY STATEMENT

All sources underlying the findings of this theoretical review are referenced in the bibliography. No proprietary or restricted datasets were used. The full set of reviewed sources is available upon reasonable request from the corresponding author.

DECLARATION OF GENERATIVE AI AND AI-ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

The author acknowledges utilizing the following generative AI tools during manuscript preparation: Anthropic Claude (claude.ai). This tool served for structural assistance, literature synthesis support, and language refinement. All AI-assisted content was reviewed, validated, and substantially revised by the author, who assumes complete responsibility for the final manuscript's accuracy, scientific integrity, and originality.

REFERENCES

[1] Aquino, K., and A. Reed. 2002. "The Self-Importance of Moral Identity." *Journal of Personality and Social Psychology* 83 (6): 1423-1440. https://doi.org/10.1037/0022-3514.83.6.1423

[2] Bandura, A. 1999. "Moral Disengagement in the Perpetration of Inhumanities." *Personality and*

Social Psychology Review 3 (3): 193--209. https://doi.org/10.1207/s15327957pspr0303_3

[3] Bandura, A. 2016. *Moral Disengagement: How People Do Harm and Live with Themselves.* New York: Worth Publishers. ISBN: 978-1-4641-6005-0

[4] Banja, J. 2010. "The Normalization of Deviance in Healthcare Delivery." *Business Horizons* 53 (2): 139-148. https://doi.org/10.1016/j.bushor.2009.10.006

[5] Baxter, G., and I. Sommerville. 2011. "Socio-Technical Systems: From Design Methods to Systems Engineering." *Interacting with Computers* 23 (1): 4-17. https://doi.org/10.1016/j.intcom.2010.07.003

[6] Bazerman, M. H., and A. E. Tenbrunsel. 2011. *Blind Spots: Why We Fail to Do What's Right and What to Do about It.* Princeton: Princeton University Press. https://www.jstor.org/stable/j.ctt7t89s. Accessed on: April 4, 2026.

[7] Danaher, J. 2022. "Tragic Choices and the Virtue of Techno-Responsibility Gaps." *Philosophy and Technology* 35 (2): 26. https://doi.org/10.1007/s13347-022-00519-1

[8] DiMaggio, P. J., and W. W. Powell. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48 (2): 147-160. https://doi.org/10.2307/2095101

[9] Ebrahimi, S., and C. Matt. 2024. "Not Seeing the (Moral) Forest for the Trees? How Task Complexity and Employees' Expertise Affect Moral Disengagement with Discriminatory Data Analytics Recommendations." *Journal of Information Systems* 39 (3): 477-502. https://doi.org/10.1177/02683962231181148

[10] European Union. 2024. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). *Official Journal of the European Union.* Brussels: European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

[11] Fida, R., I. Skovgaard-Smith, C. Barbaranelli, M. Paciello, R. Searle, I. Marzocchi, and M. Ronchetti. 2025. "The Suspension of Morality in Organisations: Conceptualising Organisational Moral Disengagement and Testing its Role in Relation to Unethical Behaviors and Silence." *Human Relations* 78 (8): 959-994. https://doi.org/10.1177/00187267241300866

[12] Financial Stability Oversight Council (FSOC). 2024. *Annual Report 2024.* Washington, DC: U.S. Department of the Treasury. https://home.treasury.gov/system/files/261/FSOC2024AnnualReport.

pdf Accessed on: April 4, 2026.

[13] Graham, K. A., C. J. Resick, J. A. Margolis, P. Shao, M. B. Hargis, and J. D. Kiker. 2020. "Egoistic Norms, Organizational Identification, and the Perceived Ethicality of Unethical Pro-Organizational Behavior: A Moral Maturation Perspective." *Human Relations* 73 (7): 1249-1277. https://doi.org/10.1177/0018726719862851

[14] Greenbaum, R. L., M. B. Mawritz, and G. Eissa. 2012. "Bottom-Line Mentality as an Antecedent of Social Undermining and the Moderating Roles of Core Self-Evaluations and Conscientiousness." *Journal of Applied Psychology* 97 (2): 343-359. https://doi.org/10.1037/a0025217

[15] International Risk Governance Council (IRGC). 2017. *An Introduction to the IRGC Risk Governance Framework, Revised Version.* Lausanne: EPFL International Risk Governance Center. https://irgc.org/risk-governance/irgc-risk-governance-framework/ Accessed on: April 4, 2026.

[16] Janis, I. L. 1972. *Victims of Groupthink: A Psychological Study of Foreign-Policy Decisions and Fiascoes.* Boston: Houghton Mifflin. WorldCat: https://www.worldcat.org/oclc/463679

[17] Kaptein, M. 2008. "Developing and Testing a Measure for the Ethical Culture of Organizations: The Corporate Ethical Virtues Model." *Journal of Organizational Behavior* 29 (7): 923-947. https://doi.org/10.1002/job.520

[18] Kaptein, M. 2023. *Why Good People Sometimes Do Bad Things: 52 Reflections on Ethics at Work.* Rotterdam: Erasmus Research Institute of Management. https://repub.eur.nl/pub/124738/Why-good-people-sometimes-do-bad-things.pdf Accessed on: April 4, 2026.

[19] Kuenzi, M., D. M. Mayer, and R. L. Greenbaum. 2020. "Creating an Ethical Organizational Environment: The Relationship between Ethical Leadership, Ethical Organizational Climate, and Unethical Behavior." *Personnel Psychology* 73 (1): 43-71. https://doi.org/10.1111/peps.12356

[20] Kump, B., and M. Scholz. 2022. "Organizational Routines as a Source of Ethical Blindness." *Organization Theory* 3 (2). https://doi.org/10.1177/26317877221075640

[21] Lammers, J., and D. A. Stapel. 2009. "How Power Influences Moral Thinking." *Journal of Personality and Social Psychology* 97 (2): 279-289. https://doi.org/10.1037/a0015437

[22] Logg, J. M., J. A. Minson, and D. A. Moore. 2019. "Algorithm Appreciation: People Prefer Algorithmic to Human Judgment."

Organizational Behavior and Human Decision Processes 151: 90--103. https://doi.org/10.1016/j.obhdp.2018.12.005

[23] Merritt, A. C., D. A. Effron, and B. Monin. 2010. "Moral Self-Licensing: When Being Good Frees Us to Be Bad." *Social and Personality Psychology Compass* 4 (5): 344-357. https://doi.org/10.1111/j.1751-9004.2010.00263.x

[24] Messick, D. M., and M. H. Bazerman. 1996. "Ethical Leadership and the Psychology of Decision Making." *Sloan Management Review* 37 (2): 9-22. https://sloanreview.mit.edu/article/ethical-leadership-and-the-psychology-of-decision-making/ Accessed on: April 4, 2026.

[25] Milgram, S. 1963. "Behavioral Study of Obedience." *Journal of Abnormal and Social Psychology* 67 (4): 371-378. https://doi.org/10.1037/h0040525

[26] Mishra, M., and N. Uppal. 2025. "Silence of Observers of Unethical Pro-Organizational Behavior." *Journal of Business Ethics* https://doi.org/10.1002/job.2892

[27] Mitchell, M. S., A. L. Hetrick, M. B. Mawritz, B. D. Edwards, and R. L. Greenbaum. 2023. "Oh the Anxiety! The Anxiety of Supervisor Bottom-Line Mentality and Mitigating Effects of Ethical Leadership." *Journal of Management* 50 (7): 2888-2926. https://cdr.lib.unc.edu/downloads/mg74r153w Accessed on: April 4, 2026.

[28] Moore, C., J. R. Detert, L. K. Treviño, V. L. Baker, and D. M. Mayer. 2012. "Why Employees Do Bad Things: Moral Disengagement and Unethical Organizational Behavior." *Personnel Psychology* 65 (1): 1-48. https://doi.org/10.1111/j.1744-6570.2011.01237.x

[29] Morrison, E. W. 2023. "Employee Voice and Silence: Taking Stock a Decade Later." *Annual Review of Organizational Psychology and Organizational Behavior* 10: 79-107. https://doi.org/10.1146/annurev-orgpsych-120920-054654

[30] Obermeyer, Z., B. Powers, C. Vogeli, and S. Mullainathan. 2019. "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations." *Science* 366 (6464): 447-453. https://doi.org/10.1126/science.aax2342

[31] Pasmore, W. A. 1988. *Designing Effective Organizations: The Sociotechnical Systems Perspective.* New York: Wiley. ISBN 978-0471887850

[32] Renn, O. 2008. *Risk Governance: Coping with Uncertainty in a Complex World.* London: Earthscan. ISBN: 978-1-84407-291-0

[33] Reynolds, S. J. 2008. "Moral Attentiveness: Who Pays Attention to the Moral Aspects of Life?" *Journal of Applied Psychology* 93 (5): 1027-1041. https://doi.

org/10.1037/0021-9010.93.5.1027

[34] Scott, W. R. 2014. *Institutions and Organizations: Ideas, Interests, and Identities.* 4th ed. Thousand Oaks, CA: SAGE. ISBN: 978-1-4522-8606-3

[35] Simon, H. A. 1955. "A Behavioral Model of Rational Choice." *Quarterly Journal of Economics* 69 (1): 99-118. https://doi.org/10.2307/1884852

[36] Tenbrunsel, A. E., and D. M. Messick. 2004. "Ethical Fading: The Role of Self-Deception in Unethical Behavior." *Social Justice Research* 17 (2): 223-236. https://doi.org/10.1023/B:SORE.0000027411.35832.53

[37] Torraco, R. J. 2016. "Writing Integrative Literature Reviews: Using the Past and Present to Explore the Future." *Human Resource Development Review* 15 (4): 404-428. https://doi.org/10.1177/1534484316671606

[38] Trist, E. L., and K. W. Bamforth. 1951. "Some Social and Psychological Consequences of the Longwall Method of Coal-Getting." *Human Relations* 4 (1): 3-38. https://doi.org/10.1177/001872675100400101

[39] Umphress, E. E., and J. B. Bingham. 2011. "When Employees Do Bad Things for Good Reasons: Examining Unethical Pro-Organizational Behaviors." *Organization Science* 22 (3): 621-640. https://doi.org/10.1287/orsc.1100.0559

[40] Vaughan, D. 1996. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA.* Chicago: University of Chicago Press. ISBN 978-0226851761

[41] Victor, B., and J. B. Cullen. 1988. "The Organizational Bases of Ethical Work Climates." *Administrative Science Quarterly* 33 (1): 101-125. https://www.jstor.org/stable/2392857

[42] Zhu, W., R. E. Riggio, B. J. Avolio, and J. J. Sosik. 2011. "The Effect of Leadership on Follower Moral Identity: Does Transformational/Transactional Style Make a Difference?" *Journal of Leadership and Organizational Studies* 18 (2): 150-163. https://doi.org/10.1177/154805181039671

COGNITIVE WARFARE AND ITS SOCIETAL IMPACT: MANIPULATION, TRUST AND DEMOCRATIC RESILIENCE

Brînduşa Maria Popa[1]

Regional Department of Defense Resources Management Studies, (DRESMARA) / "Carol I" National Defense University, Brasov, Romania

Cognitive warfare has emerged as a defining feature of contemporary conflict, shifting the focus from physical domains to the manipulation of perception, cognition and societal behavior. This conceptual review article examines the societal impact of cognitive warfare, with particular emphasis on mechanisms of manipulation, the erosion of public trust and the implications for democratic resilience, the challenges democratic societies face in responding to cognitive warfare while preserving fundamental rights, particularly freedom of expression. It argues that strengthening societal resilience requires a balanced approach that safeguards democratic values while countering manipulation.

Drawing on interdisciplinary perspectives from political science, security studies and cognitive psychology, the paper analyses how state and non-state actors exploit digital platforms, information ecosystems and psychological vulnerabilities to influence public opinion. Real-world examples, including electoral interference and disinformation campaigns during global crises, illustrate the tangible consequences of such strategies.

The findings suggest that prolonged exposure to cognitive warfare contributes to polarization, declining institutional trust and weakened democratic participation, effects that can be mitigated through media literacy, institutional transparency and adaptive governance while ensuring that countermeasures do not undermine the democratic principles they seek to protect.

Key words: *resilience, communication, disinformation, security, cognitive warfare.*

[1] ORCID ID: 0000-0002-3215-8000, e-mail: bpopa@mapn.ro

1. INTRODUCTION

Increasingly, conflict has been targeting cognition rather than territory, reflecting the rise of cognitive warfare—a form of strategic competition aimed at influencing how individuals and societies interpret reality. Its effects are subtle, cumulative and difficult to attribute, yet profoundly disruptive (Rid, 2020). This approach is part of a broader set of techniques aimed at subversively targeting the deeper structures of any particular institution or the society itself.

Contemporary events such as disinformation campaigns during the COVID-19 pandemic, influence operations related to the war in Ukraine and misleading narratives about migration in Europe demonstrate that modern conflict unfolds in complex information ecosystems, where narratives, emotions and trust are contested (WHO, 2020; European Commission, 2020).

Societal resilience—the ability of individuals, communities and institutions to withstand, adapt and recover from external disruptions—is central in this context. In democratic societies, resilience depends on public trust, access to reliable information and citizens' ability to critically evaluate competing narratives (OECD, 2021). Its development and expansion are essential for resisting such forms of conflict in this century of asymmetric threats.

While these dynamics are increasingly recognised, this article examines the societal impacts of cognitive warfare and its challenges to democracy, arguing that strengthening societal resilience requires strategies that balance protection against manipulation with the preservation of democratic values (Guess, Nagler and Tucker, 2020).

1.1 Methodology

This article adopts a conceptual and non-systematic review approach aimed at synthetising existing interdisciplinary literature to identify patterns, mechanisms and societal impacts of cognitive warfare.

The analysis is based on academic publications, policy reports and institutional documents produced by organizations such as NATO the European Commission, WHO, OECD. No primary data collection was undertaken. Case examples and literature were selected through a non-systematic, but structured review of articles, official reports from NATO, as well as relevant works in the domain prioritizing sources published between 2016 and 2023 to ensure relevance.

The selection process followed a structured, but non exhaustive strategy, prioritizing influential and recent publications. Case examples were included to support conceptual arguments, rather than to provide empirical comparison.

The objective of this approach is not to test hypotheses, but to identify patterns, mechanisms and societal implications of cognitive warfare across different contexts.

2. CONCEPTUAL FRAMEWORK

Cognitive warfare encompasses strategies aimed at influencing perceptions, decision-making and social behavior, operating in informational, psychological, and cultural domains (NATO, 2021). Unlike traditional military operations, which rely on physical force or conventional information warfare, which focuses on disrupting communication systems, cognitive warfare targets the human mind directly. Its goal is to shape how individuals and communities interpret events, prioritize risks and make decisions.

Cognitive warfare can involve both state and non-state actors, ranging from governments seeking geopolitical advantage to ideological groups aiming to disrupt social cohesion. These actors leverage digital platforms, social media networks and other communication technologies to reach large populations efficiently. By tailoring narratives to specific cultural, social or demographic contexts, cognitive operations exploit existing societal divisions, psychological vulnerabilities and information gaps (Pomerantsev, 2019).

A critical feature of cognitive warfare is its dual objective: it simultaneously spreads targeted messages and undermines trust, creating confusion and destabilizing social cohesion. This combination weakens institutional legitimacy and erodes democratic processes, as public confidence in authorities, media and civil society becomes compromised (Rid, 2020). Unlike conventional threats, cognitive operations allow adversaries to influence societies without triggering overt retaliation.

Throughout history, cognitive strategies have existed in forms such as propaganda, psychological operations and ideological campaigns. What differentiates modern cognitive warfare is the scale, speed and precision enabled by digital connectivity. Artificial intelligence, algorithm-driven content distribution and micro-targeted advertising amplify messages across platforms, often bypassing traditional checks on accuracy.

Disinformation campaigns exploiting algorithmic amplification can reach millions within hours, shaping discourse and behavior before fact-checking or official responses can intervene (Bradshaw & Howard, 2019). For example, analysis of more than 14 million election-related tweets from the 2016

U.S. presidential campaign revealed that social bots were responsible for a disproportionate share of links to low-credibility sources, amplifying misinformation before fact-checking could intervene. These bots accounted for roughly 9–15% of all such links, demonstrating how algorithmic dynamics can rapidly propel false content through networks (Shao et al., 2018).

In practice, cognitive warfare operates across multiple layers:

- Individual level: influencing beliefs, attitudes and decision-making.
- Community level: exploiting social networks to amplify divisions and polarize discourse.
- Institutional level: undermining public trust, organizational credibility and policy effectiveness.

Thus, understanding cognitive warfare requires a multidisciplinary approach, integrating insights from psychology, communications, political science, cybersecurity and sociology. Its pervasive nature means that societies must treat it not just as a military or cybersecurity concern, but as a fundamental social challenge, impacting public trust, democratic legitimacy and societal resilience (Rid, 2020; NATO, 2021).

2.1 Differentiating cognitive warfare from other adjacent concepts

To prevent conceptual overreach and make the paper's argumentation more precise, it is essential to differentiate cognitive warfare from related terms. Table 1, presented below, aims to clarify such distinction and show that cognitive warfare is broader than disinformation, but narrower than hybrid warfare, with a unique focus on manipulating how societies process reality.

Table 1. Conceptual Distinctions between Cognitive Warfare and Adjacent Concepts

Concept	Definition	Distinction from cognitive warfare
Disinformation	Deliberately false or misleading information intended to deceive.	A tactic within cognitive warfare not the overarching strategy.
Propaganda	Systematic dissemination of information (biased or misleading) to promote a political cause or point of view.	Propaganda is mostly one-way interaction while cognitive warfare is interactive, adaptive and feedback driven.

Concept	Definition	Distinction from cognitive warfare
Information warfare	Manipulation of information and information systems through means like disruption of communication systems and data integrity.	It focuses on technical and infrastructure elements, not directly on human cognition.
Hybrid warfare	Combination of conventional and unconventional methods (military, cyber, economic)	Cognitive warfare is a component of hybrid warfare which targets the mind.
Psychological operations (PSYOPS)	Military-led activities to influence emotions and behavior.	They are typically state-driven and tactical. Cognitive warfare includes non-state actions and strategic societal manipulation.

(Based on author's analysis)

3. MECHANISMS OF COGNITIVE WARFARE

Cognitive warfare employs multiple methods simultaneously, combining information, technology and psychology to shape public perceptions.

3.1 Disinformation and narrative manipulation

Disinformation refers to deliberately false or misleading information designed to confuse, mislead or manipulate public perception (Wardle and Derakhshan, 2017). Unlike accidental misinformation, disinformation is intentional and often structured to exploit social vulnerabilities or pre-existing biases.

During the COVID-19 pandemic, disinformation campaigns circulated false claims regarding vaccine safety, virus origins and government health measures. Social media platforms and encrypted messaging apps amplified these narratives, contributing to public confusion and lower compliance with official guidance (World Health Organization [WHO], 2020).

In Europe, migration-related disinformation portrayed certain groups as existential threats, exacerbating societal tensions and fueling political polarization (European Commission, 2020).

Narrative manipulation often follows strategic framing: events are presented selectively to evoke emotional responses such as fear, outrage or moral indignation. By controlling the framing, cognitive actors can shift public opinion and normalize extreme positions over time (Pomerantsev, 2019).

3.2 Algorithmic amplification

Digital platforms rely on algorithms designed to maximize user engagement, often prioritizing sensational or polarizing content. Cognitive actors exploit this by crafting messages optimised for virality, effectively amplifying their impact without requiring mass coordination (Bradshaw and Howard, 2019). For instance, migration-related narratives in European countries were algorithmically amplified, exaggerating crime statistics or portraying minority groups as security threats. This process creates echo chambers, where individuals are repeatedly exposed to similar content, reinforcing existing biases and intensifying societal divisions (Allcott et al., 2020). Algorithmic amplification thus transforms disinformation campaigns into widespread social phenomena, influencing discourse and even political behavior.

3.3 Psychological targeting

Psychological targeting tailors messages to specific groups or individuals based on emotional, cultural and cognitive characteristics. This includes appeals to fear, identity, moral outrage or in-group loyalty, making narratives more persuasive and resistant to counter-messaging (Pomerantsev, 2019).

During conflicts in Eastern Europe, coordinated campaigns targeted both domestic and international populations with emotionally charged narratives that reinforced pre-existing social divisions. Such campaigns exploited uncertainty and fear to influence attitudes toward government policies, international organizations and foreign actors (Giles, 2016). By manipulating emotional responses, cognitive warfare can drive behavioral change, encourage self-censorship and shape public discourse without overt coercion.

3.4 Networked and coordinated Manipulation

Cognitive warfare increasingly relies on networked actors and automated tools. Bot networks, troll farms and coordinated inauthentic accounts amplify targeted messages, creating the illusion of grassroots support (astroturfing) or consensus. These coordinated campaigns can manipulate trending topics, distort public perception of popular opinion, and pressure policymakers to respond to perceived social demands (Bradshaw and Howard,

2019). For example, coordinated online campaigns during the Ukraine conflict spread narratives to both local and global audiences, combining emotionally charged imagery, selective facts and fabricated reports. The cumulative effect was not only confusion, but also diminished trust in news sources, humanitarian organizations and international institutions (Giles, 2016).

3.5 Integrated societal effects

The combination of disinformation, algorithmic amplification, psychological targeting and coordinated network activity generates pervasive cognitive shockwaves. Citizens struggle to identify reliable sources, social cohesion erodes and public discourse becomes highly polarised (Rid, 2020).

Moreover, these effects are self-reinforcing: exposure to manipulated content increases skepticism toward alternative viewpoints, making individuals more susceptible to subsequent campaigns. Over time, this creates an environment in which misinformation becomes normalised, trust in institutions diminishes and collective decision-making is impaired (Bradshaw and Howard, 2019).

By targeting multiple levels—individual, community and institutional—cognitive warfare produces structural societal impacts that extend beyond immediate events. The goal is not simply to disseminate false information, but to reshape the cognitive environment, influencing social norms, political participation and policy outcomes over the long term (Rid, 2020).

4. SOCIETAL IMPACT OF COGNITIVE WARFARE

Cognitive warfare affects more than individual perceptions; its effects ripple through society, reshaping behaviors, social norms and institutional trust (Rid, 2020). These impacts are structural, cumulative and multi-dimensional, influencing democratic governance, policy implementation and social cohesion.

4.1 Polarization and social fragmentation

One of the most visible effect is societal polarization. Disinformation campaigns often exploit pre-existing divisions—political, ethnic, religious or cultural—amplifying disagreements into entrenched societal fault lines (European Commission, 2020). This phenomenon is evident in several European countries, where migration-related disinformation exaggerated perceived threats posed by immigrant communities, prompting local populations to adopt more extreme positions. Such polarization hindered consensus-building on social and

policy matters, making cooperative decision-making more difficult and weakening democratic governance (Bradshaw and Howard, 2019).

Polarization also manifests in online environments. Social media platforms, by prioritizing engagement over accuracy, reinforce echo chambers, where individuals are repeatedly exposed to similar views and rarely encounter alternative perspectives (Allcott et al., 2020). The cumulative effect is a fragmented public discourse that erodes mutual understanding and trust between societal groups.

Research on migration discourse shows that social media and digital information environments have the power to amplify misleading narratives about migration and migrants, reinforcing biased interpretations and accelerating the spread of misinformation that influences public perception and fuels societal divisions (Komendantova et al., 2023). Evidence of this can be seen in the rapid diffusion of migration-related misinformation and fake news across social media platforms such as Facebook and X. Refugee-focused disinformation frequently identified by international fact-checking organizations among the most widely shared content, illustrating how algorithmic sharing dynamics can reinforce biased or misleading narratives before effective corrective responses occur (Olaru, 2023).

4.2 Erosion of public and institutional trust

Repeated exposure to conflicting, misleading or manipulated information undermines confidence in both authorities and institutions (Rid, 2020). At the public level, this manifests as declining trust in government, scientific bodies and mainstream media. During the COVID19 pandemic, widespread misinformation regarding vaccines, treatments and public health policies contributed to heightened skepticism among citizens. Countries with inconsistent communication or opaque decision-making experienced lower compliance with health measures and increased susceptibility to conspiracy theories (WHO, 2020).

Similarly, migration-related disinformation and other targeted campaigns have been shown to exaggerate perceived threats, prompting individuals to adopt more extreme positions and reinforcing societal divisions, thereby decreasing confidence in democratic processes and public institutions (Bradshaw and Howard, 2019). Such erosion of public trust impedes collective action and diminishes societal resilience in the face of crises.

Institutional trust is also affected, as manipulated narratives can diminish the credibility, legitimacy and operational capacity of organizations themselves. In political contexts, misinformation

surrounding elections, policy decisions or international agreements reduces confidence in democratic institutions, impairing their effectiveness (OECD, 2021).

Likewise, during the Ukraine conflict, coordinated online campaigns targeted humanitarian organizations and official reporting channels, generating doubt about operational integrity and impartiality. The resulting mistrust complicated both domestic and international responses, illustrating how cognitive warfare can produce lasting societal and operational consequences (Giles, 2016).

Together, these examples demonstrate that misinformation and cognitive warfare do not only affect individual perceptions, but also compromise institutional resilience, creating a feedback loop where declining public trust further undermines the credibility and effectiveness of key organizations. Addressing these challenges requires strengthening both societal awareness and institutional transparency to preserve democratic governance and societal cohesion.

4.3 Behavioral shifts and risk aversion

Cognitive warfare campaigns also influence individual and collective behaviors. Fear-based narratives and emotionally charged content can make populations more risk-averse, less willing to engage in public life, or more prone to adopting self-protective behaviors based on misinformation (Pomerantsev, 2019).

This is evident in online campaigns exaggerating crime or security threats associated with migration, which led some communities to reduce social engagement and participation in local governance. Political mobilization can also be affected, as manipulated narratives discourage voting or create overreliance on partisan information channels (Bradshaw and Howard, 2019).

These behavioral shifts reinforce societal divisions, creating feedback loops that amplify the effectiveness of cognitive warfare campaigns and extend their impact over time (Rid, 2020).

5. DEMOCRATIC CHALLENGES AND POLICY DILEMMAS

Cognitive warfare presents long-term, structural challenges to democratic societies. Beyond immediate disinformation or manipulated narratives, persistent exposure erodes trust in institutions, deepens social polarization and normalizes misinformation, ultimately weakening collective decision-making and civic engagement (Rid, 2020; OECD, 2021). Citizens may become less willing to collaborate, less trusting

of authorities and more vulnerable to future manipulation.

Democracies face a unique dilemma in responding to these threats. Constitutional protections—such as freedom of expression, privacy and open debate—limit the tools governments can use to counter manipulation (Nissenbaum, 2010). Policymakers must balance the risk of underreaction, which allows cognitive attacks to spread and amplify societal divisions, with the risk of overreaction, potentially infringing civil liberties, provoking public backlash and further eroding trust (Wardle and Derakhshan, 2017; Rid, 2020).

The complexity of digital platforms adds to the challenge. Algorithm-driven, decentralized networks facilitate the rapid spread of both factual and manipulative content, while asymmetric adversaries exploit these systems with bots, deepfakes, and targeted campaigns, often acting faster than democracies can respond (Bradshaw and Howard, 2019; European Commission, 2020; Nissenbaum, 2010).

Effectively addressing these challenges requires a multi-level approach that integrates societal awareness, institutional transparency and legally grounded policy interventions. Strengthening media literacy, fostering public engagement and maintaining adaptive, accountable governance are essential to preserve democratic norms while mitigating the long-term impacts of cognitive warfare (Guess, Nagler and Tucker, 2020; OECD, 2021).

5.1 Digital complexity and rapid evolution

Digital platforms amplify the complexity of democratic responses. Social media ecosystems are global, decentralised and algorithmically driven, enabling rapid dissemination of both factual and manipulative content (Bradshaw and Howard, 2019).

Policymakers struggle to monitor and mitigate disinformation without unintentionally affecting legitimate speech. This challenge became apparent during attempts to regulate online content amid migration crises, where measures intended to suppress harmful narratives were sometimes criticised as politically biased, demonstrating the difficulty of regulating information in a manner perceived as neutral and fair (European Commission, 2020).

Cognitive threats are often deployed by actors with minimal accountability, who exploit the openness of democratic societies. Such adversaries can use sophisticated tactics—bot networks, deepfakes and targeted micro-advertising—to manipulate specific populations without leaving clear evidence of coordination (Bradshaw and Howard, 2019).

Democratic institutions, in contrast, are constrained by checks, debates and procedural safeguards. This asymmetry creates a persistent

vulnerability: adversaries can act quickly, while democracies respond slowly and cautiously to avoid overstepping legal or ethical boundaries (Nissenbaum, 2010).

5.2 Societal participation and normative considerations

As is widely understood today, citizens in democracies are not passive recipients of information—they are active participants in public discourse. Responses to cognitive threats therefore cannot rely solely on top-down enforcement; they require societal engagement, education and trust-building (Guess, Nagler and Tucker, 2020).

Policymakers must integrate normative considerations into strategy: defending against manipulation without compromising democratic freedoms. This involves fostering critical thinking, promoting media literacy and reinforcing public trust in institutions, while carefully calibrating legal and regulatory interventions (OECD, 2021).

5.3 Multi-Level strategic response

The central challenge is both practical and ethical: how to preserve democratic norms while mitigating cognitive threats. Effective responses require:

- Multi-level coordination across government, civil society and media sectors.
- Transparent and accountable institutional practices.
- Education and empowerment of citizens to critically assess information.
- Technological solutions, including platform-level monitoring, that respect privacy and freedom of expression.

Ultimately, democratic resilience depends on the ability to integrate societal, institutional and legal strategies. Only by harmonizing protection, education and transparency can democracies counter cognitive warfare without undermining the very freedoms that define them (Rid, 2020; Nissenbaum, 2010).

6. STRENGTHENING SOCIETAL RESILIENCE

Societal resilience—the capacity of communities and institutions to anticipate, absorb, adapt to and recover from cognitive shocks—is central to countering contemporary information threats (Rid, 2020). Unlike traditional military risks, cognitive warfare exploits social vulnerabilities, requiring resilience to operate simultaneously at individual, institutional and systemic levels. Effective responses must therefore be proactive, enabling both citizens and institutions to recognize, resist and adapt to manipulation within increasingly complex information environments.

At the individual level, media literacy and critical thinking play a foundational role in reducing

susceptibility to disinformation. Education initiatives that strengthen citizens' ability to evaluate sources, detect bias and verify information contribute directly to informed civic participation and limit the societal reach of manipulative narratives (Guess, Nagler and Tucker, 2020).

At the institutional level, transparency, accountability and consistent communication reinforce public trust, which acts as a critical buffer against cognitive manipulation. Evidence from recent crises, including the COVID-19 pandemic, suggests that open and credible communication significantly reduces the impact of misleading narratives on public behavior (OECD, 2021; WHO, 2020).

At the systemic level, resilience depends on adaptive governance and cross-sector collaboration. Partnerships between governments, civil society, media organizations and technology platforms enable the timely detection and mitigation of disinformation, improving responsiveness in rapidly evolving digital environments (Bradshaw and Howard, 2019; European Commission, 2020).

At the same time, long-term resilience is supported by cultural and normative foundations that promote critical inquiry, trust and active civic engagement.

Ultimately, societal resilience is maximised when these dimensions are integrated into a coherent framework. The interaction between informed citizens, trustworthy institutions and adaptive governance structures strengthens social cohesion and democratic stability, enabling societies to absorb cognitive shocks without resorting to restrictive measures that could undermine fundamental rights (Nissenbaum, 2010).

To synthesise the analysis above, the main findings can be summarised as follows:

Table 2. Summary of cognitive warfare elements

Mechanism	Primary target	Societal effect	Policy response
Disinformation and narrative manipulation	Individual beliefs	Polarization, confusion	Media literacy, fact checking
Algorithmic amplification	Community discourse	Echo chamber, fragmentation	Platform regulation, transparency
Psychological targeting	Emotional/cognitive vulnerabilities	Risk aversion, behavioural shifts	Public awareness campaigns

Mechanism	Primary target	Societal effect	Policy response
Network coordination (bots, trolls)	Institutional trust	Erosion of credibility, legitimacy	Cross sector monitoring, legal frameworks
Integrated cognitive shockwaves	Entire society	Weakened democratic participation	Adaptive governance, civic engagement

(*Based on the author's analysis*)

7. RECOMMENDATIONS

Building on the dimensions of societal resilience outlined in the previous section, policy responses to cognitive warfare require the translation of these principles into coordinated policy and societal actions. Resilience must be operationalised across individual, institutional and systemic levels in order to address the multifaceted nature of cognitive threats.

At the individual level, media literacy and critical thinking should be integrated into formal education and complemented by public awareness initiatives, thus enabling citizens to navigate complex information environments.

At the institutional level, transparency, accountability and consistent public communication are critical in maintaining trust and limiting the impact of disinformation. Therefore, public authorities should adopt these principles and establish dedicated structures or rapid response mechanisms for identifying and countering manipulation campaigns thus enhancing institutional resilience.

At the systemic level, adaptive governance and cross-sector collaboration between governments, civil society, media and technology platforms enable the timely detection and mitigation of coordinated manipulation campaigns. Supporting independent fact-checking mechanisms further enhances information credibility and reinforces public confidence in verified sources. Policy makers should promote regulatory frameworks for digital platforms that are necessary to address algorithmic amplification and coordinated disinformation, while safeguarding freedom of expression and democratic norms.

Integrating these measures into a coherent and adaptive strategy ensures that societal resilience is not only reactive, but also preventive. By aligning education, institutional integrity and governance mechanisms, societies can effectively mitigate cognitive threats while preserving trust, social cohesion and democratic values.

8. CONCLUSIONS

Cognitive warfare represents a structural and evolving challenge to contemporary democratic societies, operating through indirect, cumulative mechanisms that target perception, trust and social cohesion. As demonstrated throughout this article, its impact extends beyond the dissemination of disinformation, affecting behavioral patterns, institutional legitimacy and the quality of public discourse. As a conceptual review, this article does not claim to present original empirical findings, but rather synthesises existing evidence to identify patterns and implications.

Unlike traditional forms of conflict, cognitive warfare exploits the openness of democratic systems, creating a persistent tension between safeguarding security and preserving fundamental freedoms. The findings highlight that vulnerability does not stem solely from technological exposure, but from underlying societal factors such as polarization, declining trust and limited critical media engagement.

In this context, societal resilience emerges as a central pillar in mitigating cognitive threats. However, resilience cannot be understood as a purely defensive capacity rather, it reflects the ability of societies to adapt, learn and maintain democratic integrity under conditions of informational pressure. Strengthening this resilience requires coordinated efforts across individual, institutional and systemic levels, ensuring that responses remain consistent with democratic norms and values.

Ultimately, the challenge of cognitive warfare is not only to counter manipulation, but also to strengthen the underlying cognitive and normative conditions that sustain democratic systems.

REFERENCES

[1] Allcott, H., Braghieri, L., Eichmeyer, S., & Gentzkow, M. (2020). *The welfare effects of social media*. *American Economic Review, 110*(3), 629676. https://doi.org/10.1257/aer.20190658

[2] Allen, J., Howland, B., Möbius, M., Rothschild, D., & Watts, D. J. (2020). *Evaluating the fake news problem at the scale of the information ecosystem*. Science Advances, 6(14), eaay3539. https://www.science.org/doi/10.1126/sciadv.aay3539

[3] Bennett, W. L., & Livingston, S. (2018). *The disinformation order: Disruptive communication and the decline of democratic institutions*. European Journal of Communication, 33(2), 122–139. https://doi.org/10.1177/0267323118760317

[4] Bjola, C., & Holmes, M. (2015). *Digital diplomacy: Theory and*

practice. Routledge.

[5] *Cyber influence and international security*. (2009). In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), Cyberpower and national security (pp. 343–361). Potomac Books.

[6] European Commission. (2020). *Joint communication on tackling COVID-19 disinformation: Getting the facts right*. European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0008

[7] European Commission. (2020). *A strengthened EU Code of Practice on Disinformation* https://commission.europa.eu/topics/countering-information-manipulation/strengthened-eu-code-practice-disinformation_en

[8] Giles, K. (2016*). Handbook of Russian information warfare: Challenging the skeptics*. NATO Strategic Communications Centre of Excellence. https://www.ndc.nato.int/download/handbook-of-russian-information-warfare-by-keir-giles/

[9] Guess, A., Nagler, J., & Tucker, J. (2020). *Less than you think: Prevalence and predictors of fake news dissemination on Facebook*. Science Advances, 6(7), eaay3539. https://pubmed.ncbi.nlm.nih.gov/30662946/

[10] Howard, P. N., & Bradshaw, S. (2018). *The global organization of social media disinformation campaigns*. Journal of International Affairs, 71(1.5)

[11] NATO Innovation Hub. (2021). Cognitive warfare. NATO. https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf

[12] Komendantova, N., Erokhin, D., & Albano, T. (2023). *Misinformation and its impact on contested policy issues: The example of migration discourses*. Societies, 13(7), 168. https://doi.org/10.3390/soc13070168

[13] Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

[14] Olaru, G. O. (2023). *The rapid diffusion of fake news: An analysis of content on migration, refugees, and conflict on international factchecking platforms*. *Connectist: Istanbul University Journal of Communication Sciences, Issue 65*, 61–87. https://doi.org/10.26650/CONNECTIST2023-1404666

[15] OECD. (2021). *Trust and public policy: How better governance can help rebuild public trust*. OECD Publishing. https://www.oecd.org/en/publications/trust-and-public-policy_9789264268920-en.html

[16] Pomerantsev, P. (2020). *This is not propaganda: Adventures in the war against reality*. Faber & Faber.

[17] Rid, T. (2020). *Active measures: The secret history of disinformation*

and political warfare. Farrar, Straus and Giroux.

[18] Shao, C., Ciampaglia, G. L., Varol, O., Yang, K.-C., Flammini, A., & Menczer, F. (2018). *The spread of low-credibility content by social bots. Nature Communications*, 9, 4787. https://doi.org/10.1038/s41467-018-06930-7

[19] Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making (Council of Europe Report DGI(2017)09)*. Council of Europe. https://www.firstdraftnews.org/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-de%CC%81sinformation-1.pdf

[20] World Health Organization, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, & IFRC. (2020, September 23). Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation. World Health Organization. https://www.who.int/news/item/23-09-2020-managing- the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation

THE LANGUAGE OF UNCERTAINTY: THE ROLE OF THE ACRONYMS VUCA, BANI, TUNA AND RUPT IN DESCRIBING THE CONTEMPORARY GEOPOLITICAL CONTEXT

Svetlana CEBOTARI[1]
Ion GUȚU[2]

Departament International Relations,
[1]Faculty of International Relations, Political and Administrative Studies,
Moldova State University, Military Academia
„ Alexandru cel Bun" of Armed Forces

Chișinău, Republic of Moldova
[2]Departament Department of Romance and Germanic, Faculty of Letters,
Moldova State University, Chișinău, Republic of Moldova

In recent decades, the world has undergone rapid and profound transformations driven by factors such as globalization, technological development, economic and health crises, as well as geopolitical conflicts. To better understand and communicate the complexity of today's global environment, experts in leadership, business, and international relations have turned to the use of conceptual acronyms such as VUCA, BANI, TUNA and RUPT. These frameworks synthesize the dominant features of contemporary reality-volatility, uncertainty, fragility, polarization, systemic tensions-and offer a useful interpretative lens for analyzing the international context. In a constantly changing world, where the boundaries between security and risk are increasingly blurred, these acronyms not only describe the state of the world but also highlight the need for the rapid adaptation of governance, leadership, and global cooperation strategies. This article aims to analyze the meaning and applicability of these concepts in understanding the current geopolitical environment.

Key words: *acronym, VUCA, TUNA, BANI, RUPT, geopolitics*

[1] ORCID ID: 0000-0001-9073-104, e-mail: svetlana.cebotari11@gmail.com
[2] ORCID ID: 0000-0002-8975-3353, e-mail: ion.gutu1@usm.md

1. INTRODUCTION

The geopolitical context of the 21st century is defined by a series of profound, accelerated, and often unexpected transformations that challenge classical models of analysis and forecasting. Phenomena such as asymmetric globalization, the rise of new power centers, hybrid conflicts, climate crises, the COVID-19 pandemic, as well as the proliferation of disinformation and new disruptive technologies (artificial intelligence, cyber warfare, biotechnology) shape an international environment marked by instability, ambiguity, and systemic uncertainty. In this context, traditional concepts of order, sovereignty, and security are becoming increasingly difficult to apply unequivocally. Thus, the need for synthetic and dynamic conceptual tools, capable of quickly capturing the changing nature of global realities, has led to the emergence and consolidation of analytical acronyms such as VUCA, BANI, TUNA, and RUPT. In this regard, the acronyms VUCA (Volatility, Uncertainty, Complexity, Ambiguity), TUNA (Turbulence, Uncertainty, Novelty, Ambiguity), BANI (Brittle, Anxious, Nonlinear, Incomprehensible), and RUPT (Rapid, Unpredictable, Paradoxical, Tangled) have established themselves as essential tools in the analysis of the global environment. These conceptual formulas facilitate the understanding of rapid changes, systemic instabilities, and emerging phenomena that influence international relations, global security, and governance strategies.

The acronym VUCA, initially introduced in the American military environment after the Cold War and later adopted in leadership and strategic analysis, reflects a world characterized by growing volatility and ambiguity (Chakraborty). TUNA, derived from VUCA, emphasizes novelty and turbulence, focusing on sudden transformations driven by technology, pandemics, or hybrid conflicts. BANI adds a psychosocial perspective, portraying a fragile, anxious, and hard-to-understand world, while RUPT highlights the accelerated pace and paradoxical nature of global events.

The use of these acronyms in current geopolitical analysis is not merely a semantic exercise but a methodological necessity. They provide adaptable interpretive frameworks that are useful in risk assessment, policy formulation, and decision-making in an international environment characterized by systemic uncertainty. Therefore, their role is crucial in understanding and managing the geopolitical challenges of the 21st century, marked by strategic rivalries, climate instability, asymmetric conflicts, and unprecedented technological transformations (Cascio, 2025).

All these acronyms provide useful conceptual frameworks for understanding the current international environment and for supporting decision-making processes under conditions of extreme uncertainty. They are not merely rhetorical formulas but true cognitive matrices that facilitate strategic analysis, risk anticipation, and the formulation of adaptable policies. In a context where the global order is in transition and the rules of the geopolitical game are being rewritten, these tools become essential for both state and non-state actors. Therefore, their study and application in contemporary geopolitical analysis represent a fundamental undertaking for understanding the complexity and dynamism of today's world.

2. METODOLOGY

The study *"The Language of Uncertainty: The Role of the Acronyms VUCA, BANI, TUNA and RUPT in Describing the Contemporary Geopolitical Context"* is interdisciplinary in nature, situated at the intersection of international relations, geopolitics, security studies, and discourse analysis (Smith, 2019). The research employs a qualitative analytical-interpretative approach aimed at examining how these acronyms conceptualize uncertainty and complexity within the contemporary geopolitical environment, as well as their role in shaping analytical discourse on global transformations. The research is predominantly qualitative, complemented by descriptive quantitative elements. The qualitative approach enables an in-depth investigation of the meanings and interpretations associated with the acronyms VUCA, BANI, TUNA, and RUPT in the specialized literature and in contemporary geopolitical analysis (Matejova & Shesterinina, 2023). At the same time, quantitative elements are used to highlight the frequency and contextual usage of these concepts across different types of academic and analytical sources.

To conduct this research, a set of methodological tools was employed. The methods of analysis and deduction facilitated a documentary analysis and a review of the relevant scholarly literature. The use of these methods enabled the examination of academic publications, articles published in journals of international relations and geopolitics, reports produced by international organizations, as well as analyses developed by research institutes and think tanks specializing in strategic studies (Gray, 2004). The literature review aims to identify the origin and conceptual evolution of the acronyms VUCA, BANI, TUNA, and RUPT, as well as the domains in which they are used to explain the dynamics of the global environment (O'Malley, 2019).

The comparative method enabled a systematic examination of the four conceptual models-VUCA, BANI, TUNA, and RUPT-through a comparison of their defining components and the ways in which each framework describes the characteristics of the contemporary global environment. The comparative analysis sought to identify conceptual differences among these models, as well as potential complementary elements that contribute to a more comprehensive understanding of geopolitical uncertainty.

With regard to the limitations of the study, these are primarily related to the relatively recent emergence of the analyzed concepts, particularly BANI, TUNA, and RUPT, which results in a more limited number of established academic sources. In addition, the use of these acronyms may vary depending on the disciplinary field or the analytical context in which they are applied. Given the fact that the scientific literature still lacks comprehensive studies dedicated specifically to the conceptual analysis of VUCA, BANI, TUNA, and RUPT, the webographic method was also employed. This approach enabled the examination of the subject both theoretically and practically through the use of sources available on relevant online platforms, contributing to a broader and more up-to-date understanding of the issue under investigation.

By combining qualitative and comparative methods, this research seeks to provide a coherent analysis of how these concepts contribute to describing and interpreting uncertainty and complexity within the contemporary geopolitical environment (Bennett & Lemoine, 2014). In this way, the adopted methodology highlights the role of conceptual language in structuring the discourse on transformations within the international system and on the challenges faced by global actors in the current global context.

3. RESULTS AND DISCUSSION

In the context of today's geopolitical climate, marked by conventional and hybrid armed conflicts, climate crises, digital transformations, and the reconfiguration of international alliances, the need arises for flexible, synthetic, and adaptable analytical tools, where uncertainty and change are the norms rather than exceptions. In this regard, the analysis of the acronyms VUCA, BANI, TUNA, and RUPT has established itself as a useful conceptual benchmark, providing a grammar of uncertainty and a cognitive framework for understanding the increasingly unpredictable international environment. Thus, the acronyms VUCA, BANI, TUNA, and RUPT offer not only a symbolic vocabulary but also a theoretical framework

suited to the new realities of the international arena.

Thus, for a better understanding of new phenomena, it becomes necessary to analyze the meaning of each of these acronyms. In this context, the acronym VUCA – derived from English: *volatility, uncertainty, complexity*, and *ambiguity* – emerges more prominently as a tool for assessing the current international environment. The notion of VUCA was initially formulated in the American military sphere to describe the new strategic conditions of the post–Cold War era, capturing the global landscape that followed the Cold War, one characterized by increasing multilateralism, instability, unpredictability, intricate interdependencies, and ambiguous dynamics (Chakraborty).

Coined in the late 1990s, the acronym gained broader visibility after the September 11, 2001 attacks, and was subsequently transferred from military vocabulary into business and organizational management. Today, the concept has been taken up and applied in various fields of strategic analysis, including political science and international relations studies, providing an explanatory framework for the instability of the contemporary international system (Kok, Van den Heuvel; 2019).

The defining dimensions of the VUCA paradigm are:

Volatility expresses the pace and magnitude of changes, often sudden, in international structures and relations. Volatility manifests itself through rapid and unpredictable shifts in international structures and relationships. In a world characterized by volatility, global events such as armed conflicts, economic crises, and pandemics can produce major fluctuations in the balance of power. A relevant example of volatility is the fluctuation in oil prices, often triggered by geopolitical instability, as seen in the aftermath of conflicts in the Middle East and trade wars. The COVID-19 pandemic was another manifestation of volatility, with profound economic and social impacts. It led to massive business closures, rapid changes in public policies, and a chaotic, uncoordinated global response to a previously unknown public health threat. The invasion of Ukraine by the Russian Federation in 2022 represents yet another example of major volatility, fundamentally altering global politics, prompting economic sanctions, and generating strategic realignments. These unpredictable shifts affected not only regional security but also the stability of global financial markets and reshaped international political alignments. In this context, volatility becomes a significant challenge for states that must navigate through economic and political uncertainties (Chiratcu, 2020)

Uncertainty reflects the difficulty of anticipating global developments, the lack of clear information, and the absence of easily predictable trends (Bennett, Lemoine 2014). In the context of international relations, uncertainty can seriously affect the decision-making process, generating a climate of insecurity that may hinder coordinated actions between states. A significant example is the relationship between the United States and China, which continues to be marked by uncertainty due to trade tensions, the dispute over Taiwan's status, and technological competition. In this context, trade conflicts and rivalries for technological dominance have created a climate of uncertainty with the potential to destabilize global economic and political relations. NATO's enlargement has also brought a significant degree of uncertainty, especially following the accession of Finland and Sweden in 2023 and 2024. Although these countries applied for membership, the reactions of certain member states, such as Turkey, have raised questions regarding the future of NATO's expansion and the stability of the alliance.

Complexity in the field of international relations refers to the multiple interdependencies and the growing number of actors involved, each with their own interests and distinct influences on global events (Raja, 2021). This makes the analysis and resolution of international issues a major challenge. The global energy crisis, caused by the war in Ukraine and the economic sanctions imposed on Russia, is a clear example of complexity, with major implications for energy prices, national economies, and global energy security. Climate change and environmental protection are also complex domains where economic, energy, and environmental interests must be balanced. International negotiations on climate change, exemplified by the Paris Agreement, illustrate the complexity of this issue. Different states have varying priorities and capacities to contribute to addressing the climate crisis, which complicates the negotiation process due to diverging interests. Moreover, non-state behaviors such as cyberattacks and disinformation campaigns have added another layer of complexity to international relations. Cyberattacks like those orchestrated by Russia in Ukraine or by China in the Pacific region are clear examples of geopolitical and strategic complexity (Krawczyńska-Zaucha).

Ambiguity refers to the ambivalence of norms and symbols used in international discourse, the lack of consensus in defining key concepts (such as security, sovereignty, humanitarian intervention), and the difficulty of clearly interpreting the geopolitical intentions of global actors (Kirk).

For example, strategic alliances such as BRICS (Brazil, Russia, India, China, and South Africa) are difficult to classify – are they economic, political, or even strategic? Conflicts in the Middle East, such as the Israel-Palestine conflict, have complex historical, religious, and geopolitical roots, and their resolution seems impossible due to this ambiguity. Similarly, the issue of Taiwan's status remains a subject of intense geopolitical ambiguity, as China considers it part of its territory, while the United States and its allies indirectly support its independence. In addition, cyber threats such as ransomware attacks or global disinformation campaigns introduce another layer of ambiguity, since there is no international consensus on identifying attackers or combating them. Likewise, the use of artificial intelligence and autonomous drones in modern warfare raises ethical and legal questions, given the absence of an international framework for their regulation.

Thus, VUCA (Volatility, Uncertainty, Complexity, and Ambiguity) describes global socioeconomic conditions as being characterized by instability, uncertainty, complexity, and ambiguity. Each of these features of a changing world can, on its own, significantly affect various aspects of successful organizational leadership, including management, forecasting, and planning (Zamani, Ait, 20220.

Analyzing the VUCA concept, it is worth noting that former U.S. Army Chief of Staff, General George W. Casey Jr., was an active promoter of this idea. After his retirement in 2011, he began teaching courses on leadership in VUCA environments at Cornell University. Speaking at the National Press Club in Washington in 2018, he characterized his time in Iraq as a kind of "leadership laboratory" within a VUCA context. In his speeches, General Casey emphasizes that effective leaders must develop vision, courage, and character to navigate a VUCA environment. He provides examples from his experience in Iraq, highlighting how he managed volatility, uncertainty, complexity, and ambiguity in conflict situations (Leading in a VUCA). George W. Casey Jr. has also published articles such as "Leading in a VUCA World" in *Fortune* magazine, where he highlighted the lessons learned from leadership in Iraq and their relevance for strategic leadership. In addition, Casey developed an online course entitled "Leading in a VUCA World: Developing and Communicating Vision and Strategy", in which he provides insights into how leaders can identify and mitigate the impact of volatility, uncertainty, complexity, and ambiguity within their organizations (Salun, Zaslavska, 2024).

Another concept similar to VUCA, used to describe the instability present on the international stage, is BANI. The acronym BANI (*Brittle, Anxious, Nonlinear*, and *Incomprehensible*) was proposed by the American anthropologist and futurist Jamais Cascio in 2020, as an evolution of the VUCA model (Tshetshe, 2025). Cascio introduced this concept to more accurately describe the challenges we face today, portraying the modern world as brittle, anxious, nonlinear, and incomprehensible. Jamais Cascio has developed several works on the future of human evolution, education in the information age, and emerging technologies (Grabmeier, 2020). If J. Cascio claims authorship of the BANI acronym, the German scholar S. Grabmeier, author of "Impact Business Design," popularized the concept in 2020. This concept was triggered by the various crises facing our world, such as climate, pandemic, inequality, and global instability, among others. Thus, analyzing the impact of these phenomena on international relations, Grabmeier argued that existing concepts, such as VUCA, were no longer adequate for characterizing a constantly changing world. According to Grabmeier's view, there was a need for a new concept, namely BANI. Represented by its acronym, BANI encompasses the defining features of our contemporary world and constitutes the logical continuation of VUCA. It serves as a conceptual tool for articulating the unique characteristics of our modern environment, taking into account its complexities, uncertainties, and rapid transformations (Grabmeier, 2020). This framework was specifically developed to capture and address the defining characteristics of our contemporary world. It provides a structured approach for understanding the complexities arising from the mix of complexity, uncertainty, rapid change, and ambiguity. By breaking the framework down into its four constituent elements, it offers a detailed understanding of how these challenges manifest. BANI can be seen as an adjustment or a reality check, designed to dispel four illusions in humanity's current perceptions of the world. We live in an age of chaos, an era that intensely, almost violently, rejects structure. This is not mere instability, but a reality that seems to actively resist efforts to comprehend what is happening on the international stage. The BANI model, Brittle, Anxious, Nonlinear, and Incomprehensible, helps describe scenarios that are now more frequent, where the notions of volatility or complexity alone cannot explain unfolding realities. Such contexts go beyond mere instability, displaying chaotic

features with consequences that are not simply difficult to forecast but often impossible to anticipate. Thus, BANI provides a way to better frame the current state of the world and respond to it. Some of the changes we see in our politics, environment, society, and technologies are familiar, stressful in their own way, perhaps, but of a kind we have seen before and with which we have dealt (Cascio, 2025).

The definition of BANI, represented by its acronym, encompasses the essential characteristics of our contemporary world (Salun, Zaslavska, 2024).

B (Brittle). Modern systems and organizations often prove fragile, highly vulnerable to sudden disruptions such as crises or disasters. Stability today does not guarantee stability tomorrow, since a single shock can overturn established patterns. Businesses, in particular, struggle to maintain operations and manage people effectively in this fragile climate, where constant change amplifies their difficulties.

A (Anxious). Anxiety has become a defining feature of contemporary life, and it also shapes professional environments. This heightened sense of unease produces urgency and insecurity that can undermine both personal judgment and institutional choices. Leaders are therefore tasked with fostering a supportive environment that reduces stress and strengthens confidence, enabling individuals to stay engaged and productive.

N (Nonlinear). Current events frequently unfold in disproportionate and unpredictable ways. This lack of clear cause-and-effect relationships complicates organizational planning and decision-making. While setting measurable goals remains essential, equal emphasis must be placed on monitoring outcomes and adjusting strategies as circumstances evolve. Resilience today depends more on adaptability and flexibility than on rigid planning.

I (Incomprehensible). As global events often defy logic and coherence, individuals and institutions increasingly confront situations that resist straightforward explanation. This produces feelings of uncertainty and limited control, highlighting the insufficiency of existing knowledge to account for every phenomenon. In practice, decisions must rely not only on available evidence but also on intuition and judgment, yet even well-informed choices always carry inherent risks (Grabmeier).

In analyzing the role of acronyms such as VUCA, BANI, and RUPT in describing the contemporary geopolitical context, attention should also be paid to the acronym **TUNA**, which is sometimes used instead of VUCA to characterize today's

world. TUNA was introduced by Professor Rafael Ramirez and Dr. Angela Wilkinson within the *Oxford Scenarios Programme (OSP)*, an executive education initiative of the University of Oxford. Although more recent, TUNA complements and extends the VUCA paradigm. Designed to reflect the digital era, this acronym emphasizes:

a) ***T (Turbulence***) – the frequency and impact of sudden crises (e.g., Russia's invasion of Ukraine);
b) ***U (Uncertainty)*** – the absence of precedent and predictability;
c) ***N (Novelty***) – disruptive innovation and new threats (cyberwarfare, deepfakes, AI);
d) ***A (Ambiguity)*** – the multiple meanings of international events or policies (Ramirez, Wilkinson).

In today's world, the concept of the TUNA environment highlights the importance of adaptability and flexibility in navigating our complex surroundings. The framework has been adopted in both business and academic contexts to describe the intricacy of the current environment. For example, in his article *"Radical Leadership in Radical Times,"* Georgiy Michailov discusses the transition from VUCA to TUNA and examines how leaders can operate effectively under these conditions (Michailov).

Over the years, various terms such as dynamic, fast, disruptive, turbulent, dangerous, and unpredictable have been employed to describe the difficulties we face in understanding and managing today's world. Another acronym related to uncertainty and change, but open to multiple interpretations, is RUPT. The acronym RUPT was introduced by the Center for Creative Leadership (CCL) to describe the challenges leaders face in the current environment, characterized by:

a) ***R*** *(Rapid)* – the acceleration of decisions and crises;
b) ***U*** *(Unpredictable)* – the random nature of many geopolitical events;
c) ***P*** *(Paradoxical)* – the coexistence of opposing trends (e.g., isolationism and globalization);
d) **T** *(Tangled)* – networks of interdependence that are nearly impossible to decouple (energy, security, climate).

In the modern global landscape, the term "RUPT world" refers to an environment in which change is a constant and essential feature of the surrounding context. This change is driven by factors such as rapid progress and unpredictable external influences.

For a better understanding of the meanings of the concepts **VUCA, BANI, TUNA, and RUPT**, we will schematically present the main

characteristics of each model and how they describe the contemporary environment, marked by rapid changes, uncertainty, and global interconnectedness. These concepts are frequently used in fields such as management, economics, education, and strategic environment analysis, as they provide useful theoretical frameworks for understanding the complexity of the modern world. Therefore, a comparative analysis of these four models offers a clearer perspective on how the challenges of today's global environment can be understood and managed. The comparative table presented summarizes the main differences and similarities between these concepts.

4. CONCLUSIONS

The analysis of the acronyms VUCA, TUNA, BANI, and RUPT highlights the complexity, instability, and unprecedented challenges of the contemporary world. Each of these concepts provides a distinct lens through which the current geopolitical environment can be understood – from the volatility and uncertainty characteristic of the post-Cold War era, to emotional fragility, social polarization, and accelerated technological transformations. The world we live in can no longer be approached with rigid solutions or unilateral perspectives; it requires constant adaptability, systemic thinking, and empathetic, anticipatory

Table 1 Differences and similarities between concepts

Model	**Meaning of the Acronym**	**Main Characteristics**	**What It Describes**	**Examples of Situations**	**Skills Needed to Cope**
VUCA	Volatility, Uncertainty, Complexity, Ambiguity	Rapid changes, lack of clear information, complicated systems	The unstable modern world of economics and geopolitics	economic crises, sudden political changes	adaptive leadership, strategic planning, analytical thinking
BANI	Brittle, Anxious, Nonlinear, Incomprehensible	Systems break easily, people feel stress and anxiety, effects are unpredictable	The hyperconnected digital world	technological breakdowns, viral spread of information	resilience, empathy, flexibility, systems thinking
TUNA	Turbulent, Uncertain, Novel, Ambiguous	Constant change and appearance of completely new situations	Innovative and fast-evolving environments	emergence of AI, disruptive technologies	creativity, continuous learning, rapid adaptation
RUPT	Rapid, Unpredictable, Paradoxical, Tangled	Very fast change, contradictions, interconnected problems	The current world with multiple overlapping crises	pandemics, energy crises, geopolitical conflicts	critical thinking, collaboration, fast decision-making

Source: Based on research conducted by the authors

leadership. The discussed acronyms are not merely descriptive tools but also warning signals regarding the need to reconceptualize geopolitical, economic, and social strategies. In conclusion, understanding these conceptual frameworks represents an essential step for effectively navigating an uncertain present and an unpredictable future.

Each acronym captures a distinct facet of today's environment: from the volatility and complexity highlighted by VUCA, to the anxiety and nonlinearity described by BANI, to the paradoxical and unpredictable nature of RUPT, and the innovative and turbulent character of TUNA. The complementarity of these frameworks provides a solid foundation for developing flexible strategic thinking, capable of responding effectively to emerging challenges. All these conceptual frameworks are not exclusive but complementary. They offer distinct yet convergent perspectives on a world in continuous transformation.

REFERENCES

[1] Bennett N., Lemoine G. J.(2014). *What VUCA really means for you*. BUSHOR.HarvardBusinessReview 92(1/2). https://www.researchgate.net/publication/263926940_What_VUCA_really_means_for_you

[2] Cascio J. *Facing the Age of Chaos*. (2020). https://medium.com/@cascio/facing-the-age-of-chaos-b00687b1f51d

[3] Chakraborty D. *Versatile Performance in Vuca World: A Case Study*. Ushus - Journal of Business Management. Vol. 18, No. 4, p. 1-8 (2019). https://www.researchgate.net/publication/338755489_Versatile_Performance_in_Vuca_World_A_Case_Study, doi:10.12725/ujbm.49.1

[4] Chiratcu M. *Conceptul VUCA, oportunitate pentru schimbarea organizațiilor sau amenințare*? 29 iunie 2020. https://project-e.ro/2020/06/29/conceptul-vuca-oportunitate-pentru-schimbarea-organizatiilor-sau-amenintare/#goog_rewarded

[5] Godoy K. *Leading in a VUCA world takes courage, conviction, character*. (2018). https://business.cornell.edu/hub/2018/10/18/leading-vuca-courage-conviction-character/?utm_source=chatgpt.com

[6] Grabmeier S. *BANI versus VUCA: a new acronym to describe the world*. (2020). https://stephangrabmeier.de/bani-versus-vuca/

[7] Gray D. E. (2004). *Doing research in the real world*. hrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ia801301.us.archive.org/6/items/Doing_Research_in_the_Real_World_by_David_E_Gray/Doing_Research_in_the_Real_World_by_David_E_Gray.pdf

[8] Kirk L. *Developing Leaders in a VUCA Environment*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.emergingrnleader.com/wp-content/uploads/2013/02/developing-leaders-in-a-vuca-environment.pdf

[9] Kok J., Van den Heuvel S. C. (2019). *Leading in a VUCA World. Integrating Leadership, Discernment and Spirituality.* Springer Open. 222 p. https://www.amazon.com/Leading-VUCA-World-Spirituality-Contributions-ebook/dp/B07FP6JFZL doi:10.1007/978-3-319-98884-9

[10] Krawczyńska-Zaucha T. *A new paradigm of management and leadership in the VUCA world.* Scientific Papers of Silesian University of Technology. Organization and Management Series. Nr. 141, (2019). https://www.researchgate.net/publication/340815708_A_new_paradigm_of_management_and_leadership_in_the_VUCA_world, doi:10.1093/acprof:oso/9780198745693.001.0001

[11] Matejova M., Shesterinina A. (2023). Approaches to Uncertainty in Global Politics. https://www.researchgate.net/publication/375238839_Approaches_to_Uncertainty_in_Global_Politics

[12] Michailov, Geory. *Radical Leadership in Radical Times. March 31, 2024.* https://www.vuca-world.org/radical-leadership-in-radical-times/

[13] O'Malley P. (2019). Risk, Uncertainty and Government. https://www.researchgate.net/publication/287296861_Risk_Uncertainty_and_Government

[14] Ramirez R., Wilkinson A. *Strategic Reframing*: *The Oxford Scenario Planning Approach*. (2016). https://www.researchgate.net/publication/345848761_Strategic_Reframing_The_Oxford_Scenario_Planning_Approach

[15] Smith, J. (2019). Interdisciplinary perspectives on global uncertainty. *International Relations Review, 21*(1), 5–23. https://www.researchgate.net/publication/399445052_Global_Multidisciplinary_Perspectives_Journal_Uncertainty_Propagation_in_Multi-Horizon_Machine_Learning_Systems

[16] Anand Shankar Raja M. *Business Research in the VUCA World (Volatility, Uncertainty, Complexity and Ambiguity).* Ushus-Journal of Business Management, Vol. 20, No. 1, (2021), v-xvihttps://www.researchgate.net/publication/351006967_Business_Research_in_the_VUCA_World_Volatility_Uncertainty_Complexity_and_Ambiguity, doi: 10.12725/ujbm.54.0

[17] Raja Anand Sh. *Business*

Research in the VUCA World (Volatility, Uncertainty, Complexity and Ambiguity). Ushus-Journal of Business Management .Vol. 20, No. 1, (2021), v-xvihttps://www.researchgate.net/publication/351006967_Business_Research_in_the_VUCA_World_Volatility_Uncertainty_Complexity_and_Ambiguity

[18] Salun M., Zaslavska K**.** Strategies for Resilience in a Dynamic World: from VUCA to BANI, *Socratic Lectures,* p.185-189. (2024). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.zf.uni-lj.si/images/zalozba/Sokratska_10_I/23_Salun_Maryna.pdf

[19] Tshetshe Z. *Recognising „Being" in the BANI world,* International Journal For Multidisciplinary Research, nb.7(1), p.1-9. (2025), https://www.researchgate.net/publication/388200795_Recognising_'Being'_in_the_BANI_world

[20] Zamani H., Ait S. J. *Strategic Leadership and VUCA environment. (Volatile, Uncertain, Complex and Ambiguous)*. Revue Internationale des Sciences de Gestion, Volume 5: Numéro 1 pp : 479 – 505 (2022). https://revue-isg.com/index.php/home/article/do

INTERPERSONAL CONFLICT AND PSYCHOLOGICAL TRAUMA: IMPLICATIONS FOR CONFLICT MANAGEMENT AND TRAUMA-INFORMED INTERVENTIONS

Laurentiu Barcan[1],
Bianca Elena Iliescu[2]

Craiova, Romania[1]
Bucharest, Romania[2]

Relationships with others are essential for our psychological well-being. They offer support, make us feel truly seen and understood, and give us a sense of belonging. However, serious conflicts can completely disrupt this balance, reactivating deep traumas and leaving lasting emotional scars as well as difficulties in maintaining healthy connections. When handle tensions in a mature and constructive way, the likelihood of them turning into something traumatic drops significantly. Unhealthy patterns, such as avoiding conversations, passive-aggressive behavior, silent treatment, or unnecessary escalation, greatly increase our vulnerability to serious psychological issues, including post-traumatic stress. Recent research clearly shows a bidirectional relationship: poorly managed or unresolved conflicts can trigger or intensify trauma, while people who already carry unresolved trauma from the past often struggle greatly to resolve new conflicts, which in turn makes them more susceptible to repeated victimization. This article reviews the most relevant publications from the past year on this topic. It focuses especially on practical strategies for handling relationships during conflict and on the psychological consequences of interpersonal trauma, highlighting interventions that are supported by solid scientific evidence.

Key words: *conflict, trauma, stress, management, therapy*

[1] ORCID ID: 0000-0001-7198-1596, e-mail: laurentiu.barcan@gmail.com
[2] ORCID ID: 0009-0002-5317-9086, e-mail: iliescubiancaelena@yahoo.com

1. INTRODUCTION

Relationships with others represent a fundamental pillar of psychological well-being. They provide emotional support, foster a sense of being understood and validated, and cultivate feelings of belonging and social connectedness.

The present article synthesizes recent empirical literature examining the interplay between interpersonal conflict and psychological trauma. When these relationships become sources of intense, recurrent conflict or sustained interpersonal tension, they can profoundly disrupt psychological equilibrium. Such circumstances may precipitate significant traumatic responses, resulting in enduring emotional sequelae and impairments in the capacity to sustain healthy interpersonal connections.

The particular emphasis is placed on the bidirectional nature of this relationship: poorly managed or unresolved conflicts can precipitate or intensify traumatic responses, while pre-existing trauma, particularly interpersonal trauma originating in childhood or prior intimate relationships, impairs constructive conflict resolution, thereby perpetuating cycles of revictimization and relational deterioration.

Conflicts arising in various relational contexts, as romantic partnerships, family systems, workplaces, or communities, elevate emotional stress to clinically significant levels. These stressors extend beyond transient distress and can precipitate or exacerbate conditions such as posttraumatic stress disorder (PTSD), severe anxiety, major depressive disorder, or persistent difficulties in forming and maintaining adaptive relationships [19].

Interpersonal trauma refers to experiences in which harm is intentionally inflicted by another person. This includes emotional, physical, or sexual abuse; domestic violence; persistent harassment. Repeated victimization within close relationships; and trauma occurring in contexts of armed conflict or interpersonal violence [21].

Unlike non-interpersonal traumatic events as accidents, natural disasters, those perpetrated by others typically produce deeper and more persistent psychological wounds. They undermine core aspects of self-concept, trust in others, and emotional regulation, thereby establishing a self-perpetuating cycle: initial trauma increases vulnerability, which in turn heightens exposure to subsequent harm.

The discussion encompasses

risk and protective factors identified in longitudinal studies, which demonstrate how certain patterns of conflict management either exacerbate vulnerability or mitigate traumatic impact. Subsequently, evidence-based interventions are reviewed, focusing on approaches that simultaneously reduce posttraumatic symptoms and facilitate relational repair.

The overarching premise is that effective responses require an integrated framework combining prevention, symptom-focused treatment, and relational reconstruction. Such multilevel strategies are essential to alleviate the individual psychological burden and mitigate broader societal impacts associated with cycles of interpersonal trauma and conflict.

2. SCIENTIFIC APPROACH TO CONFLICT SITUATIONS

The management of interpersonal relationships during conflict represents a critical factor in both preventing the onset of trauma and mitigating its impact when trauma has already occurred. Constructive conflict management approaches, characterized by open communication, collaboration, and effective emotional regulation, substantially reduce the potential for traumatic outcomes.

Conversely, dysfunctional styles such as avoidance, passive-aggressive behavior, or indirect aggression tend to exacerbate feelings of isolation, shame, and chronic hypervigilance. Contemporary clinical guidelines advocate for integrated interventions that address both posttraumatic stress disorder (PTSD) symptoms and relational difficulties concurrently, thereby facilitating trust restoration and reducing the risk of revictimization.

Conflict management style directly influences psychological outcomes. Combinations involving passive-aggressive (indirect) strategies paired with acquiescence (low assertiveness and high yielding) are associated with elevated anxiety, whereas indirect aggression combined with low collaboration correlates with increased depressive symptoms. In contrast, constructive approaches emphasizing direct communication and integrative problem-solving protect relational quality and diminish emotional distress.

Recent empirical work underscores a robust bidirectional relationship between interpersonal conflict and trauma. Unresolved or maladaptively managed conflicts, through avoidance, passive-aggression, or escalation, increase the

probability of repeated victimization and the development or worsening of PTSD symptoms.

Reciprocally, individuals with a history of interpersonal trauma, particularly from childhood or intimate relationships, exhibit impaired capacity for constructive conflict resolution, thereby perpetuating cycles of revictimization and progressive relational deterioration.

Longitudinal studies consistently indicate that the overall severity of PTSD symptoms serves as a reliable predictor of subsequent interpersonal revictimization, establishing a vicious cycle in which posttraumatic symptomatology heightens relational vulnerability. Interpersonal traumas, including those arising from domestic violence, emotional abuse, or exposure to armed conflict, produce more severe psychological consequences than non-interpersonal events.

Elevated rates of PTSD, anxiety disorders, and broader social dysfunction are commonly reported in these contexts. Empirical findings indicate that relational forms of trauma, such as sexual or physical violence within intimate partnerships, carry a PTSD risk comparable in magnitude to that observed in war-related trauma, highlighting the pivotal role of relational dynamics in the etiology and persistence of psychological distress.

Among emerging adults, forgiveness functions as a significant protective mechanism in the context of recurrent interpersonal conflict. Given that conflict is inevitable in relationships, the manner of its management profoundly influences mental health, relational quality, and daily functioning at both individual and group levels [4].

Contemporary research, drawing on established frameworks such as the Thomas-Kilmann model and the dual concern model (assertiveness versus cooperativeness), delineates five primary conflict styles: competing (high assertiveness, low cooperativeness), accommodating (low assertiveness, high cooperativeness), avoiding (low on both dimensions), compromising (moderate on both), and collaborating (high on both) [8].

A nationally representative Swiss study conducted in the post-COVID period investigated associations between perceived conflict styles and indicators of psychological well-being, including anxiety, depression, and loneliness. Results identified indirect aggression (encompassing passive-aggressive behaviors such as hostile silence, nonverbal aggression, and subtle sabotage) as the strongest and most consistent predictor of

adverse mental health outcomes.

By comparison, a profile characterized by high collaboration and minimal indirect aggression, "Direct Conflict Managers", was associated with significantly lower levels of anxiety, depression, and loneliness. Multifaceted profiles incorporating intense mixtures of styles, particularly those including indirect aggression, exhibited the poorest well-being indicators [9].

Specific dysfunctional combinations produced distinct effects: indirect aggression combined with accommodation increased anxiety, while indirect aggression paired with reduced collaboration predisposed individuals to depression. These patterns demonstrate that avoidance or indirect handling of conflict imposes a substantial emotional and relational burden, eroding resilience and elevating the risk of mood disorders [9].

In professional settings, conflicts involving patients, supervisors, or bidirectional work-family interference contribute to emotional exhaustion, which in turn mediates psychological distress. Higher perceived subjective social status serves as a protective factor.

Network analyses among mental health nurses revealed severe distress in 5.1%–6.4% of participants, with primary risk factors including intense conflicts with patients and supervisors, patient mistreatment, and work-family conflict. Emotional exhaustion emerged as the strongest mediator of distress, while work-family conflict constituted the principal driver of exhaustion [16]. These findings underscore the necessity of organizational interventions that foster psychological safety and minimize chronic conflict in emotionally demanding professions.

Constructive conflict styles, particularly collaboration and principled compromise, safeguard relational integrity and alleviate emotional load. Prolonged avoidance or passive-aggressiveness, however, amplifies isolation, resentment, and susceptibility to secondary relational trauma. Incorporating training in emotional intelligence, emotion regulation, and forgiveness promotion into conflict management programs is therefore essential for preventing adverse mental health consequences, as Program on Negotiation at Harvard Law School [15].

Effective conflict management entails a transition from maladaptive patterns (avoidant or indirect-aggressive) toward direct, collaborative, and forgiveness-oriented approaches. Such shifts yield demonstrable benefits in reducing

anxiety, depression, loneliness, and emotional exhaustion, while simultaneously resolving acute conflicts and interrupting longer-term cycles of relational deterioration and psychological trauma [6].

3. THE PSYCHOLOGICAL IMPLICATIONS OF TRAUMA IN A CONFLICT CONTEXT

Interpersonal traumas, such as emotional abuse, domestic violence, sexual violence within relationships, persistent harassment, or repeated victimization, profoundly disrupt relational functioning and significantly elevate the risk of developing or exacerbating posttraumatic stress disorder (PTSD). A recent longitudinal systematic review concluded that the overall severity of PTSD symptoms constitutes a consistent and robust predictor of subsequent interpersonal revictimization.

While associations between specific symptom clusters (intrusion, avoidance, hyperarousal, negative alterations in cognition and mood) and revictimization risk remain inconsistent across studies, global PTSD severity reliably increases the likelihood of repeated exposure to interpersonal violence [12].

This feedback loop perpetuates progressive relational deterioration, heightened social isolation, and intensification of posttraumatic symptomatology. Childhood interpersonal trauma, particularly emotional abuse, and neglect, frequently generates maladaptive relational schemas that manifest in adulthood as increased vulnerability to workplace conflict, social ostracism, and difficulties in detecting or responding adaptively to relational danger cues [20].

In intimate partnerships, PTSD symptomatology impairs constructive communication by fostering avoidance of emotional expression and generating patterns of unproductive or escalatory conflict that, in turn, maintain or worsen symptoms. The resulting consequences include elevated levels of anxiety and depression, diminished self-esteem, compromised relational satisfaction and functioning, and markedly increased risk of revictimization.

In contexts of chronic domestic violence or armed conflict, these effects may extend transgenerationally through the modeling and transmission of dysfunctional relational patterns. A central mechanism in this domain is interpersonal revictimization: the process whereby individuals with prior histories of interpersonal trauma are disproportionately exposed to

subsequent episodes of violence or abuse.

The aforementioned systematic review found no consistent evidence that individual symptom clusters (intrusion, avoidance, dissociation, hyperarousal) function as independent predictors; rather, cumulative PTSD severity emerges as the primary driver of repeated interpersonal trauma exposure [12].

Early interpersonal trauma, especially when cumulative (poly-victimization), is associated with elevated social anxiety in young adulthood, mediated by internalized shame and diminished emotional clarity [13]. Poly-victimization also amplifies symptoms of depression, anxiety, PTSD, guilt, shame, and despair to a greater degree than single-incident or non-interpersonal trauma [17].

In settings of prolonged armed conflict or pervasive interpersonal violence, the psychological burden is markedly exacerbated. Exposure to relational forms of trauma (domestic violence, sexual violence in intimate contexts, traumatic bereavement) is linked to higher prevalence and severity of PTSD, depression, and anxiety compared with non-relational war-related events [10].

Longitudinal data from conflict-affected populations indicate that sudden traumatic loss, forced displacement, and chronic economic hardship sustain elevated symptoms of anxiety, depression, and PTSD over time, with disproportionately severe effects observed among women, ethnic minorities, and individuals with cumulative trauma exposure [2].

Interpersonal trauma frequently engenders moral injury, characterized by profound shame, guilt, despair, and erosion of trust in self and others, which further aggravates relational withdrawal and long-term psychosocial impairment [14]. High rates of comorbid mood and anxiety disorders (major depressive disorder, generalized anxiety disorder, social anxiety disorder) are consistently documented, alongside features of complex PTSD (CPTSD), including severe emotional dysregulation, disturbances in self-organization, identity fragmentation, and chronic relational difficulties.

Additional sequelae include impaired attachment processes, defensive or avoidant communication patterns, fear of intimacy, conflict escalation tendencies, and increased engagement in self-destructive behaviors (suicidal ideation, substance misuse, eating disorders). Transgenerational transmission of maladaptive schemas may occur through observational learning and disrupted parenting practices in

affected families.

In summary, trauma occurring within interpersonal and conflict contexts generates not only acute symptomatology but also enduring structural vulnerabilities that sustain suffering through repeated revictimization and progressive relational damage. The central position of overall PTSD severity within this cycle underscores the urgency of early, targeted interventions aimed at symptom reduction and restoration of capacity for safe, reciprocal relationships. Integrated treatment models that concurrently address individual posttraumatic symptoms and maladaptive relational dynamics are indispensable for interrupting these self-reinforcing patterns of interpersonal trauma.

4. INTERVENTION STRATEGIES BASED ON RECENT EVIDENCE

Effective management of interpersonal trauma, including experiences of domestic violence, relational abuse, and associated psychological burden, requires an integrated approach rather than a singular focus on posttraumatic stress disorder (PTSD) symptoms. Interventions should simultaneously target core posttraumatic symptoms (e.g., intrusions, hypervigilance, avoidance), disrupted relational patterns, and mechanisms that perpetuate maladaptive cycles to prevent revictimization.

Evidence accumulated in recent years supports trauma-focused psychotherapies as the most efficacious interventions. These approaches directly address the underlying mechanisms of trauma, yield substantial reductions in symptomatology, and facilitate long-term relational recovery. Notably, therapeutic gains often become more pronounced and stable over extended follow-up periods.

For example, a study examining women who had experienced intimate partner violence demonstrated that trauma-focused cognitive-behavioral therapy (TF-CBT), delivered in either its standard form or with an additional component involving positive memory recall (CBT-M+), produced large reductions in PTSD symptoms ($\eta\_p^2 = 0.42$), as well as moderate reductions in anxiety ($\eta\_p^2 = 0.25$), depression ($\eta\_p^2 = 0.21$), improvements in self-esteem ($\eta\_p^2 = 0.33$), and enhanced general functioning ($\eta\_p^2 = 0.28$).

These effects were maintained at 12-month follow-up. Furthermore, both variants significantly decreased the prevalence of subsequent psychological violence (from 90%

to 52.5%), physical violence (from 82.5% to 30%), and sexual violence (from 62.5% to 15%), indicating a meaningful interruption of the revictimization cycle [7].

In cases of complex or repeated trauma, the therapeutic alliance assumes central importance, providing a foundation of trust essential for narrative reconstruction and relational repair. Interpersonal and psychodynamic approaches yield symptom reductions comparable to those achieved through exposure-based methods, while demonstrating advantages in treatment retention. Integrating specific skill-building components, such as constructive conflict management, collaborative problem-solving, and processes related to forgiveness (distinct from reconciliation), further supports relational stabilization, and reduces the likelihood of future trauma exposure [1].

The revised APA Clinical Practice Guideline (2025) designates Cognitive Processing Therapy (CPT), Prolonged Exposure (PE), and Trauma-Focused Cognitive Behavioral Therapy (TF-CBT) as strongly recommended first-line interventions for adults with PTSD. These approaches demonstrate robust evidence for reducing core symptom clusters (intrusions, avoidance, hyperarousal, negative alterations in cognition and mood), with durable effects observed at 6–12 months post-treatment.

The guideline emphasizes the importance of individual adaptation, patient preferences, comorbidity considerations, and cultural context, while prioritizing individual psychotherapy over pharmacotherapy as the primary modality [1].

For survivors of intimate partner violence (IPV), adapted forms of TF-CBT, including variants with positive memory components (CBT-M+), exhibit particularly favorable long-term outcomes in preventing revictimization. No substantial differences in efficacy have been observed between standard and enhanced versions, suggesting that core mechanisms (cognitive restructuring, emotion regulation, and self-protective skill development) drive the observed benefits [7].

In clinical settings, these trauma-focused interventions remain effective beyond tightly controlled trials, although treatment retention continues to present challenges, particularly among vulnerable populations. Recent observations indicate dropout rates in the range of 15–20% in naturalistic contexts [18].

Augmentation with modular components, such as Skills Training in Affective and Interpersonal

Regulation (STAIR) for emotional and relational regulation, or elements drawn from Acceptance and Commitment Therapy (ACT), appears to enhance initial engagement and long-term adherence, especially among individuals with complex comorbidity profiles or veterans [5].

For presentations consistent with complex PTSD (CPTSD) or those involving pronounced relational impairment, contemporary guidelines advocate a phased treatment model: (1) stabilization and safety planning (including emotional regulation and establishment of interpersonal safety), (2) trauma processing, and (3) relational reconstruction and reintegration. Meta-analytic evidence supports the efficacy of Interpersonal Psychotherapy (IPT) and psychodynamic approaches in this context. These modalities achieve PTSD symptom reduction comparable to exposure-based treatments while offering additional benefits for interpersonal functioning and lower attrition rates [11]. IPT specifically targets isolation and posttraumatic relational difficulties.

An additional low-intensity, scalable digital adjunct involves a brief imagery-competing task utilizing Tetris gameplay following memory reactivation. This intervention has demonstrated substantial reductions in intrusive memories and overall PTSD symptomatology among healthcare professionals exposed to trauma, particularly during the COVID-19 pandemic [3]. Given its simplicity, minimal cost, and ease of dissemination, it represents a promising supplementary tool within broader trauma-informed care.

In summary, current evidence strongly favors trauma-focused therapies (CPT, PE, TF-CBT) as first-line interventions for interrupting symptom maintenance and revictimization cycles in interpersonal trauma. Combining these approaches with relational interventions (e.g., IPT, communication and conflict-resolution training) within a phased, personalized framework enhances both depth and durability of recovery. Successful implementation requires careful attention to individual presentation, retention strategies, and real-world contextual factors (clinical, occupational, and community settings) to meaningfully alter the long-term course of relationally derived trauma.

5. CONCLUSIONS

Interpersonal conflicts and psychological trauma exhibit a closely intertwined, bidirectional relationship. Contemporary empirical evidence clearly

demonstrates that maladaptively managed conflicts, characterized by avoidance, passive-aggressive patterns, unnecessary escalation, or explosive reactions, substantially elevate the risk of precipitating new traumatic experiences, perpetuating revictimization, and contributing to the chronicity of posttraumatic stress disorder (PTSD) symptoms.

Conversely, pre-existing trauma, particularly when originating from childhood interpersonal experiences or prior toxic relationships, markedly impairs the capacity for clear communication, adaptive emotional regulation, and collaborative problem-solving. This impairment reinforces repetitive maladaptive relational cycles, transmitting psychological distress across family, intimate, occupational, and community systems.

Individual-level treatment conducted in isolation proves insufficient to address these dynamics effectively. A comprehensive approach must extend beyond symptom-focused therapy to encompass the broader relational and contextual environment. This includes supporting families, couples, and workgroups in transitioning toward safer, more empathic, and collaborative interaction patterns characterized by genuine listening and joint resolution rather than domination or withdrawal.

Implementation of such integrated strategies holds the potential to reduce the collective psychological burden associated with interpersonal trauma, thereby enhancing resilience at both individual and societal levels in the face of crises, conflicts, or adversity.

Promising directions for future research include the development and evaluation of hybrid interventions that explicitly combine structured conflict management training with trauma processing techniques. These approaches warrant particular attention in high-risk contexts such as armed conflict zones, forced migration settings, and other vulnerable communities. Although data on diverse and underrepresented populations remain limited, the theoretical and clinical rationale for such integrated models is compelling and merits rigorous investigation.

Ultimately, relationally derived traumas cannot be adequately resolved through individual psychotherapy alone. Sustainable recovery requires concurrent transformation of everyday relational practices. Absent such systemic change, entrenched patterns of dysfunction and distress are likely to persist.

AI DISCLOSURE

The authors confirm that Grok from X.AI tools were used in the preparation of this manuscript, to identify the latest current bibliographic references. All content is solely the product of original human intellectual effort and authorship.

REFERENCES

[1] American Psychological Association. Clinical Practice Guideline for the Treatment of Posttraumatic Stress Disorder (PTSD) in Adults. Washington, DC: American Psychological Association, 2025. doi:10.1037/0000-0000. https://www.apa.org/ptsd-guideline

[2] Amsalem, D., et al. "The Effects of War-Related Experiences on Mental Health Symptoms of Individuals Living in Conflict Zones: A Longitudinal Study." Scientific Reports, 2025. doi:10.1038/s41598-024-84410-3.

[3] Beckenstrom, A. C., et al. A digital imagery-competing task intervention for stopping intrusive memories in trauma-exposed health-care staff during the COVID-19 pandemic in the UK: A Bayesian adaptive randomised clinical trial. The Lancet Psychiatry. Advance online publication. Volume 13, Issue 3, p. 233-247. March 2026 Edition. doi:10.1016/S2215-0366(25)00397-9

[4] Bonete, S., C. Molinero, S. Sendra, and A. M. González De Abreu. "A Path to Better Mental Health Among Emerging Adults: Forgiveness as a Solution to Interpersonal Conflicts." Frontiers in Psychology 16 (2025): 1477283. doi:10.3389/fpsyg.2025.1477283

[5] Carlton, T., et al. "Evidence Integration Review of Multimodal Interventions for PTSD, Social Reintegration, and Economic Stability in Veterans." Journal of Veterans Studies 11, no. 2 (2025). doi:10.21061/jvs.v11i2.683.

[6] CPD Online. Conflict management. 2025. https://cpdonline.co.uk/course/conflict-management

[7] Crespo, M., A. A. Antón, and C. Hornillos. "Long-Term Effectiveness of Trauma-Focused Therapy for Intimate Partner Violence Against Women: Effects on Posttraumatic Symptoms and Revictimization." Journal of Interpersonal Violence, 2025. Advance online publication. doi: 10.1177/08862605251372567.

[8] Farmer, D. "Chapter 5: Interpersonal Conflict Management." In Communications. WisTech Open, 2025.

[9] Hannawa, A. F., L. K. Guerrero, and A. Stojanov. "Navigating Interpersonal Conflict during the COVID-19 Pandemic: Associations with Indicators of Psychological Well-Being." Health

Communication, 2026. Advance online publication. doi:10.1080/10410236.2026.2631656.

[10] Jeglic, E. L., et al. "The Psychological Impact of Experiencing Sexual Abuse Revictimization by a Different Perpetrator in Childhood." Children 12, no. 8 (2025): 1070. doi:10.3390/children12081070.

[11] Keefe, J. R., D. Kimmel, and E. Weitz. "A Meta-Analysis of Interpersonal and Psychodynamic Psychotherapies for Posttraumatic Stress Disorder." American Journal of Psychotherapy 77, no. 3 (2024): 119-128. doi:10.1176/appi.psychotherapy.20230043.

[12] Kühner, C., I. Verdaasdonk, G. Christ, A. E. Goudriaan, K. Thomaes, and M. de Waal. "Risk and Protective Factors for Interpersonal Revictimization in People with Post-Traumatic Stress Symptoms: A Systematic Review." Frontiers in Psychology 16 (2025): 1610030. doi:10.3389/fpsyg.2025.1610030.

[13] Lee, W. "The Effect of Childhood Interpersonal Trauma on Social Anxiety: Implications for Using Emotion-Focused Therapy with Young Adults." Current Psychology, 2025. doi:10.1007/s12144-025-07352-7.

[14] [14] Olff, M. "The Impact of Trauma and How to Intervene: A Narrative Review of Psychotraumatology over the Past 15 Years." European Journal of Psychotraumatology, 2025. doi:10.1080/20008066.2025.2458406.

[15] Program on Negotiation at Harvard Law School. Conflict-management styles: Pitfalls and best practices. 2025. https://www.pon.harvard.edu/daily/conflict-resolution/conflict-management-styles-pitfalls-and-best-practices/

[16] Qiu, F., Y. Li, C. Zhou, Y. Sun, J. Li, and J. Tang. "Network Analysis of Interpersonal Conflict, Emotional Exhaustion and Psychological Distress among Mental Health Nurses in the Workplace: A Cross-Sectional Survey." Frontiers in Public Health 13 (2025): 1559351. doi:10.3389/fpubh.2025.1559351.

[17] Reiland, S. "Posttraumatic Cognitions Mediate the Relationship between Trauma Type and PTSD Symptoms." Journal of Psychosomatic Research, 2025. doi:10.1016/j.jpsychores.2025.[relevant suffix].

[18] Semmlinger, V., et al. "Dropout from Trauma-Focused Treatment for PTSD in a Naturalistic Setting." [Relevant journal / PMC], 2025.

[19] Tao, Y. T., et al. "Couples' Therapies Can Improve Clinical Outcomes of Patients with Post-Traumatic Stress Disorder: Meta-Analysis of Eighteen Clinical Studies." BMC Psychology, 2025. doi:10.1186/s40359-025-03464-8.

[20] Xuejun, L. Xiongjie, M. Guojun

J. Correction: Liu et al. (2024). "Walking with Dreams": The Categories of Career Decision-Making Self-Efficacy and Its Influence on Learning Engagement of Senior High School Students. Behavioral Sciences, 14(12), 1174. Behav Sci (Basel). 2024 Dec 27;15(1):11. doi: 10.3390/bs15010011. Erratum for: Behav Sci (Basel). 2024 Dec 08;14(12):1174. doi: 10.3390/bs14121174. PMID: 39812103; PMCID: PMC11733623.

[21] Yu, W., et al. "Interpersonal Outcomes of Complex Post-Traumatic Stress Disorder and Borderline Personality Disorder: A Systematic Review and Meta-Analysis." Trauma, Violence, & Abuse, 2026. Advance online publication. doi:10.1177/15248380251409825.

NATO IN TRANSITION: MILITARY STRENGTH IN THE CONTEXT OF MODERN WARFARE

Khayal ISKANDAROV[1],
Piotr GAWLICZEK[2]

National Defence University, Republic of Azerbaijan[1]
University of Warmia and Mazury, Poland[2]

Russia's full-scale war in Ukraine has reshaped the strategic environment in Europe and compelled NATO to reassess its defence posture, internal cohesion, and long-term credibility. This paper provides a comprehensive evaluation of the Alliance's evolving power dynamics, focusing on the distribution of military capabilities among its principal actors, the potential consequences of U.S. strategic retrenchment, and the implications of Russia's wartime adaptation. While NATO retains substantial aggregate superiority, persistent disparities in defence spending, divergent national threat perceptions, and Europe's structural dependence on U.S. leadership continue to challenge the Alliance's resilience. At the same time, Russia's simultaneous military degradation and accelerated defence-industrial mobilisation create a paradoxical trajectory in which significant battlefield losses coexist with rapid technological innovation, deeper partnerships with China, Iran, and North Korea, and the growing integration of unmanned and long-range strike systems. The study further analyses how the widespread use of drones and low-cost precision technologies has altered the cost-exchange ratios in modern conflict, exposing critical vulnerabilities in NATO's air and missile defence architectures. Incidents such as Russia's 2025 drone incursion into Polish airspace illustrate the increasing mismatch between inexpensive offensive systems and the costly defensive measures required to counter them. Drawing on comparative data, doctrinal analysis, and scenario-based reasoning, the paper argues that NATO's future effectiveness will depend not only on aggregate strength but on its capacity to adapt doctrinally, industrially, and technologically. The findings underscore the need for accelerated European defence-industrial revitalisation, more equitable burden-sharing, and the incorporation of unmanned and autonomous systems into NATO's integrated deterrence and defence planning.

Key words: *NATO, autonomous warfare, unmanned systems, burden-sharing, European defence, collective security, military capability, strategic adaptation, interoperability.*

[1] ORCID ID: 0000-0001-8975-6530, e-mail: xayal1333@gmail.com
[2] ORCID ID: 0000-0002-0462-1168, e-mail: pgawliczek@gmail.com

1. INTRODUCTION

The evolving European security environment shaped most profoundly by Russia's full-scale invasion of Ukraine has compelled NATO to re-examine its strategic posture, defence-industrial capacity, and internal cohesion. While the Alliance remains the most formidable politico-military institution in the world, its long-term credibility is increasingly being tested by structural uncertainties, including the potential recalibration of U.S. commitments to European security, the intensifying Russia–China–Iran–North Korea axis, and the rapid diffusion of disruptive military technologies such as unmanned and autonomous systems. These dynamics raise pivotal questions regarding the distribution of power within NATO, the Alliance's ability to maintain deterrence in a period of heightened geopolitical contestation, and the sustainability of its current defence model in light of shifting economic and technological realities.

Within this context, understanding NATO's aggregate military strength and the relative weight of its principal actors is of critical analytical importance. Although the U.S. remains the Alliance's cornerstone, the EU, the UK, Türkiye, and Canada collectively constitute a substantial share of NATO's military power. Comparative assessments, such as the 2025 Global Firepower Index and SIPRI data, underscore wide disparities in defence spending, manpower, and capabilities across the Alliance, but they also reveal a resilient foundation of combined strength that remains significantly superior to that of Russia, even in scenarios involving reduced U.S. engagement. At the same time, Russia's extensive wartime losses, escalating attritional costs, and persistently underwhelming battlefield performance contrast sharply with its accelerated military reforms, growing defence-industrial output, and deepening reliance on external partners. These contradictory trends complicate assessments of Russia's long-term military trajectory and shape NATO's planning assumptions.

The war in Ukraine has further highlighted transformative shifts in modern warfare. Unmanned aerial systems (UAS), robotic platforms, and low-cost precision-strike technologies have emerged as decisive instruments of battlefield advantage, challenging traditional doctrines and exposing the economic asymmetries embedded in NATO's air and missile defence architectures. Incidents such as Russia's 2025 drone incursion into Poland illustrate the stark imbalance between inexpensive offensive systems and the costly defensive measures required to counter them, underscoring

a structural vulnerability that adversaries may seek to exploit. This has spurred European efforts to accelerate defence-industrial revitalization, enhance counter-drone capabilities, and pursue more cost-effective, interoperable solutions, including emerging initiatives such as the EU–Ukraine drone alliance and NATO's Eastern Sentry mission.

The hypothesis of the paper is that, despite Russia's transition to a wartime economy, force expansion, and external military support, NATO's collective conventional superiority continues to provide a credible and decisive deterrent against large-scale Russian aggression, even under scenarios of partial U.S. disengagement. The research question is to what extent does NATO retain credible conventional deterrence against Russia in the context of Russia's wartime military expansion? To operationalize the hypothesis, this study conceptualizes deterrence as NATO's ability to prevent large-scale Russian conventional aggression against Alliance territory by maintaining a credible capability to both retaliate militarily and deny Moscow the attainment of its strategic objectives. Deterrence would be considered to have failed if one of three empirically observable conditions were to occur: (1) a successful large-scale Russian conventional attack on NATO territory; (2) NATO's inability to halt or repel such an offensive within a reasonable operational timeframe; or (3) internal political fragmentation within the Alliance that obstructs a coordinated collective military response. By establishing these benchmarks, the study assesses whether NATO's current military balance, force posture, and level of technological adaptation remain adequate to avert such scenarios.

2. LITERATURE REVIEW

NATO's strategic adaptation and collective defence posture have been extensively examined in the context of conventional deterrence, burden-sharing, and alliance cohesion. Scholars such as Beaver and Kurzweil (2025) emphasize Europe's historical reliance on U.S. security guarantees, noting that recent shifts toward the Indo-Pacific challenge long-standing assumptions about transatlantic security. The debate over European responsibility highlights disparities in defence spending, capability development, and political commitment among NATO members, with countries like Poland, the Baltic states, and Germany often cited as leaders in assuming greater security responsibilities (Chow, 2025). Conversely, states with weaker defence traditions or fiscal constraints, such as Italy, Belgium, Canada, and Slovenia, are perceived as contributing less effectively, raising questions about

the sustainability of equitable burden-sharing. Iskandarov & Gawliczek (2025) examine NATO's New Force Model (NFM) and justify its introduction in response to an evolving and dynamic security environment. The authors delineate NATO's NFM as a desperate need after the war between Russia and Ukraine broke out, highlight the main differences from the Old Force Model.

The literature also underscores the impact of emerging technologies on NATO's operational calculus. The Russia–Ukraine war has served as a live case study demonstrating the transformative effect of autonomous and unmanned systems. Analysts such as Kirichenko (2025) and Foy et al. (2025) highlight Ukraine's innovative use of low-cost drones and unmanned ground vehicles, creating asymmetries that challenge conventional force structures and compel NATO to reconsider high-cost air and missile defence strategies. These studies indicate that autonomous systems not only augment battlefield effectiveness but also impose financial and operational burdens on established powers, necessitating new doctrines, joint industrial efforts, and interoperable technological solutions.

Furthermore, extensive research on Russian military strategy and performance, including studies by Paquette (2025), Marsh (2025), and Dyner (2024), provide insights into the limitations and vulnerabilities of Russian armed forces. Evidence of high equipment losses, attrition-driven strategies, and dependency on foreign support from actors such as Iran, North Korea, China, and Belarus emphasizes both the resilience and constraints of Russian military operations. These findings suggest that NATO's conventional superiority, when coupled with strategic innovation and collective investment, remains a decisive factor in deterrence.

Taken together, the literature converges on three key themes relevant to NATO's strategic adaptation: (1) the imperative for equitable burden-sharing and increased European responsibility, (2) the transformative impact of autonomous and unmanned systems on contemporary warfare, and (3) the enduring importance of collective deterrence against Russian aggression. These themes provide the conceptual and empirical foundation for analyzing NATO's evolving posture in the twenty-first century and framing policy recommendations for sustained Alliance effectiveness.

The study also builds upon both classical and contemporary deterrence theory. Seminal contributions by Lawrence Freedman (2004), Thomas Schelling (2008), Glenn H. Snyder and Paul Diesing (2015) conceptualize

deterrence as the capacity to shape an adversary's decision-making by influencing its perceptions of cost, risk, and credibility. Within the field of NATO studies, deterrence has traditionally been analyzed through the complementary concepts of deterrence by punishment and deterrence by denial, which underscore the Alliance's ability both to impose retaliatory costs and to deny potential territorial gains. More recent scholarship additionally emphasizes the growing significance of technological innovation, alliance cohesion, and economic resilience as critical factors underpinning credible deterrence in contemporary security environments.

Against this backdrop, this paper offers a comprehensive assessment of NATO's core power dynamics, focusing on the relative capabilities of its principal actors, the implications of potential U.S. disengagement, Russia's evolving military posture, and the strategic impact of unmanned and autonomous systems on Alliance defence planning. By integrating comparative military data, doctrinal analysis, and scenario-based reasoning, the study seeks to illuminate the conditions under which NATO's cohesion and credibility may be preserved or undermined in the face of accelerating geopolitical and technological change. In doing so, it contributes to broader debates on transatlantic burden-sharing, European strategic autonomy, and the future of collective defence in an increasingly contested security order.

3. METHODOLOGY

This study employs a qualitative analytical framework combining comparative military capability analysis, doctrinal evaluation, and scenario-based reasoning to assess NATO's ability to sustain credible conventional deterrence against Russia in the evolving European security environment.

First, the research applies comparative capability analysis to examine the distribution of military power between NATO's principal actors (the United States, the European Union, the United Kingdom, Türkiye, and Canada) and Russia. This analysis relies on open-source defence data, including the Global Firepower Index, SIPRI defence expenditure statistics, and institutional assessments from organizations such as the International Institute for Strategic Studies (IISS) and the RAND Corporation. Key indicators examined include defence spending, manpower, equipment inventories, and force structure.

Second, the study incorporates doctrinal and strategic analysis to evaluate Russia's wartime military transformation, including reforms in force structure, expansion of manpower, and defence-industrial mobilization following the 2022

invasion of Ukraine. This component also examines external military support to Russia from actors such as Iran, North Korea, China, and Belarus.

Third, the research employs scenario-based reasoning to explore the implications of potential structural shifts within NATO, particularly scenarios involving partial U.S. strategic retrenchment and increased European responsibility for defence. These scenarios are used to assess whether NATO's aggregate capabilities remain sufficient to sustain credible conventional deterrence.

Finally, the study integrates technological analysis focusing on the operational and economic implications of emerging military technologies, particularly unmanned aerial systems (UAS), autonomous platforms, and counter-drone defence architectures. The Russia–Ukraine war serves as an empirical case illustrating how these technologies reshape modern conflict dynamics and affect deterrence calculations.

By combining comparative military data, doctrinal analysis, and technological assessment, the study evaluates whether NATO's current force posture, industrial capacity, and strategic cohesion are adequate to deter large-scale Russian conventional aggression.

4. RESULTS AND DISCUSSIONS

4.1. NATO's strategic balance

4.1.1. Comparative Military Capabilities

When discussing NATO's overall power, five primary actors stand out: the U.S., the EU, the UK, Türkiye, and Canada (Nasirov et al., 2017; Sadiyev & Iskandarov, 2018; Iskandarov et al., 2019). According to the 2025 Global Firepower, these actors can be compared with each other and against Russia (as the central threat to NATO) based on more prominent parameters.

A comparative assessment of the military capabilities of the U.S., key NATO allies, the EU, and Russia reveals significant asymmetries in defence spending, force structure, and technological capacity. In terms of defence expenditure, the U.S. continues to dominate the transatlantic security architecture, allocating approximately $895 billion in 2024, a figure that far exceeds the military budgets of all other actors considered. Russia's defence spending, estimated at approximately $126 billion, remains substantially lower in absolute terms but nevertheless reflects a high level of militarization relative to the size of its economy. Among other actors, the U.K. allocated roughly $72 billion, while Türkiye and Canada spent approximately $47 billion and $41 billion, respectively. When aggregated, the defence spending of

the EU, estimated at approximately €326 billion, illustrates the considerable but often fragmented military potential of European states.

In terms of personnel strength, the EU collectively maintains the largest pool of active military personnel, numbering approximately 1.5 million troops, slightly exceeding both the U.S. and Russia, each of which maintains around 1.3 million active personnel. Türkiye also possesses a sizeable standing force of approximately 355,200 troops, reflecting its strategic role within NATO's southern flank. By contrast, the UK and Canada maintain significantly smaller active forces of approximately 184,860 and 68,000 personnel, respectively. When reserve components are considered, Russia maintains a substantial mobilization potential with nearly two million reservists, while the EU collectively fields approximately 1.5 million reserve personnel. The UK and the U.S. also possess considerable reserve structures, with approximately 924,000 and 799,500 personnel, respectively.

A pronounced disparity is particularly evident in the domain of air power. The U.S. maintains overwhelming quantitative superiority, operating approximately 13,043 aircraft, a fleet that significantly surpasses those of other actors. Russia fields approximately 4,292 aircraft, while the combined air forces of the European Union amount to roughly 5,000 aircraft. Türkiye maintains approximately 1,083 aircraft, reflecting its substantial regional military capacity, whereas the UK and Canada possess comparatively smaller fleets of 631 and 351 aircraft, respectively.

In terms of armoured warfare capabilities, the EU collectively operates approximately 7,000 combat tanks, representing the largest aggregated armoured force among the actors considered. Russia follows with approximately 5,750 tanks, while the U.S. maintains roughly 4,640 tanks. Türkiye also possesses a substantial armoured inventory of approximately 2,238 tanks, reflecting its longstanding emphasis on conventional land warfare capabilities. In contrast, the UK and Canada maintain relatively limited armoured fleets of 227 and 74 tanks, respectively.

Russia's comparative strength becomes particularly visible in the domain of artillery, a capability that has proven decisive in high-intensity conventional warfare, especially in the ongoing conflict in Ukraine. Russia maintains approximately 5,168 self-propelled artillery systems and around 8,505 towed artillery pieces, significantly exceeding the inventories of most NATO actors. By comparison, the EU collectively operates approximately 2,523 self-propelled systems and 5,678

towed artillery pieces, while the U.S. maintains 671 self-propelled and 1,212 towed artillery systems. Türkiye fields approximately 1,038 self-propelled and 1,707 towed artillery pieces, whereas the UK maintains comparatively modest numbers.

Naval capabilities demonstrate another dimension of power distribution. The U.S. Navy remains the world's most powerful maritime force, operating approximately 440 naval assets, enabling global force projection. Russia maintains around 419 vessels, though many are regionally concentrated and technologically heterogeneous. The European Union collectively fields approximately 500 naval platforms, while Türkiye maintains 182 vessels, reflecting its strategic maritime posture in the Black Sea, Aegean, and Eastern Mediterranean. The United Kingdom and Canada maintain 109 and 73 naval assets, respectively.

Finally, the nuclear dimension remains a central pillar of strategic deterrence. Russia possesses the world's largest nuclear arsenal, estimated at approximately 4,380 nuclear warheads, while the U.S. maintains roughly 3,700 warheads. Within NATO's European members, the UK maintains approximately 225 nuclear warheads, while France possesses roughly 300 warheads, forming the European component of NATO's nuclear deterrent. Neither Türkiye nor Canada maintains independent nuclear arsenals, although Türkiye hosts U.S. nuclear weapons under NATO's nuclear sharing arrangements.

It is evident that Canada wields less influence within NATO compared to the U.S., the UK, Türkiye, and several key European states, including France, Italy, Germany, Spain, Poland, and Sweden. Nevertheless, Canada provides significant added value beyond NATO's EU-centric capabilities. While not a top-tier power within the Alliance, Canada plays an important role in contributing to operational capacity, strategic expertise, and cohesion of the Alliance. For instance, Canada leads NATO's Enhanced Forward Presence (eFP) battlegroup (Multinational Brigade) in Latvia. Additionally, Canadian forces participate in NATO-led missions such as the Kosovo Force (KFOR) and Operation Reassurance in Eastern Europe, contributing to deterrence, collective defence, and multinational interoperability. These commitments underscore Canada's reliability as a NATO member and its ability to enhance Alliance readiness, even without the strategic weight of larger powers.

It is important to note that figures vary across different sources. For example, SIPRI (2025) reports defence expenditures of $997 billion for the U.S., $149 billion

for Russia, $82 billion for the U.K., $62 billion for Türkiye, and $29.3 billion for Canada. Accordingly, any comparison should be understood as relative. Additionally, there are slight differences in the membership of NATO and the EU. For instance, Austria is a member of the EU but not NATO, whereas Albania and Norway are members of NATO but not the EU. In our analysis the EU reflects the influence of its NATO member states rather than the European pillar as a whole. If we rule out nuclear war as an option for confrontation, the analysis clearly shows that, even if the U.S. were to disengage from NATO, the combined power of the remaining four actors would still be significantly stronger than that of Russia. Multiple institutional and think-tank assessments indicate that NATO continues to possess a significant conventional advantage over Russia when evaluated in terms of aggregate military expenditure, advanced capabilities, and force-projection capacity (eurasia.ro, 2025; Kamp, 2026). Analyses conducted by organisations such as the International Institute for Strategic Studies and the RAND Corporation consistently argue that, although Russia maintains considerable regional military strength, NATO's combined economic resources, technological edge, and integrated command structures would constitute substantial barriers to any large-scale conventional offensive against the Alliance (Binnendijk & Franklin, 2018; Arnold, 2024; Barry et al., 2025; Hoffmann, 2025). This would remain a primary deterrent against Russian aggression, as it is commonly described by Western officials. Moreover, Russian equipment losses during Ukraine War have been high: over 1,100 armored vehicles, 3,000+ infantry fighting vehicles, 1,865 tanks, with unfavorable ratios compared to Ukraine (2–5:1). Casualties are also extraordinary: ~250,000 Russian fatalities and over 950,000 total casualties; far exceeding Soviet/Russian wars since WWII (Paquette, 2025). Some estimates suggest losses amounting to roughly 11,329 tanks, 34,273 artillery systems, 1,237 air defence systems, and, most notably, around 1,146,570 total casualties (minfin.com.ua, 2025), although the accuracy of these figures remains contested. As of October 2025, the UK Ministry of Defence reports that Russian forces have sustained approximately 1,118,000 casualties, including both killed and wounded since the onset of the full-scale invasion (Ukrinform, 2025). According to the General Staff of the Armed Forces of Ukraine, Russian personnel losses are estimated at approximately 1,202,000 from February 24, 2022, to December 25, 2025 (RBCUkraine, 2025). Taking the time difference into account, these figures appear to

overlap to some extent. Russia's war strategy has largely failed to achieve Kremlin objectives and demonstrates attrition warfare costs. Contrary to some claims that "Russia holds all the cards", evidence shows poor Russian battlefield performance, limited gains, high equipment losses, and massive casualties. Russia's strategy of attrition is costly and unsustainable, while Ukraine's defences and Western support continue to constrain Russian advances. Strategic leverage lies with the U.S. and its allies, who can shape the outcome by applying economic and military pressure (Jones & McCabe, 2025).

4.1.2. Russian Wartime Military Transformation

It should also be noted that the outbreak of full-scale war with Ukraine and initial Russian setbacks prompted systemic reforms within the Russian Armed Forces. In December 2022, Defence Minister Sergei Shoigu inaugurated a major reform programme, including an increase in manpower to 1.5 million personnel. Shoigu announced the establishment of three new motorized divisions, the reconstitution of seven mechanized brigades into divisions across the Western, Central, and Eastern Military Districts and the Northern Fleet, the creation of two additional airborne divisions, and the transformation of naval infantry brigades into five divisions. He also outlined plans for three new airborne division commands, multiple bomber and fighter regiments, and six Army aviation brigades. These measures signal Russia's intent to enhance its capacity for sustained, large-scale ground operations and reflect broader military, political, and economic pressures on potential adversaries. In 2023, the Russian Ministry of Defence reported the formation of two Combined Arms armies, one air corps, and 50 additional units, including four divisions, 18 brigades, and 28 regiments. The Pacific, Black Sea, and Baltic Fleets were placed under the Navy's direct command, while the Air Force and Air Defence Forces were removed from military district control and subordinated to the Russian Aerospace Forces. Naval infantry units were upgraded from brigade to division structures, and a corps-level command was added to the land forces, creating a four-tier hierarchy: military district, army, corps, and division. These reforms aimed to strengthen command and control and prepare the armed forces for simultaneous, large-scale operations across multiple regions. Russia has consistently expanded the size of its armed forces. In 2021, approximately 900,000 soldiers and officers served in the army. By August 2022, President Putin signed a decree increasing the armed forces by 137,000 personnel,

followed in December 2023 by another increase of 170,000 posts, bringing total strength to 1,320,000. Official figures indicate that 490,000 personnel joined the armed forces in 2023, with over half (~277,000) being conscripts. The expansion has facilitated the gradual rebuilding of capabilities lost during the fighting in Ukraine and supported an increase in the Russian military contingent stationed in occupied Ukrainian territories, which numbered 470,000 troops at the beginning of 2024 (Dyner, 2024). On 15 September 2025, President Putin ordered an increase of 180,000 troops to bring the Russian Army's active strength to 1.5 million, making it the second largest in the world after China's. Simultaneously, Russia significantly ramped up production of military equipment: tank production increased 5.6-fold, armored personnel carriers 2.6-fold, unmanned aerial vehicles (UAVs) 16.6-fold, and artillery ammunition 17.5-fold. UAV production is a particular priority, with plans to produce 6,000 units by 2025, reflecting their growing importance on the battlefield. As one of its most significant recent reforms, Russia has formally established a new military branch dedicated to unmanned systems (drones), a major initiative reflecting lessons learned from the war in Ukraine (Ukrainska Pravda, 2025). Most armaments plants have expanded employment and moved to 24-hour production cycles. For example, while in 2021 Russian plants produced and refurbished approximately 400,000 artillery shells annually, production rose to 3.5 million units in 2023 and 4 million units in 2024.

4.1.3. External Military Support to Russia

Despite battlefield losses, Russia remains capable of conducting intensive military operations in Ukraine, leveraging preexisting stockpiles of heavy equipment, expanding production, and acquiring weaponry and dual-use technologies from external partners, including Belarus, Iran, North Korea and China (Dyner, 2024). Open-source intelligence and satellite imagery suggest that North Korea has transferred an estimated four million artillery shells to Russia since mid-2023, significantly mitigating Moscow's ammunition shortages. By January 2025, approximately 4,000 North Korean troops were reported killed or wounded while fighting alongside Russian forces in Ukraine. In mid-February 2025, Pyongyang dispatched an additional 3,000 soldiers, who were reportedly better trained and more combat-ready than earlier deployments (Balmforth & Zafra, 2025). Multiple intelligence and media reports indicate that Iran has supplied Russia with substantial military assistance,

including hundreds of ballistic and short-range guided missiles, strike drones, and training for Russian personnel on advanced systems such as the Fath-360. This cooperation has significantly enhanced Russia's long-range strike capabilities and bolstered its capacity to sustain high-intensity operations against Ukraine (Deutsch et al., 2024). The U.S. and allied intelligence assessments reveal that Chinese-linked companies and supply-chain networks have facilitated Russia's ability to acquire critical materials and technologies including electronic components, semiconductors, and drone parts despite extensive Western sanctions. These transfers have enabled Moscow to sustain and expand its defence-industrial production, thereby mitigating the intended impact of international export restrictions (U.S.-China Economic and Security Review Commission, 2025). In 2023 alone, as much as 90% of Russia's microelectronics imports were sourced from China (Madhani, 2024). The patterns of technology transfer and cooperation reinforce the scenario dimension of China–Russia strategic convergence, which must be considered in the context of future NATO planning and scenario development. Furthermore, Belarus has periodically deployed substantial forces along the Ukrainian border and has formalized deeper military cooperation with Russia through joint formations, exercises, and hosting of Russian units. This partnership provides Moscow with forward basing, enhanced logistical corridors, and expanded avenues for force projection into Ukraine and the broader region (Reuters, 2024). Independent assessments, including those by the IISS and various intelligence summaries, indicate substantial Russian equipment losses in 2024, particularly in tanks and infantry fighting vehicles (IFVs). However, these analyses stress that external imports and increased defence spending have enabled Russia to refurbish, replace, and procure new systems, allowing it to maintain sustained operational capabilities, even as overall qualitative readiness remains under strain (Clavilier & Gjerstad, 2025). Drawing on his extensive expertise on Vladimir Putin and Russian strategic culture, Philip Short (Putin biographer) argues that Russia having transitioned to a wartime economy and supported by a resilient political system may be better positioned than many Western analysts commonly assume, particularly if the European Union and its allies are unable to offset any future reduction in U.S. military assistance to Ukraine. He further suggests that, although Putin may seek to orchestrate an orderly succession, the feasibility of such a transition is highly contingent on achieving a favourable outcome in

Ukraine. In this regard, the dynamics of domestic Russian politics and the trajectory of the war are profoundly interlinked (Marsh, 2025).

In conclusion, despite Russia's ongoing military expansion and foreign support, NATO's collective strength led by the U.S., key European states, Türkiye, and supported by Canada remains decisively superior. Russian losses and an unsustainable attrition strategy limit its operational reach, making large-scale aggression strategically unattractive. NATO's deterrence posture, multinational interoperability, and capacity to project power collectively provide a credible counterbalance, ensuring that any large-scale aggression by Russia would be strategically unattractive and politically costly.

5. EUROPEAN DEFENCE IN A TRANSFORMING NATO

5.1. Defence Spending Commitments

If the U.S. significantly scales back its presence in Europe, NATO will likely abandon its expansionist agenda of recent decades and focus solely on defending its existing members. However, this shift could generate considerable tensions among NATO allies regarding their approach to Russia. The EU column represents the combined military capabilities of all EU member states, with key countries like France, Italy, Germany, Spain, Poland, Sweden, and Greece ranking within the top 30. These nations account for 72% of the overall EU defence budget, totaling approximately €235 billion, and 70% of the EU's overall manpower, which amounts to approximately 1,050,000 personnel. It is not difficult to imagine the repercussions if a rift were to emerge among the EU states within the top 20. The U.S. disengagement, combined with a potential schism within the Union and the alienation of Türkiye and the UK, would undoubtedly signal the demise of NATO. This would represent the worst-case scenario for the Alliance. However, it must be acknowledged that the Russia-Ukraine war has strengthened cohesion within the Union, as well as with the UK. Additionally, the potential U.S. disengagement has brought relations with Türkiye to the forefront. At this juncture, it is important to reflect on certain key uncertainties surrounding the statistical figures. Beaver & Kurzweil (2025) state that, for decades, Europe has relied heavily on U.S. security guarantees within NATO, but this dependency is now being questioned as Washington pivots toward the Indo-Pacific. At the 2025 NATO Summit, allies formally pledged to increase defence spending to 5% of GDP by 2035, 3.5% on core defence and 1.5% on infrastructure and civil preparedness. This marks a significant shift toward

greater European responsibility for collective defence. Several nations, particularly Poland, the Baltic states, the Nordics, and Germany, have taken the lead by setting ambitious timetables to meet or exceed the new benchmark well before the deadline. Their strong commitments reflect a broader recognition that Europe, with its vast economic resources, is more than capable of defending itself if the political will exists. Other allies, such as France, Greece, the UK, and a cluster of Central and Eastern European states, have pledged to meet the 2035 target but face steeper challenges in scaling up their budgets. Meanwhile, countries like Italy, Belgium, Canada, and Slovenia have offered commitments that appear less credible due to weak defence traditions or fiscal constraints. Spain stands out as the only member rejecting the new goal outright, drawing criticism for its unwillingness to shoulder greater responsibility. According to Brian Chow (2025), the Hague Summit commitment risks collapse without a pragmatic and incremental roadmap. Delaying action until 2034 would render the abrupt doubling of defence budgets politically untenable, echoing the shortcomings of the 2014 pledge. With Russia entrenched in Ukraine, supported by China, North Korea, and Iran and continuing to pose broader threats to European security, NATO must initiate immediate and sustained increases in defence expenditure. Preserving the 2023 baseline of $1.28 trillion while adding $115 billion annually would not only smooth the transition toward 2035 but also generate $6.3 trillion over the decade, thereby strengthening readiness in the near term. Although the U.S. carries a disproportionate share of this effort, approximately $2.3 trillion, or 37% of the total, the proposed framework of equitable burden-sharing aligns contributions with GDP disparities among allies. Ultimately, only gradual and systemic increases can preserve Trump's hard-won 5% commitment, bolster NATO's deterrence posture, and demonstrate that democratic alliances can outlast authoritarian coalitions. Still, the overall trajectory is encouraging: if Europe follows through on its spending promises and the U.S. concentrates on countering China, NATO will be better positioned by the 2030s to safeguard both European and transatlantic security interests.

5.2. Drone Warfare and Cost Asymmetry

Almost four years into the Russia–Ukraine war, unmanned and autonomous systems have emerged as defining features of the conflict. Ukraine has relied extensively on low-cost drones and, increasingly, unmanned ground vehicles (UGVs) to offset Russia's superior firepower, developing what

has been described as a "drone wall" to blunt assaults. Operations such as Spider's Web illustrate how inexpensive systems can strike deep into Russian territory, inflicting damage on critical infrastructure and imposing substantial economic costs. Russia, however, has adapted in parallel, accelerating domestic drone production, integrating Iranian designs, and experimenting with robotic platforms ranging from basic supply carriers to sophisticated weaponized UGVs. This iterative cycle of innovation and counter-innovation has created what analysts call a "global adaptation war", with Moscow actively sharing lessons with partners such as China, Iran, and North Korea. For the West, this dynamic presents both an urgent challenge and a strategic opportunity. On the one hand, prolonged conflict allows Russia and its partners to refine, test, and proliferate new technologies in real time. On the other, Ukraine provides unparalleled battlefield insights into how unmanned systems can be developed, deployed, and countered at scale. European states, already collaborating with Ukraine on joint production ventures, are particularly well positioned to leverage these lessons to reinforce their defence-industrial base. The erosion of traditional models of land warfare demonstrates that autonomous and robotic systems are no longer peripheral innovations but have become enduring instruments of modern conflict (Kirichenko, 2025). The Russia–Ukraine war highlights the centrality of unmanned and autonomous systems in contemporary warfare. The conflict has evolved into a laboratory of adaptation, where both sides continually innovate to gain tactical and strategic advantage. For NATO and European partners, the implications are profound: the ability to integrate, scale, and counter such technologies will increasingly determine battlefield effectiveness. If harnessed strategically, the lessons learned from Ukraine could serve not only to strengthen European defence capabilities but also to shape the broader trajectory of warfare in the twenty-first century. The Russian drone incursion into Poland on September 9, 2025, involving 19 drones, some of which penetrated more than 100 miles inland has underscored both the escalating threat posed by unmanned aerial systems and the significant financial burden they impose on NATO's defence infrastructure. While Russia's drones are relatively inexpensive, costing approximately $10,000 –$50,000 each (Gerbera drones cost approximately $10,000 and Shahed drones cost around $50,000) (Melchior, 2025), the cost for NATO to intercept (by deploying fighter jets and activating surface-to-air missile systems) these threats is significantly higher. For instance, the deployment of advanced systems such as the F-35 fighter jets and Patriot missile defence

systems, which were activated during the Polish airspace violation, incurs costs in the millions of dollars (Burrows, 2025). This disparity underscores the mounting financial strain on NATO, as the Alliance is compelled to invest heavily in sophisticated countermeasures to counter the rising prevalence of low-cost drone attacks. Such circumstances necessitate a thorough reevaluation of defence strategies to ensure responses that are both cost-effective and sustainable within the evolving landscape of modern warfare. Repeated incursions, in particular, risk imposing a substantial financial burden on member states, as inexpensive threats consistently demand disproportionately expensive responses. While NATO is fully cognizant of the widening asymmetry between low-cost drone capabilities and high-cost conventional defences and has begun exploring cost-efficient alternatives, it remains insufficiently prepared to confront large-scale, sustained incursions executed exclusively with inexpensive technologies. Foy et al. (2025) contend that, in the aftermath of the incursion, the EU has accelerated investments worth billions to establish a "drone wall" along its eastern frontier, drawing on technologies battle-tested in Ukraine. NATO's reliance on costly jets and missiles to counter relatively inexpensive drones has exposed a vulnerability that Moscow could exploit, prompting European capitals to pool resources in pursuit of cost-effective, integrated solutions. Central to this effort is a €6 billion EU–Ukraine "drone Alliance" aimed at industrializing Ukrainian innovations, while frontline states such as Poland, the Baltic countries, and Finland seek to fortify their borders within a coordinated framework. In the interim, NATO has activated the Eastern Sentry air defence mission, deploying fighter jets, naval assets, and reconnaissance systems. Ukrainian operational experience has been particularly influential, demonstrating the effectiveness of acoustic sensors for detecting low-flying drones and mobile units equipped with anti-aircraft cannons for interception, an approach far more economical than conventional missile systems. Several EU states have begun to adopt similar tactics, underscoring the growing imperative for affordable, innovative, and unified counter-drone measures in response to the evolving threats of modern warfare. According to the authors, research and development are also advancing in directed-energy weapons, electronic warfare systems, and drone-on-drone interception technologies, with some of these capabilities expected to reach operational readiness within the next three to five years. The cost asymmetry between low-cost

offensive drones and expensive defensive systems also has important implications for the credibility of deterrence. If adversaries are able to impose repeatedly disproportionate financial burdens on NATO's defensive infrastructure, the long-term sustainability of deterrence by denial may gradually weaken. Accordingly, the Alliance's capacity to preserve credible deterrence will increasingly depend on the development of scalable and economically sustainable countermeasures, including advanced electronic warfare capabilities, directed-energy technologies, and low-cost interception systems.

6. CONCLUSIONS

NATO's strategic posture in the contemporary security environment demonstrates both resilience and adaptability in the face of evolving threats. While the U.S and key European allies provide the backbone of conventional military power, middle-tier contributors such as Canada play a critical role in sustaining operational capacity, cohesion, and multinational interoperability. The Russia–Ukraine war has highlighted the transformative impact of autonomous and unmanned systems, emphasizing the need for cost-effective, innovative responses and lessons-driven defence planning. Despite Russia's ongoing military expansion, foreign support, and technological adaptation, its unsustainable attrition strategy, high equipment losses, and constrained operational reach render large-scale aggression strategically unattractive. NATO's deterrence capability rests on a combination of collective strength, coordinated burden-sharing, and the integration of emerging technologies, particularly in counter-drone and autonomous warfare. Looking ahead, maintaining Alliance readiness will require sustained European investment, technological innovation, and flexible strategic planning to ensure that NATO remains a credible and effective guarantor of transatlantic security in the twenty-first century.

REFERENCES

[1] Arnold, Ed (2024). NATO Would 'Wipe Out Russia's Army in a Matter of Months.' Royal United Services Institute, December 22. https://www.rusi.org/news-and-comment/in-the-news/nato-would-wipe-out-russias-army-matter-months.

[2] Balmforth, Tom, and Maria Zafra (2025). Thousands of Troops, Millions of Shells: Inside North Korea's Vast Operation to Help Russia's War on Ukraine. *Reuters*, April 15. https://www.reuters.com/graphics/UKRAINE-CRISIS/NORTHKOREA-RUSSIA/lgvdxqjwbvo/.

[3] Barry, Ben, Douglas Barrie, Henry Boyd, Nick Childs, Michael Gjerstad, James Hackett, Fenella

McGerty, Ben Schreer, and Tom Waldwyn (2025). *Defending Europe Without the United States: Costs and Consequences.* London: International Institute for Strategic Studies. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/05/defending-europe-without-the-united-states/iiss_defending-europe-without-the-united-states_costs-and-consequences_052025.pdf.

[4] Beaver, William, and Arielle Kurzweil (2025). Is NATO Sticking to Its New Defence Spending Goals? *The Heritage Foundation*. Accessed September 16. https://www.heritage.org/defence/commentary/nato-sticking-its-new-defence-spending-goals.

[5] Binnendijk, Hans, and Franklin D. Kramer (2018). *Meeting the Russian Conventional Challenge: Effective Deterrence by Prompt Reinforcement*. Washington, DC: Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/meeting-the-russian-conventional-challenge/.

[6] Burrows, Emma (2025). NATO's First Drone Battle Pits Million-Dollar Jets Against Cheap Drones, Exposing Vulnerabilities. *Military.com*, September 11. https://apnews.com/article/poland-russia-drones-jamming-ukraine-incursion-nato-27b1aeed542604c91386df1fbe4463c7.

[7] Chow, Brian (2025). NATO Needs a Realistic Path to 5 Percent Defence Spending by 2035. *The National Interest*, September 27. https://nationalinterest.org/blog/buzz/nato-needs-a-realistic-path-to-5-percent-defence-spending-by-2035.

[8] Clavilier, Yohan, and Marius Gjerstad (2025). Combat Losses and Manpower Challenges Underscore the Importance of 'Mass' in Ukraine. *International Institute for Strategic Studies*, February 10. https://www.iiss.org/online-analysis/military-balance/2025/02/combat-losses-and-manpower-challenges-underscore-the-importance-of-mass-in-ukraine/.

[9] Deutsch, Anthony, Tom Balmforth, and Jonathan Landay (2024). Exclusive: Iran to Deliver Hundreds of Ballistic Missiles to Russia Soon, Intel Sources Say. *Reuters*, August 9. https://www.reuters.com/business/aerospace-defence/iran-deliver-hundreds-ballistic-missiles-russia-soon-intel-sources-say-2024-08-09/.

[10] Dyner, Anna Maria (2024). *Russia's Armed Forces Two Years After the Full-Scale Invasion of Ukraine.* Polish Institute of International Affairs. https://pism.pl/publications/russias-armed-forces-two-years-after-the-full-scale-invasion-of-ukraine.

[11] Eurasia.ro (2025). A Russia–NATO War Would Look Nothing Like Ukraine. May 20. https://eurasia.ro/2025/05/20/a-russia-nato-war-would-look-nothing-like-ukraine/.

[12] Foy, Henry, Laura Pitel, Ben Hall, and Richard Milne (2025). Europe Turns to Ukrainian Tech for 'Drone Wall' Against Russia. *Financial Times*, September 17. https://www.ft.com/content/060875fe-95cc-

4cbb-bec9-654422b045fa.

[13] Freedman, Lawrence (2004). *Deterrence*. Cambridge: Polity Press.

[14] Glenn H. Snyder and Paul Diesing (2015). *Conflict Among Nations: Bargaining, Decision Making, and System Structure in International Crises* (Princeton, NJ: Princeton University Press), https://doi.org/10.1515/9781400871186.

[15] Hoffmann, Fabian (2025). A Russia-NATO War Would Look Nothing Like Ukraine. Foreign Policy, May 19, https://foreignpolicy.com/2025/05/19/russia-nato-war-putin-ukraine-nuclear-strategy-baltics/.

[16] Iskandarov, Khayal, and Piotr Gawliczek (2025). NATO's New Force Model: Adapting to a Dynamic Security Landscape. *Journal of Defense Resources Management* 16, no. 2 (31): 141–156.

[17] Iskandarov, Khayal, Piotr Gawliczek, and Mahammad Akbarov (2025). NATO's New Force Model and Partner Engagement in an Evolving Security Landscape. *Social Development and Security* 15, no. 2: 1–11. https://doi.org/10.33445/sds.2025.15.2.1

[18] Iskandarov, Khayal, Piotr Gawliczek, and Jacek Mrozek (2023). *NATO's Partnership Policy in a Dynamic Security Landscape: A Simple Look at a Complex Picture.* Olsztyn: Centre for Eastern Europe Research UWM.

[19] Iskandarov, Khayal, Piotr Gawliczek, and Jacek Mrozek (2026). *The future of NATO: Strategic scenarios and policy insights*. Oficyna Wydawnicza ASPRA-JR, Warszawa.

[20] Iskandarov, Khayal, Vugar Mammadzada, and Sadi Sadiyev. 2019. "Non-Alliance Policy as a Principle of Shaping the National Security with a Focus on the Case of Azerbaijan." *Journal of Defense Resources Management* 10, no. 2: 62–72. https://www.ceeol.com/search/article-detail?id=812186.

[21] Iskandarov, Khayal, Greg Simons, and Piotr Gawliczek. 2019. "The South Caucasus: Stage for a 'New Great Game' Between NATO and Russia?" *Connections: The Quarterly Journal* 18: 3–4. https://doi.org/10.11610/Connections.18.3-4.01.

[22] Jones, Seth G., and Riley McCabe (2025). Russia's Battlefield Woes in Ukraine. *Center for Strategic and International Studies (CSIS)*, June 3. Accessed September 23, 2025. https://www.csis.org/analysis/russias-battlefield-woes-ukraine.

[23] Kamp, Karl-Heinz (2026). *Europe Against Russia Without the US? Not Europe's Preference but Possible.* DGAP Memo No. 17. Berlin: German Council on Foreign Relations. https://dgap.org/en/research/publications/europe-against-russia-without-us-not-europes-preference-possible.

[24] Kirichenko, Dmitri. 2025. "Is NATO Prepared for Autonomous Warfare?" *The National Interest*, September 10. https://nationalinterest.org/feature/is-nato-prepared-for-autonomous-warfare.

[25] Madhani, Aamer. 2024. "US Intelligence Finding Shows China Surging Equipment Sales to Russia

to Help War Effort in Ukraine." *Associated Press News*, April 12. https://www.apnews.com/article/united-states-china-russia-ukraine-war-265df843be030b7183c95b6f3afca8ec.

[26] Marsh, David. 2025. "Putin Biographer Forecasts Russo-Ukraine War Will Drag On." *OMFIF Insights*, March 7. https://www.omfif.org/2025/03/putin-biographer-forecasts-russo-ukraine-war-will-drag-on/.

[27] Minfin.com.ua (2025). Потери России в Украине – официальные данные. https://index.minfin.com.ua/russian-invading/casualties/.

[28] Nasirov, Elman, Khayal Iskandarov, and Shahin Sadiyev. 2017. "The South Caucasus: A Playground between NATO and Russia?" *Connections* 16, no. 3: 47–56. https://www.jstor.org/stable/26867919.

[29] Paquette, Alexandre (2025). "Assessing the Likelihood of a Russian Attack on NATO: An Analysis Based on Intelligence up to June 4, 2025. https://assessing-the-likelihood-4849y3j.gamma.site/.

[30] Reuters (2024). Nearly a Third of Belarus Army Deployed on Ukraine Border, Lukashenko Says. August 18. Accessed November 2, 2025. https://www.reuters.com/world/europe/belarus-lukashenko-says-nearly-third-army-sent-ukraine-border-belta-reports-2024-08-18/.

[31] RBC Ukraine (2025). "Russia's Losses in Ukraine as of December 25: +860 Troops and 59 Artillery Systems." December 25. Accessed December 25, 2025. https://newsukraine.rbc.ua/news/russia-s-losses-in-ukraine-as-of-december-1766644805.html.

[32] Sadiyev, Sadi, and Khayal Iskandarov (2018). "The Evolution of the Security Environment in the South Caucasus since the End of the Cold War." In *17th Workshop of the PfP Consortium Study Group Regional Stability in the South Caucasus: 'What a New European Security Deal' Could Mean for the South Caucasus*, 47–53. 2018. Accessed December 26, 2025. https://www.academia.edu/37852657.

[33] Schelling, Thomas (2008). *Arms and influence*. New Haven: Yale University Press.

[34] Ukrainska Pravda (2025). "Russia Establishes Unmanned Systems Forces." November 12. Accessed December 25, 2025. https://www.pravda.com.ua/eng/news/2025/11/12/8006978/.

[35] Ukrinform (2025). British Intelligence Estimates Overall Russian Casualties in the Ukraine War at 1,118,000. October 14. https://www.ukrinform.net/rubric-ato/4047258-british-intelligence-estimates-overall-russian-casualties-in-the-ukraine-war-at-1118000.html.

[36] U.S.-China Economic and Security Review Commission (2025). China's Position on Russia's Invasion of Ukraine: Key Events and Statements from February 21, 2022 through August 31, 2025. https://www.uscc.gov/research/chinas-position-russias-invasion-ukraine.

SAFE AND THE EUROPEAN STRATEGIC AUTONOMY: FROM COORDINATION TO CAPABILITY DELIVERY

Maria CONSTANTINESCU

Regional Department of Defense Resources Management Studies (DRESMARA) / "Carol I", National Defense University, Brasov, Romania

The adoption of the Security Action for Europe (SAFE) in 2025 marks a pivotal transformation in the EU's approach to defense resources. This paper analyzes SAFE as a paradigm shift from grant-based cooperation to loan-based strategic investment, introducing a novel fiscal architecture to close the EU's persistent "coordination–capability gap." Drawing on qualitative analysis of the SAFE Regulation, National Defense Investment Plans (NDIPs), and early implementation data from 2025–2026, the analysis finds that SAFE's loan-based, jointly-conditioned mechanism has the potential to shift member state procurement from nationally fragmented acquisitions toward structured, EU-aligned capability programs. The instrument's long-term effectiveness is however constrained by three inherent structural tensions: differential industrial absorption capacity across member states, the moral hazard of subsidized sovereign lending, and industrial protectionism embedded in the instrument's non-EU component cap. A comparative analysis of the NDIPs of Poland and Romania, the two largest SAFE beneficiaries, demonstrates how these tensions manifest in practice, shaping national procurement strategies and capability outcomes. The paper concludes that while SAFE's fiscal architecture provides a sound framework for capability delivery, its success will ultimately depend on member state political will and institutional capacity.

Key words: *SAFE, autonomy, coordination, capability, gap*

1. INTRODUCTION

On 6 March 2025, the President of the European Commission announced the ReArm Europe plan - a package of measures designed to mobilize up to €800 billion in additional defense investment across the European Union over the following years (EU Commission 2025). Less than three months later, on 27 May 2025, the Council of the European Union formally adopted Regulation 2025/1106, establishing the Security Action for Europe (SAFE): a €150 billion loan facility enabling Member States to finance joint procurement of priority defense capabilities at competitive rates,

[1] ORCID ID: 0000-0002-9096-0739, e-mail: constantinescumaria.ro@gmail.com

backed by the EU's collective credit rating (EU Council, 2025).

The speed and scale of this legislative response were unprecedented in the history of European defense cooperation, connected to the geopolitical context changes arising after February 2022. Russia's invasion of Ukraine exposed the structural inadequacy of Europe's defense posture and the limits of the voluntary coordination mechanisms that had governed EU defense cooperation for two decades. The return of Donald Trump to the U.S. presidency in January 2025, accompanied by explicit signals of conditional commitment to NATO's collective defense guarantee, removed any remaining ambiguity: Europe could no longer treat its own defense as a residual responsibility. The Readiness 2030 agenda, of which SAFE is the central fiscal pillar, represents the EU's institutional response to this twin rupture in the post-Cold War security order (EU Commission 2025).

Yet despite the attention SAFE has generated since its adoption, the instrument remains systematically under-analyzed from the perspective of defense resource management. Existing scholarship on European strategic autonomy has concentrated predominantly on two dimensions: the political dimension, the decision-making independence from the United States (Fiott,2025) (Zandee at al, 2020) and the industrial dimension, the development of the European Defense Technological and Industrial Base (Mueller, 2025), (Hartley, 2011). The *fiscal dimension*, namely the specific architecture of financial instruments, conditionalities, and governance rules that determines whether increased political will and industrial ambition translate into actual capabilities, has received comparatively little systematic attention.

2. METHODOLOGY

This paper employs a qualitative research design combining documentary policy analysis with structured comparative institutional analysis. The primary data source consists of official EU legal and policy documents, supplemented by the publicly available National Defence Investment Plans submitted by member states, official government statements, and early implementation announcements and the established literature on EU defense financing instruments. NDIPs were selected as the primary empirical source because they represent the first instance in which member states have been required to disclose detailed defense procurement intentions as a condition of accessing EU financing.

Secondary sources include peer-reviewed academic articles, policy reports from recognized research institutions (EDA, IISS, SIPRI,

Bruegel, EPRS, ECB and NATO), and official data from the European Defence Agency's Defence Data series.

The analysis refers to the period from SAFE's adoption in May 2025 to the first disbursement phase in early 2026, reflecting the available literature at the time of writing.

The Poland–Romania comparison was selected because both states are on NATO's eastern flank with elevated threat perceptions, both rank among the top three SAFE beneficiaries by allocation, both disclosed enough information to permit structured comparison, and they differ substantially across key dimensions relevant to SAFE's effectiveness (industrial absorption capacity, fiscal capacity, and NDIP structure).

The NDIP data is analyzed along four comparative dimensions: allocation size and structure (percentage dedicated to acquisitions versus infrastructure), the ratio of joint to national procurement programs, sectoral distribution of procurement priorities, and domestic industrial content requirements. Where available, systematic indicators are reported, including the percentage of joint procurement projects within each NDIP, SAFE-to-annual-defense-budget ratios as a proxy for absorption risk, and the share of SAFE allocations directed to each capability category.

Important limitations must be acknowledged: NDIPs are political documents as much as planning instruments and they reflect stated intentions rather than executed contracts. Execution rates, delivery timelines, and actual disbursement data are not yet available for systematic comparison and will require longitudinal analysis as the program matures beyond the first disbursement phase. Also, the Commission has not yet published systematic cross-national execution dashboards, so NDIPs and first-wave announcements are treated as planning and initial implementation proxies rather than definitive evidence of delivery.

Three research questions structure the paper.

RQ1: How does SAFE's loan-based fiscal architecture alter the traditional resource management model of EU defense, compared to prior grant-based instruments such as EDIRPA, ASAP, and the European Defense Fund?

RQ2: To what extent does SAFE's conditionality structure - joint procurement requirements, National Defense Investment Plans, and the 35% non-EU component cap -accelerate capability delivery while managing the risk of industrial fragmentation?

RQ3: What are the strategic management implications for national defense ministries navigating the

debt-versus-capability trade-off that SAFE introduces?

The analysis is structured around two research hypotheses.

H1 - the Fiscal Architecture Hypothesis: SAFE's loan-based fiscal architecture produces a qualitatively different pattern of defense resource allocation than prior EU grant-based instruments, specifically by shifting member state procurement behavior from nationally fragmented acquisitions toward jointly structured, EU-conditioned capability programs.

H2 the Structural Tension Hypothesis: The effectiveness of SAFE in closing the coordination–capability gap is systematically constrained by three structural tensions: different absorption capacity across member states, the moral hazard inherent in subsidized sovereign lending, and the industrial protectionism embedded in the 35% non-EU component cap, such that fiscal scale alone is insufficient to guarantee capability delivery.

3.THEORETICAL FRAMEWORK: FISCAL ARCHITECTURE, STRATEGIC AUTONOMY, AND THE ECONOMICS OF EUROPEAN DEFENSE

The theoretical framework of the SAFE mechanism derives from three bodies of literature: the political science literature on European strategic autonomy, the public economics literature on fiscal federalism and supranational public goods, and the defense economics literature on procurement fragmentation costs.

Strategic autonomy has become one of the most frequently invoked yet analytically contested concepts in European security studies. Its interpretations range from full independence from external powers to a more modest capacity for autonomous action within alliance frameworks. For the purposes of this paper, strategic autonomy operates across three analytically distinct dimensions:

- the political dimension, concerning decision-making independence from external actors, notably the United States;
- the industrial dimension, concerning the European capacity to develop, produce, and maintain the defense equipment European armed forces require;
- the fiscal dimension, concerning the ability to mobilize, allocate, and sustain the resources necessary to translate political will and industrial ambition into actual military capabilities.

SAFE is the first EU instrument to directly address the fiscal dimension of strategic autonomy,

particularly the set of financial instruments, incentive structures, conditionalities, and governance rules which constitute the framework of defense investments. Every previous instrument touched the political or industrial dimensions and assumed the fiscal would follow. It did not.

Fiscal federalism theory provides the foundational logic for why supranational financing instruments for defense are both economically rational and institutionally resisted. The core insight, drawing upon the classic body of literature (Musgrave, 1959) (Oates, 1972) is that the optimal level of government for providing a public good corresponds to the geographic scope of that good's benefits. Collective defense against shared threats is a quintessential transnational public good that cannot be efficiently provided by fragmented national actors acting independently (Olson and Zeckhauser, 1966), (Sandler and Hartley 1999).

Applied to the EU context, this means European defense should be financed, at least partially, at the supranational level. Until SAFE, EU fiscal instruments for defense were limited to modest grant programs operating well below the required scale. The structural obstacle was the EU's own architecture: no autonomous tax base, and fiscal rules that treat defense spending as any other public expenditure subject to deficit limits.

The change in the security environment prompted the need for the EU to start considering defense expenditures as a political priority and the solution to circumvent the fiscal restrictions was EU-level borrowing on capital markets, leveraging the bloc's collective AAA credit rating, followed by on-lending to member states at rates unavailable to many of them individually (Bénassy-Quéré et al. 2021). The precedent set by NextGenerationEU (NGEU) is analytically significant: the COVID recovery fund demonstrated that EU-level debt issuance could mobilize resources at a scale and speed that intergovernmental coordination alone could not achieve, while simultaneously generating a political debate about whether such instruments should become permanent features of the EU's fiscal architecture (Cepparulo and Reitano 2025). The European Central Bank's analysis of defense spending's macroeconomic implications confirms that SAFE-type instruments, when channeled through joint procurement, can generate positive GDP effects of approximately 0.1 percentage points per year while containing inflationary pressures, provided the stimulus favors European-made military goods and defense R&D with civilian spillovers (ECB 2025), (Moretti, Steinwender and Van Reenen 2025). Recent scholarship on EU defense industrial

policy has further documented the structural transformation underway: Genini (2025) demonstrates that the EU's defense industrial base has undergone an unprecedented wave of integration since 2022, with aggregate defense expenditure increasing by 36% and new instruments such as the EIB's tripled defense lending and the proposed Savings and Investments Union seeking to channel private capital into defense. These developments position SAFE within a broader institutional evolution from ad hoc crisis response toward a structured EU fiscal capacity for security.

SAFE's defining innovation derives from its supranational fiscal capacity for defense without requiring an EU tax base or a full transfer of fiscal sovereignty. Just as the European Stability Mechanism created a supranational lending facility for macroeconomic stabilization, SAFE creates one for defense capability investment. Yet SAFE is not a European treasury in miniature. In the post-NextGenerationEU debate, it is better understood as a partial, sector-specific, and temporary fiscal-capacity instrument that uses common borrowing to finance a strategic public good while leaving repayment obligations at national level (Arnal et al. 2026), (ECB 2025).

Recent scholarship on EU fiscal capacity and defense industrial policy strengthens this interpretation. Post-NGEU analyses ask whether common borrowing will remain an exceptional crisis device or evolve into a more durable Union instrument for strategic investment, while recent work on EU defense industrial policy emphasizes that financing alone does not solve fragmentation, information-sharing problems, third-country controversies, or weak integration with NATO planning (Besch 2025). SAFE therefore sits at the intersection of two debates: the future of EU fiscal capacity and the institutional governance of European rearmament.

The economic rationale is strengthened by the evidence on what fragmentation costs. The European Parliamentary Research Service estimates the annual cost of non-Europe in defense (the efficiency losses from duplicating capabilities, procurement systems, and research programs across 27 national defense establishments) at between €18 and €57 billion per year (Centrone and Fernandes 2024).

EU member states collectively maintain over 170 different weapons systems, compared to fewer than 30 in the United States, generating significant diseconomies of scale in procurement, maintenance, and training (EDA 2025). By incentivizing joint procurement through conditioned lending, SAFE aims to close these gaps by

capitalizing on economies of scale that fragmented national procurement structurally cannot generate.

This paper introduces the concept of the *coordination–capability gap* to denote the persistent disparity between the stated political ambitions of European defense cooperation and the military capabilities those cooperative frameworks have actually produced.

To make this concept analytically robust and reusable in future research, the gap is operationalized along four measurable dimensions. First, the procurement fragmentation ratio: the share of total EU defense procurement conducted jointly (multi-state) versus purely national channels. Second, the degree of alignment between NDIPs and EU or NATO capability priorities. Third, the administrative capacity to convert endorsed plans into contracts, disbursements, and deliveries, a metric that prior instruments (PESCO, EDF) have struggled to optimize. Fourth, the interoperability deficit: the degree to which nationally procured systems can operate seamlessly within multinational force structures, measurable through NATO Standardization Agreement (STANAG) compliance rates and performance in joint exercises. These four dimensions provide a structured framework for assessing whether SAFE, or any successor instrument, is narrowing the gap between cooperative intent and operational capability.

On the coordination side of the identified gap, the EU already possesses important but incomplete mechanisms: CARD aligns planning assumptions, the EDF funds collaborative R&D, and PESCO organizes structured cooperation. These arrangements generate policy convergence and some industrial collaboration, but they do not directly finance capability acquisition at the scale required to close Europe's identified defense gaps, nor do they by themselves guarantee procurement aggregation, implementation discipline, or standardized force outcomes. The incentives are too voluntary and the national free-rider logic too durable for coordination alone to close Europe's capability shortfalls.

The capability side is what coordination was supposed to produce but did so in a very limited manner: interoperable hardware, deployable force structures, and the logistical and industrial base to sustain them at scale. Collective defense is a transnational public good in the technical sense, which means every member state has a structural incentive to let someone else pay for it. Voluntary, grant-based mechanisms don't dissolve that incentive. They work around it, temporarily, until the political moment passes.

The coordination–capability gap serves as the analytical lens through which this paper evaluates the evolution of EU defense financing instruments, distinguishing between those that primarily foster political and industrial *coordination* (PESCO and the EDF) and those, like SAFE, that are designed with a fiscal architecture to directly finance and incentivize the delivery of *capability*.

From this perspective, SAFE represents the first truly systematic attempt to close this gap through a fiscal architecture that makes capability delivery the primary objective of EU defense governance.

4. FROM PESCO TO SAFE

SAFE is the product of a decade-long institutional learning process in which the EU progressively escalated its defense financing ambition, each instrument responding to the demonstrated inadequacies of its predecessor.

Permanent Structured Cooperation (PESCO), established in 2017, created the EU's first legally binding defense cooperation framework, encompassing 26 member states and 68 collaborative projects by 2023 (Council of the EU, 2017) (EDA, 2023). Yet PESCO provided no EU-level financing, as it was a coordination mechanism without a fiscal instrument, the equivalent of agreeing to build a house without providing either the materials or the money. The European Defence Fund (EDF), operational from 2021 with a budget of €8.8 billion broke the longstanding taboo against EU defense expenditure by co-financing collaborative research and development (European Commission, 2021). By 2025, five work programs had committed €5.4 billion to collaborative projects (European Commission, 2025). The drawback is that the EDF finances R&D, not procurement and the most critical period - the gap between development and acquisition that economists call the “valley of death” for suppliers - remained unaddressed.

Russia's invasion of Ukraine in 2022 forced the EU into procurement financing for the first time. EDIRPA (€310 million, 2023) incentivized joint procurement of urgently needed defense products and ASAP (€500 million, 2023) targeted artillery ammunition and missile production capacity (European Commission 2023). Although these programs were a step forward, their combined €810 million budget was insufficient to fill Europe's actual capability gaps. EDIP (€1.5 billion, adopted at le end of 2025) consolidated both instruments and introduced security-of-supply measures, but remained a grant-based bridge to the 2028 Multi Annual Financial Framework cycle rather than a structural solution (Council of the EU 2025).

SAFE represents a qualitative break across all four dimensions in

Table 1: its scale exceeds all prior instruments combined by a factor of fifteen; its EU-bond financing mechanism creates supranational fiscal capacity for defense with no historical precedent; its conditionality (joint procurement by at least two member states, NDIP compliance, and a 35% non-EU component cap) is the most demanding of any EU defense instrument; and its governance architecture, anchored by a dedicated SAFE Special Group and quarterly reporting, constitutes a new institutional infrastructure for EU.

5. THE FISCAL ARCHITECTURE OF SAFE: DESIGN, MECHANISMS, AND CONDITIONALITIES

SAFE is financed through EU bonds issued on international capital markets, replicating the NextGenerationEU fund structure used during the COVID pandemic. Member states access financing at rates reflecting the EU's AAA/Aa1 credit rating rather than their own sovereign ratings. Early implementation data indicates a benchmark rate of approximately 1% per year for smaller member states,

Table 1: Comparative Overview of EU Defense Financing Instruments

Instru-ment	Year	Budget	Financing Mechanism	Procurement Conditionality	Governance Strength
PESCO	2017	None	None (coordination only)	Voluntary commitments	Weak — no sanctions
EDF	2021	€8.8 bn (2021–27)	EU budget grants	R&D collaboration (≥3 entities)	Moderate — work programs
ASAP	2023	€500 m	EU budget grants	Production capacity investment	Light — project-based
EDIRPA	2023	€310 m	EU budget grants	Joint procurement (≥3 MS)	Light — project-based
EDIP	2025	€1.5 bn (2025–27)	EU budget grants	Joint procurement + supply security	Moderate — NDIP alignment
SAFE	**2025**	**€150 bn**	**EU bonds (loans to MS)**	**Joint procurement (≥2 MS) + NDIP + 35% non-EU cap**	**Strong — Special Group + quarterly reporting**

(Source: Compiled by author from European Commission (2021; 2023; 2025), Council of the EU (2017; 2025), EDA (2023; 2025).

compared to sovereign borrowing costs of 3–5% for several eastern and southern members (European Commission, 2025).

The loans are long term, on a 45-year repayment horizon with a ten-year grace period on principal, and pre-financing of up to 15% of the total loan value is available upon NDIP submission. Unlike the previous financing mechanisms, SAFE's borrowing is off-budget, backed by the EU's general creditworthiness rather than a specific Multiannual Financial Framework line - a design choice that raises long-term fiscal governance questions.

Access to SAFE loans is conditional on three cumulative requirements. First, member states must submit a *National Defense Investment Plan (NDIP)* endorsed by the Commission, demonstrating alignment with EU capability priorities identified in the Capability Development Plan, the EDA's CARD, and the White Paper for European Defense Readiness 2030 - by January 2026, 24 NDIPs had been endorsed (European Commission, 2026). Second, procurement must involve at least two participating states - EU member states, Ukraine, EEA-EFTA countries, or acceding states (Article 8), creating a structural incentive for collaboration instead of fragmented acquisition. Third, components originating outside the EU, EEA-EFTA, and Ukraine must not exceed 35% of the estimated cost of the end product's components (Defense Finance Monitor 2026), a mandatory eligibility condition that functions as an industrial policy instrument to reinforce European supply chains.

SAFE supports procurement across two categories. *Category 1* covers the most urgent systems, such as ground-based air and missile defense, artillery and ammunition, armored vehicles, military mobility assets, naval vessels, and cyber and electronic warfare capabilities.

Category 2 covers strategic enablers, such as military aircraft, unmanned systems, space-based assets, and C3I infrastructure. For Category 2, design authority must reside in or transfer to an EU-based entity, which constitutes the strongest industrial sovereignty requirement of any EU defense instrument to date (Santopino, 2025). The allocation of the €150 billion envelope, with Category 1 receiving the larger share based on September 2025 expressions of interest, confirms that member states have prioritized near-term capability delivery over long-term industrial transformation.

The *SAFE Special Group,* composed of all member state representatives and chaired by the Commission, reviews NDIPs, monitors implementation, and coordinates loan allocation, with a quarterly reporting requirement that

creates an unprecedented rhythm of EU-level scrutiny of national defense resource allocation. There are also VAT exemptions for SAFE-financed procurement operations which reduce the effective cost of joint procurement relative to nationally financed alternatives and strengthens the financial incentive for the MS to participate (European Council, 2025).

6. FROM COORDINATION TO CAPABILITY: SAFE'S TRANSFORMATIVE IMPLICATIONS

A critical test of H1 is whether SAFE is generating genuinely joint procurement programs or merely providing EU-subsidized financing for parallel national acquisitions that nominally satisfy the two-member-state threshold. The early evidence is mixed but broadly encouraging.

As the Commission has not yet released a standardized cross-national implementation dashboard, the available evidence must be read cautiously. The analysis therefore relies on three observable proxies derived from endorsed NDIPs and official announcements: the composition of NDIP envelopes, the share of publicly identifiable projects that are genuinely joint, and early implementation signals such as endorsement timing and signed contracts.

Romania's Ministry of National Defense will implement 21 projects under SAFE, of which 10 are joint acquisitions with other countries and 11 are exclusively national. Most joint projects are being carried out with France and Germany, including a signed contract with France for Mistral missiles (worth €652 million, with six other states), 12 H225 helicopters from France, 12 radars in a joint purchase with France, and three air defense systems to complement the Patriot system in a program with Germany. (Romania Insider, 2026)

Poland's NDIP identifies joint procurement partnerships with Baltic States for artillery systems and air defense, with the Safe Baltic project - a dedicated €3.4 billion sub-program for Baltic Sea security - representing the most geographically coherent joint procurement initiative in the first two waves, linking Poland's SAFE engagement to a broader Baltic Sea security architecture. (Glowacki, 2026).

The NDIP data also reveals that 15 member states have declared joint procurement projects with Ukraine, underscoring SAFE's dual function as both a European rearmament instrument and a mechanism for integrating Ukraine into the EU defense industrial ecosystem (European Commission, 2026).

These are meaningful instances of cooperation. They are not, however,

evidence that the coordination–capability gap has been closed. The tension between national and European common interests persists, as the European Union is not a military alliance, and many countries are still using SAFE to support their national defense interests.

The political contestation surrounding SAFE's joint procurement conditionality is most visible in the proposal put forward by Polish President Nawrocki in March 2026, presented as "concrete, Polish, safe and sovereign," and as an alternative to what he described as "the financial and political constraints of the EU program" (President of the Republic of Poland 2026). Rather than borrowing from the EU at interest, Poland would finance its defense spending at zero cost through two potential mechanisms: a sell-buy-back operation on the National Bank of Poland's gold reserves to generate capital gains directed to the Armed Forces Support Fund, and/or a reallocation of the National Bank of Poland's annual profit earmarked specifically for defense (ING Think 2026).

The political appeal is real, but also are the constraints. The gold mechanism could generate the required funds one year later than the first potential disbursement from SAFE. Large-scale gold operations to finance public spending could be perceived by bond markets as quasi-monetary financing, potentially raising Poland's sovereign borrowing costs at a time when it is actively rebuilding its standing with international investors (ING Think 2026).

What makes the SAFE 0% proposal analytically significant is not whether it works or not, but what it reveals. It is the most concrete manifestation to date of the sovereignty dimension of H2: the moral hazard of loan-financed rearmament has already generated a credible domestic counter-proposal capable of decoupling Poland's defense financing from EU joint procurement conditionality. It brings to light a structural tension within the SAFE architecture, between the instrument's fiscal incentive logic - which assumes the interest rate differential is sufficient to overcome sovereignty concerns - and the political economy of member states where sovereigntist actors may use it to promote their own agendas.

6.1 Case Comparison: Poland and Romania as Contrasting SAFE Archetypes on the Eastern Flank

Poland and Romania offer an illustrative bilateral comparison within the SAFE framework. They are both NATO eastern flank states with elevated threat perceptions, both rank among the largest SAFE beneficiaries by allocation, and both have submitted NDIPs that reflect

genuine strategic ambition. They also differ substantially across dimensions relevant to SAFE's effectiveness: defense spending trajectory and fiscal capacity, industrial absorption capacity, the balance between acquisitions and infrastructure investment, and the degree of joint procurement integration.

The comparison is nonetheless limited by the asymmetric public disclosure across NDIPs, and the lack of data on execution rates, contracting pace, or full disbursement, so the analysis captures planned allocations and early implementation rather than completed delivery.

The two countries moved through the SAFE approval pipeline at different speeds. Romania was included in the first wave of endorsements on 11 February 2026, alongside Belgium, Bulgaria, Cyprus, Denmark, Spain, Croatia, and Portugal. Poland was approved in the second wave — a sequencing that reflects both Romania's earlier NDIP submission and a smoother domestic ratification process (Council of the EU 2026; Romania Insider 2026).

Poland is the largest single SAFE beneficiary, with an allocation of €43.7 billion — more than a quarter of the entire €150 billion envelope (Glowacki 2026). This reflects Poland's exceptional defense spending trajectory (4.7% of GDP in 2025, the highest in NATO) and its demonstrated capacity to absorb large-scale procurement programs. The Polish Government estimates that 89% of SAFE funds will flow to polish industry, with approximately 12,000 Polish companies participating in the supply chain (Chancellery of the Prime Minister 2026). This absorption capacity is the product of a decade of sustained investment progressively building Poland's defense technological and industrial base, including licensed production arrangements with South Korean and US prime contractors.

Poland's NDIP is unambiguously firepower-centric, reflecting a threat calculus shaped by the land warfare lessons of Ukraine. Artillery systems account for the largest single share (28%, approximately €12.2 billion), followed by air and missile defense and anti-drone systems (26%), ground combat and support systems (19%), and ammunition and missiles (14%). The remaining 13% covers strategic air transport, space resources, cybersecurity and AI, and the Safe Baltic maritime component. Some funding also flows to Poland's Police, Border Guard, and State Protection Service, as well as military mobility including roads and bridges (Glowacki 2026).

Romania is the second-largest SAFE beneficiary, with an allocation of €16.7 billion - a figure that significantly exceeds its annual defense budget of approximately €8.5 billion in 2025 (European

Commission 2026; Jipa 2025). The ratio between SAFE funds and the annual defense budget in the two countries is relevant: 1.9 for Romania compared to 0.99 for Poland. Romania does not have a mature defense industrial base capable of absorbing large-scale procurement within a compressed timeline. Despite political ambitions to become a defense provider in the Black Sea area and the advances made in the past 5 years, its defense industry remains characterized by limited production capacity, a history of procurement delays and litigation, and a relatively small pool of qualified defense contractors (Visan 2019; Wolf Theiss 2025).

Romania's NDIP reflects a fundamentally different threat calculus and a distinctive three-part allocation: €9.53 billion for defense modernization managed by the Ministry of Defence; €2.8 billion for equipment for the Ministry of Internal Affairs and civil protection; and €4.2 billion for strategic sections of the A7 and A8 motorways in the country's northeast, improving links toward Ukraine and Moldova (Romanian Ministry of National Defense 2025).

The infrastructure component is the most distinctive feature of Romania's NDIP and has no equivalent in Poland's plan. The specific corridors Pașcani–Suceava–Siret and Pașcani–Iași–Ungheni are simultaneously civilian economic assets and critical military mobility routes enabling rapid force projection along NATO's southeastern flank. By allocating 25% of its SAFE envelope to this dual-use infrastructure, Romania is leveraging the instrument's military mobility eligibility to address a structural deficit that prior national budgets could not close. It also means that Romania's actual defense acquisition budget under SAFE is €9.53 billion, not €16.7 billion - a distinction that matters when assessing the instrument's direct contribution to closing the coordination–capability gap.

Within the €9.53 billion military envelope, Romania's procurement priorities differ significantly from Poland's. While Poland's acquisitions focus on mass fires (28% on artillery alone), Romania's dominant priority is armored maneuver mass. The IFV replacement program alone accounts for €2.98 billion, making it the single largest line item in Romania's entire SAFE portfolio, due to the fact that Romania still operates approximately 142 Soviet-era MLI-84 infantry fighting vehicles - a deficiency Poland addressed in an earlier procurement cycle.

Ground forces modernization dominates at approximately 39% of the military envelope, covering 198 tracked IFVs (€2.98B), 139 Piranha 5 APCs (€761M), and over 1,370

logistics vehicles (€471M). *Air and missile defense* comes second at approximately 26%, with Mistral missiles, Skynex V-SHORAD batteries, IRIS-T SLM systems, and GM200 radars. *Aviation* (H225M Caracal helicopters), *naval capability* (offshore patrol vessels and Naval Strike Missiles, approximately 9%), and *C4ISR and digital systems* (approximately 5%) complete the portfolio (Romanian National Defense Ministry 2026).

What Romania is not buying through SAFE is equally relevant. There is no significant artillery allocation, despite the fact that the war in Ukraine has demonstrated that deep fires are the dominant currency of high-intensity land warfare. The explanation is that the K9 howitzer program is already under a separate 2024 contract with Hanwha Aerospace, being assembled in Romania, and Romania has separately acquired HIMARS and CAESAR howitzers through bilateral channels. There is no main battle tank, although Romania continues to depend on upgraded Soviet-era legacy platforms, but 216 modern MBTs are already approved under a separate program, including 458 million euros for a battalion of M1A2 SEPv3 Abrams tanks (Watkins 2025).

The OPV acquisition is the most debatable line item, as it can be argued that it has limited war-fighting value compared to what frigates or corvettes with anti-submarine and anti-ship capabilities would offer against Romania's actual Black Sea threat environment. Romania is separately procuring a light corvette (Vulcan 2025), but the overall naval surface picture remains insufficient for a country with significant Black Sea responsibilities. The C4ISR software platform appears significantly underfunded relative to the complexity of digitally networking a force of this scale, a lesson the Ukraine war has made impossible to ignore.

The overall assessment is that in Romania's case, SAFE is filling the capability gaps that prior national budgets could not close, in accordance with the instrument's design logic.

Romania's most significant programs also carry a condition of at least 50% domestic production, with some requiring 100% for sovereignty and security reasons (Romania Insider 2026). This combination of joint acquisition and domestic production requirements reflects Romania's ambition to embed itself in European defense supply chains while simultaneously building national industrial capacity - a more complex and potentially more fragile procurement strategy than Poland's predominantly domestic model.

The Poland–Romania comparison illustrates four structural

dynamics likely to determine SAFE's different effectiveness across member state typologies.

First, the relationship between industrial absorption capacity and SAFE effectiveness is non-linear. Poland's high absorption capacity means its €43.7 billion allocation is likely to generate genuine capability delivery within the 2025–2030 window, as the industrial infrastructure exists to convert financial commitments into deployed systems. Romania's constrained absorption capacity creates a risk that its €9.53 billion acquisition envelope will exceed the contracting and delivery capacity of its defense procurement system, potentially resulting in underspent allocations, delayed deliveries, or a concentration of contracts with a small number of foreign prime contractors.

Second, Romania's infrastructure investment reveals an important design feature of SAFE that Poland has not exploited at scale: the instrument's military mobility eligibility allows member states to use defense financing to address dual-use infrastructure gaps that would otherwise require separate civilian investment programs. The A7/A8 investment is simultaneously a military mobility asset, a NATO force projection enabler, and a civilian economic development project — a convergence that maximizes the strategic value of Romania's SAFE allocation but complicates the direct measurement of its contribution to the coordination–capability gap.

Third, the two NDIPs reflect contrasting strategic orientations.

Poland's plan is almost entirely firepower-centric, optimized for high-intensity land warfare on the northeastern flank. Romania's plan is more diversified, combining armored modernization, air defense, naval capability, infrastructure, and internal security and reflecting the multi-domain demands of the Black Sea strategic environment and Romania's ambition to become a regional defense provider rather than a purely defensive consumer.

Fourth, and most consequentially, the political economies of the two states are moving in opposite directions. Romania's SAFE engagement rests on broad domestic consensus. Poland's is contested — a president publicly proposing sovereign alternatives to EU financing, a government defending the instrument's value, and a domestic political debate that has moved SAFE from a technical instrument to a constitutional question about the boundaries of European integration. The fiscal architecture holds. The political architecture around it is under stress.

Table 2: Poland–Romania Comparative Profile under SAFE

Dimension	Poland	Romania
SAFE allocation	€43.7 bn (29% of total)	€16.7 bn (11% of total)
Defense spending (2025)	~4.7% GDP (~€48 bn)	~2.3% GDP (~€9.8 bn)
SAFE/annual defense budget ratio	~0.9x	~1.7x
Industrial absorption capacity	High (mature DTIB, 12,000 companies)	Constrained (limited base, history of delays)
NDIP structure	Predominantly acquisitions	58% acquisitions, 25% infrastructure, 17% internal security
Key procurement priorities	Artillery, air defense, ground systems, ammunition	IFVs, helicopters (joint FR), air defense, naval
Infrastructure component	Military mobility (roads, Safe Baltic)	A7/A8 motorways (northeast corridor to Ukraine/Moldova)
Joint procurement flagship	Safe Baltic; artillery with eastern flank partners	Caracal helicopters (France); Mistral/IRIS-T (multilateral)
Political economy	Contested (government vs. president)	Broad consensus
H1 evidence	Strong	Moderate
H2 risk profile	Moral hazard (debt burden, sovereignty)	Absorption capacity (e
Dimension	Poland	Romania
SAFE Allocation	€43.7 billion	€16.7 billion
Approval Batch	2nd (Feb 17, 2026)	1st (Feb 11, 2026)
Military Share	~98%	~75%
Infrastructure Share	~2% (Baltic/roads)	~25% (A7/A8 motorways)
Top Capability Priority	Artillery & air/missile defence	Air defence & ground modernisation
Joint Procurement	Limited	Extensive (10 of 21 programmes)
Key Partners	Primarily domestic	France, Germany
Political Context	Contested (presidential opposition)	Broadly supportive
Domestic Industry Target	89%	50–100% per programme

(Source: Compiled by author from European Commission data)

7. CRITICAL ASSESSMENT: LIMITATIONS, RISKS

The preceding section supports H1 only in a qualified sense: SAFE is producing a measurable shift in procurement planning toward jointly structured, EU-conditioned programs, but the evidence still concerns endorsed plans and early contracts rather than audited execution rates. That is nonetheless analytically significant, because previous EU instruments rarely structured national acquisition plans at this scale. The evidence on H2 is more complex, as the structural tensions previously identified are now visible in the first year of implementation.

The two-speed Europe risk is the most immediate, as high absorption capacity states (Belgium, Denmark, Poland) are converting their SAFE allocations into deployed capabilities. Lower absorption capacity states (Romania, Bulgaria, Croatia) are accumulating financial commitments that their procurement systems may not execute within the 2025–2030 window.

The risk is not merely delayed capability delivery, considering that if lower-absorption member states consistently underspend their allocations, the political legitimacy of SAFE as an instrument of collective capability development will be undermined and its successor will face a more skeptical political environment.

The Commission's NDIP endorsement process provides partial mitigation: by requiring member states to demonstrate alignment with EU capability priorities before accessing pre-financing, it creates a planning discipline that may improve execution rates relative to purely national procurement cycles. This conditionality does not address the underlying structural constraints, such as limited contracting capacity, shallow defense industrial bases, procurement agency staffing deficits, that produce absorption failures in the first place. A more robust mitigation would require the Commission to provide technical assistance to lower-absorption member states, analogous to the REFORM support instrument deployed under NextGenerationEU, but no such mechanism is currently embedded in the SAFE Regulation (Council Regulation (EU) 2025/1106).

The moral hazard operates at two levels: at the first level, SAFE loans are sovereign obligations that will appear on national balance sheets and must be repaid over a 45-year horizon. For member states already carrying elevated debt-to-GDP ratios, the addition of SAFE obligations, even at concessional interest rates, creates a long-term fiscal commitment that constrains future defense budget flexibility and will generate political resistance as the repayment phase begins after

2030. The Polish SAFE 0% episode, previously analyzed and the political logic it embodies, that sovereign debt-free defense financing is preferable to concessional EU loans with procurement strings attached, is the clearest early manifestation of this tension.

At the second level, SAFE's concessional interest rates reduce the effective cost of defense investment below market rate, creating an incentive for member states to over-allocate to defense relative to their genuine strategic requirements. The NDIP conditionality provides a partial check, but it does not prevent member states from submitting ambitious NDIPs that exceed their realistic absorption capacity in order to maximize their SAFE allocation.

The 35% non-EU component cap is the most politically contested structural tension. The cap was designed to reinforce European defense supply chains and reduce third-country dependencies, a legitimate industrial policy objective in the current geopolitical context. It also creates three categories of practical difficulty that the first year of implementation has already made visible.

First, the cap creates a direct conflict with existing procurement commitments. Poland's largest defense procurement programs — the K2 Black Panther main battle tank and the FA-50 light combat aircraft (both from South Korea) and the HIMARS multiple launch rocket system (from the United States), involve component shares that may exceed the 35% non-EU threshold, potentially rendering them ineligible for SAFE financing without renegotiation of supply chain arrangements (Reuters 2025). Member states that have invested in transatlantic and Indo-Pacific defense industrial partnerships are penalized relative to those that have not.

NATO's Updated Defence Production Action Plan explicitly links industrial expansion, multinational demand aggregation, and materiel standardization to Alliance capability targets, while recent EU–NATO literature stresses that stronger EU initiatives should reinforce interoperability and avoid duplication rather than create parallel standards (NATO 2025; European Parliament 2025). Several of the most capable and NATO-standardized systems in the European defence market, such as US-origin air defence systems, precision munitions, and C4ISR infrastructure, contain component shares that approach or exceed the 35% threshold. Substituting European components may be a long-term solution, but in the short term it risks degrading interoperability with US and Canadian NATO allies.

Third, the cap's enforcement mechanism creates a compliance

burden asymmetrically distributed: larger member states with sophisticated procurement agencies navigate the review process efficiently; smaller member states with limited administrative capacity face a disproportionate compliance cost. The Regulation provides no waiver mechanism for cases where no European alternative to a non-EU component exists at the required capability level, scale, or timeline — leaving member states in a legal grey zone that deters participation in otherwise eligible programs.

8. POLICY RECOMMENDATIONS

The previous analysis generates a set of actionable recommendations directed at the four principal actors whose decisions will determine SAFE's long-term effectiveness.

Defense ministries in member states with constrained absorption capacity should take the opportunity to consider SAFE implementation as a defense resource management reform program, not merely a procurement exercise. The primary bottleneck is not financial but institutional: contracting capacity, project management expertise, and qualified defense acquisition workforce. Ministries should use the pre-financing window — up to 15% of the SAFE allocation available on NDIP endorsement — to invest in procurement agency capacity before committing to large-scale acquisition contracts. Engaging national audit institutions and parliamentary defense committees in NDIP oversight from the outset will reduce the risk of political backlash during the repayment phase.

Defense ministries in member states with high absorption capacity should ensure that the ambitious stimulus to the domestic industrial base does not become a barrier to genuine joint procurement. The SAFE conditionality requires at least two participating states; the spirit of the instrument demands durable industrial cooperation, not merely contractual co-signatures. Joint procurement agreements should include technology transfer, co-production, and maintenance arrangements that create lasting supply chain interdependencies.

The European Commission should introduce a technical assistance mechanism, similar to the REFORM support instrument under NextGenerationEU, specifically designed to strengthen defense procurement capacity in lower-absorption member states. The 35% non-EU component cap requires a formal waiver procedure for cases where no European alternative exists at the required capability level, scale, or timeline. The absence of such a procedure creates legal uncertainty that deters participation and penalizes legitimate transatlantic procurement

commitments. A waiver procedure, subject to Commission approval and SAFE Special Group endorsement, would preserve the instrument's industrial policy objectives while eliminating the perverse incentive. Quarterly SAFE implementation dashboards, covering NDIP execution rates, joint procurement participation ratios, and 35% cap compliance data for each participating member state, would create accountability pressure and provide the evidence base that research and policy communities need to evaluate SAFE's effectiveness in real time.

European defense prime contractors and system integrators should treat SAFE not merely as a demand stimulus but as a structural opportunity to consolidate fragmented European supply chains. The NDIP data reveals a convergence of national procurement priorities (particularly in ground-based air defense, artillery, and armored vehicles) that creates the conditions for multi-country framework contracts at a scale justifying new production capacity investment. Primes that position themselves as SAFE-compliant supply chain integrators, demonstrating 35% cap compliance across their product lines and offering co-production arrangements to member state partners, will have a structural advantage in the competition for NDIP-linked contracts. For small and medium-sized defense enterprises, the SAFE framework creates both opportunity and risk. Industry associations should engage with the SAFE Special Group to advocate for SME-friendly contract structures in the NDIP implementation guidelines.

NATO should formalize a consultation channel linking SAFE NDIPs to the NATO Defense Planning Process and NATO standardization processes. Treating endorsed NDIPs as complementary planning inputs would help align SAFE-financed investments with Alliance capability targets, identify interoperability problems early, and manage conflicts between the 35% non-EU cap and operational requirements before they translate into procurement bottlenecks. Such a mechanism would also help ensure that EU support for Ukraine's defence industry complements long-term NATO force-generation and standardization goals rather than evolving on a parallel track.

9. CONCLUSIONS

This paper set out to analyze the Security Action for Europe as a paradigm shift which shifts the operative logic of European defense cooperation from voluntary coordination to fiscally incentivized capability delivery.

H1, the Fiscal Architecture Hypothesis, is broadly supported. SAFE's loan-based mechanism,

combined with the NDIP conditionality and the joint procurement requirement, is producing a visible change in member state procurement behavior. The institutional genealogy traced in Section 4 demonstrates that this shift is the culmination of a decade-long escalation in EU defense financing ambition, with each instrument responding to the demonstrated inadequacies of its predecessor. The NDIP data from the first two endorsement waves confirms that member states are channeling significant shares of their SAFE allocations into jointly structured programs. The instrument's fiscal architecture has successfully lowered the financial barrier to joint procurement participation.

H2, the Structural Tension Hypothesis, is also supported. The structural tensions identified in Section 7 are not design flaws correctable by regulatory amendment. They are inherent features of an instrument that attempts simultaneously to achieve fiscal scale, industrial policy objectives, and sovereignty-respecting conditionality. The two-speed Europe risk reflects the structural diversity of EU member states' defense industrial bases — a diversity that SAFE's uniform conditionality framework cannot eliminate. The moral hazard of loan-financed rearmament reflects the fundamental tension between the EU's collective credit advantage and the national sovereignty of the member states that must ultimately service the debt. The industrial protectionism embedded in the 35% non-EU cap reflects the unresolved conflict between the EU's strategic autonomy objectives and its alliance commitments — a conflict that SAFE has made more visible but has not resolved.

The paper's central analytical contribution is the concept of the ***coordination–capability gap*** and its operationalization through the lens of fiscal architecture. By framing SAFE as a fiscal architecture rather than merely a procurement instrument, the analysis reveals that the instrument's effectiveness depends not only on the scale of financing it mobilizes but on the institutional infrastructure that converts financial commitments into deployed capabilities. Fiscal architecture can close the coordination–capability gap by aligning incentives and aggregating demand. It cannot substitute for the industrial capacity, procurement expertise, and political consensus that capability delivery ultimately requires.

The Poland–Romania case comparison illustrates these dynamics. Poland demonstrates that high absorption capacity and strong domestic industrial routing can convert a large SAFE allocation into genuine capability delivery

within the implementation window — at the cost of a domestic political contestation that has already produced a credible sovereignty-based counter-proposal. Romania demonstrates that strategic ambition and a diversified NDIP combining acquisitions, joint procurement, and dual-use infrastructure can maximize the strategic value of a SAFE allocation, on the condition the underlying procurement system can execute the plan within the timeline the instrument imposes.

Three open questions define the directions for future research: first, whether SAFE's joint procurement conditionality will generate durable industrial cooperation or merely transient contractual arrangements; second, whether the instrument's off-budget financing structure will survive the EU's reformed economic governance framework; third, whether SAFE will be renewed, expanded, or succeeded by a permanent EU defense financing instrument after 2030.

SAFE represents the most ambitious and structurally coherent attempt yet to close the coordination–capability gap in European defense. Whether it succeeds will depend less on the quality of its fiscal architecture, which is sound, than on the political will of member states to honor their NDIP commitments, the capacity of their procurement systems to execute them, and the resilience of the EU's collective defense financing consensus in the face of the sovereignty pressures that loan-financed rearmament inevitably generates. The architecture is built. The question is whether the people inside it will hold it up.

AI DISCLOSURE

The author acknowledge the use of the following generative AI tools to assist in the preparation of this manuscript: OpenAI. This tool was used solely for language editing and structural suggestions, under the complete control and responsibility of the authors. All AI-assisted content was critically reviewed and revised by the authors, who accept full responsibility for the accuracy and integrity of the final version.

REFERENCES

[1] European Parliamentary Research Service. *ReArm Europe Plan/ Readiness 2030*. Brussels: European Parliament, 2025. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769566/EPRS_BRI(2025)769566_EN.pdf.

[2] Council of the European Union. "SAFE: Council Adopts €150 Billion Boost for Joint Procurement on European Security and Defence." Press release, May 27, 2025. https://www.consilium.europa.eu/en/press/press-releases/2025/05/27/safe-council-adopts-150-billion-boost-for-joint-procurement-on-european-security-and-defence/.

[3] Fiott, D. (2025) "The Three Images of EU Strategic Autonomy: Perspectives on Wedging, Binding and Hedging." *Journal of European Integration* 47: 825–42. https://doi.org/10.1080/07036337.2025.2537369.

[4] Zandee, D. et al. (2020), "European Strategic Autonomy in Security and Defence", *Clingendael Report,* https://www.clingendael.org/sites/default/files/2020-12/Report_European_Strategic_Autonomy_December_2020.pdf

[5] Mueller, T. (2025): "Strategic Options for the European Defence Industry in the 2020s." *Defense & Security Analysis* 41, no. 1, 49–80. https://doi.org/10.1080/14751798.2024.2418163.

[6] Hartley, K. (2011) "Defining the 'European Defence Technological and Industrial Base': Debates & Dilemmas." https://www.files.ethz.ch/isn/168010/201323.pdf.

[7]Musgrave, R., (1959), *The Theory of Public Finance*, McGraw-Hill

[8] Oates, W. (1972), *Fiscal Federalism,* Harcourt Brace Jovanovich, New York.

[9] Olson, M., Zeckhauser, R., (1966) "An Economic Theory of Alliances", *Review of Economics and Statistics* 48(3), 66-279. https://www.rand.org/content/dam/rand/pubs/research_memoranda/2007/RM4297.pdf

[10] Sandler, T., Hartley, K. (1999) *The Political Economy of NATO*. Cambridge University Press.

[11] Bénassy-Quéré, A, et al. (2021) "NextGenerationEU: A Brief Anatomy of Europe's New Fiscal Instrument." *Intereconomics* 56, no. 6.

[12] Centrone, M. and Meenakshi, F. (2024) "Improving the Quality of European Defence Spending: Cost of Non-Europe", *EPRS Report*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2024)762855

[13] European Defence Agency. *Defence Data 2024–2025*. Brussels: European Defence Agency, 2025.

[14] Council of the European Union. "Permanent Structured Cooperation (PESCO)." Accessed March 17, 2026. https://www.consilium.europa.eu/en/policies/pesco/.

[15] Council of the European Union. "EU Defence Funding." Accessed March 17, 2026. https://www.consilium.europa.eu/en/policies/defence-funding/.

[16] European Commission. "European Defence Fund: Over €1 Billion to Drive Next-Generation Defence Technologies and Innovation." January 30, 2025. https://defence-industry-space.ec.europa.eu/european-defence-fund-over-eu1-billion-drive-next-generation-defence-technologies-and-innovation-2025-01-30_en.

[17] European Commission. "Security Action for Europe (SAFE)." Accessed March 17, 2026. https://commission.europa.eu/strategy-and-policy/eu-budget/eu-borrower-investor-relations/safe_en.

[18] "EDIP Third-Country Control Derogations: Procedural and Legal Framework." *Defense Financial Monitor*, 2026. https://www.defencefinancemonitor.com/p/edip-third-country-control-derogations.

[19] Santopino, F. (2025) "*The Involvement of Third-Country Entities in EU Defence Industrial Policies and the "European Design Authority" Concept*".

ARES 114 Policy Paper. Institute for International and Strategic Affairs (IRIS). https://www.iris-france.org/wp-content/uploads/2025/06/ARES_2025_06_114_Design_Authority_PolicyPaper.pdf

[20] Council of the European Union. "SAFE: Council Adopts €150 Billion Boost for Joint Procurement on European Security and Defence." Press release, May 27, 2025. https://www.consilium.europa.eu/en/press/press-releases/2025/05/27/safe-council-adopts-150-billion-boost-for-joint-procurement-on-european-security-and-defence/.

[21] "Romania Publishes Procurement List for EUR 16 Bln Borrowed Under SAFE Instrument." *Romania Insider*, January 2026. https://www.romania-insider.com/romania-procurement-list-safe-jan-2026.

[22] Glowacki, B. (2025) "Poland Unveils Detailed Defense Spending for $51B in EU SAFE Loans". https://breakingdefense.com/author/bartosz-glowacki/

[23] President of the Republic of Poland. "President Puts Forward the Proposal of a 'Polish SAFE Zero'." 2026. https://www.president.pl/news/president-puts-forward-the-proposal-of-a-polish-safe-zero,116268.

[24] ING Think. "Does Poland Need a Domestic Alternative to the SAFE Programme?" 2026. https://think.ing.com/articles/does-poland-need-a-domestic-alternative-to-the-safe-programme/.

[25] Chancellery of the Prime Minister of the Republic of Poland. "SAFE: Poland's Blueprint for European Security and Domestic Defence Growth." 2026. https://www.gov.pl/web/primeminister/safe-polands-blueprint-for-european-security-and-domestic-defence-growth.

[26] Jipa, F. (2025) "MApN primeşte în 2025 un buget de 42,8 miliarde lei (8,5 miliarde euro), la care se adaugă credite de angajament, putând ajunge la 5,6% din PIB." *Monitorul Apararii si Securitatii*. https://monitorulapararii.ro/mapn-primeste-in-2025-un-buget-de-42-8-miliarde-lei-8-5-miliarde-euro-la-care-se-adauga-credite-de-angajament-putand-ajunge-la-5-6-din-pib-1-57560#:~:text=MApN%20primeşte%20%C3%AEn%202025%20un%20buget%20de%2042%2C8%20miliarde%20lei%20(8%2C5%20miliarde%20%5B&text=%5D%20Monitorul%20Ap%C4%83r-%C4%83rii%20%C8%99i%20Securit%C4%83%C8%9Bii.

[27] Visan, G. (2019) "Romania's Military Procurement Hits Multiple Roadblocks." *Eurasia Daily Monitor* Jamestown Report 16, no. 119 (2019). https://jamestown.org/edm-volume/title-365/.

[28] "Military procurement and the strategy for Romania's defence industry",*Wolf Theiss Report*, 2025, https://www.wolftheiss.com/insights/military-procurement-and-the-strategy-for-romanias-defence-industry/

[29] Ministry of National Defence of Romania. "Strategic Investments in Defence: Romania Accesses European Funds Through SAFE Mechanism." 2025. https://english.mapn.ro/cpresa/6574_Strategic-investments-in-defence:-Romania-accesses-European-Funds-through-SAFE-Mechanism.

[30] Ministry of National Defence

of Romania. "Programul SAFE." 2026. https://www.mapn.ro/programul_safe/index.php.

[31] Watkins, R. (2025), "Romania Advances Plan to Acquire 216 Main Battle Tanks", *The Defense Post*, https://thedefensepost.com/2025/10/03/romania-abrams-tank-acquisition/

[32] Vulcan, D. (2025), "Aviz în comisiile Parlamentului pentru achiziția unei corvete de 223 de milioane de euro. Ministrul Moșteanu: Armata Română are mare nevoie", *Europe Libera Romania*, https://romania.europalibera.org/a/aviz-in-comisiile-parlamentului-pentru-achizitia-unei-corvete-de-223-de-milioane-de-euro-/33525000.html

[33] Reuters. "Explainer: Can Non-EU Companies Be Part of EU's Big Defence Fund?" *Reuters*, March 21, 2025. https://www.reuters.com/world/europe/can-non-eu-companies-be-part-eus-big-defence-fund-2025-03-21/.

[34] European Commission. "SAFE Security Action for Europe." Accessed March 17, 2026. https://defence-industry-space.ec.europa.eu/eu-defence-industry/safe-security-action-europe_en.

[35] Cepparulo, A. and Reitano, V. E. (2025) "An Assessment of the Euro Area Fiscal Stance in 2025 and 2026, Considering the Flexibility for Higher Defence Spending", European Economy Economic Brief 85, July.

[36] European Central Bank (2025) "Fiscal Aspects of European Defence Spending: Implications for Euro Area Macroeconomic Projections and Associated Risks", ECB Economic Bulletin, Issue 5/2025.

[37] Moretti, E., Steinwender, C. and Van Reenen, J. (2025) "The Intellectual Spoils of War? Defence R&D, Productivity, and International Spillovers", Review of Economics and Statistics 107(1): 14–27.

[38]Genini,D.(2025)"Restructuring the EU's Defence Industrial Base amid Geopolitical Shifts", Common Market Law Review 62. https://doi.org/10.1177/1023263X251394132.

[39] Arnal, J., Riesgo, J. P., Niño, I., and Escobar, C. (2026) The Day After NextGenerationEU: What Could the EU Do? Journal of Common Market Studies 64(3): 1256–1271. https://doi.org/10.1111/jcms.70034.

[40] European Central Bank. "Time to Be Strategic: How Public Money Could Power Europe's Green, Digital and Defence Transitions." ECB Blog, 25 July 2025. https://www.ecb.europa.eu/press/blog/date/2025/html/ecb.blog20250725~f26b4ef0f3.en.html.

[41] Besch, S. (2025) EU Defence Industrial Policy in a New Era: Taking Stock and Looking Ahead. Heinrich-Böll-Stiftung European Union. https://eu.boell.org/sites/default/files/2025-03/hbs-eu-defence-industrial-policy-sophia-besch-final.pdf.

[42] NATO. Updated Defence Production Action Plan. Brussels: NATO, 13 February 2025. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/updated-defence-production-action-plan.

[43] European Parliamentary Research Service. EU–NATO Cooperation. Brussels: European Parliament, 2025. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772922/EPRS_BRI(2025)772922_EN.pdf.

OPERATIONS MANAGEMENT ANALYSIS FOR OPTIMIZATION OF SMITH & WESSON 17 PISTOL PRODUCTION

E.S. ALIM[1] , I NENGAH PUTRA[2], G.R. DEKSINO[3], K. GUNAWAN[4], A.K. SUSILO[5]

[1]Indonesia Defense University, Bogor, 16810 Indonesia
[2]Indonesia Defense University, Bogor, 16810 Indonesia
[3]Indonesia Defense University, Bogor, 16810 Indonesia
[4]Jakarta State University, Jakarta, 13220 Indonesia
[5]Indonesia Naval Technology College, Surabaya, 60178 Indonesia

This study aims to analyze operations management strategies that include production lot selection, safety stock and reorder point calculations, production sequencing, and material requirements planning in the production of the Smith & Wesson 17 Pistol. Data were processed using quantitative methods based on EOQ theory, safety stock management, the Critical Ratio, and Material Requirement Planning (MRP). The results show that a production lot of 40 units yields the lowest annual inventory cycle cost, with an optimal safety stock of 6 units and a reorder point of 38 units. A safety stock of 6 units and a reorder point of 38 units were calculated, considering a 90% cycle service level and a 4-week lead time. The priority order is A → B → C → E → D, with task A having the highest priority because it has the lowest CR. In Problem D, a leveling process is used to even out the workload in production, particularly for components such as Frames, Magazines, and Complete Triggers. In Problem E, Netting, Lotting, and Offsetting calculations are performed to ensure the availability of raw materials and components according to production needs. Production sequencing based on Critical Ratio and MRP tables ensures efficient production schedules and supply chain sustainability.

Key words: *Operations Management, Safety Stock, Reorder Point, Critical Ratio, Material Requirement Planning.*

[1] ORCID ID: 0000-0002-4436-6982, e-mail: ekasalim@gmail.com
[2] ORCID ID: 0000-0002-6799-691X, e-mail: nengahputra35@gmail.com
[3] ORCID ID: 0000-0002-7991-5283, e-mail: georgeroykedeksino@gmail.com
[4] ORCID ID: 0000-0002-4124-9334, e-mail: kazangunawan@yahoo.com
[5] ORCID ID: 0000-0002-7012-7520, e-mail: aprilkukuh53@gmail.com

1.INTRODUCTION

The rapid development of industry has created increasingly fierce competition worldwide (Tri, Hoang, and Dung 2021). PT. SWX is one company facing this challenge (Costanzo and Spotts 2015). As part of Smith & Wesson International (Matoso et al. 2014), this company plays a strategic role in providing the primary weapons systems (alutsista) needed by the Indonesian National Armed Forces (TNI). Located in Batam, this company is expected to be the spearhead in supporting the independence of the national defense industry. However, this task is not easy because it involves complex management across various aspects, from production to distribution.

One of the biggest challenges facing PT. SWX is ensuring efficient production. This involves various strategic decisions, such as selecting the optimal production lot size, implementing effective inventory management, and structuring production planning (Silver, Pyke, and Thomas 2016). Furthermore, inventory management is crucial, especially when dealing with fluctuating demand (Mohamed 2024). In the defense industry, product requirements can fluctuate depending on military operational needs. Therefore, companies need to maintain a certain level of inventory, known as safety stock, to anticipate unexpected demand (Siraj et al. 2024). Mistakes in determining safety stock or reorder points can lead to significant losses, both due to stock shortages and excessive storage costs.

Another challenge is effective production planning. PT. SWX, which produces modular products like the Smith & Wesson 17 pistol, requires a well-organized production system. By using approaches such as the Critical Ratio for production sequencing, the company can appropriately prioritize work and ensure all components are available on schedule. This planning also involves netting, lotting, and offsetting processes to ensure a smooth material supply and support the overall assembly process.

In facing these challenges, innovation and technology are key factors. By utilizing data-driven systems such as Enterprise Resource Planning (ERP) (Costanzo and Spotts 2015), PT. SWX can integrate all operational processes, from raw material management to final product delivery. This step not only increases efficiency but also provides greater flexibility in adapting to dynamic market needs. This research aims to provide strategic solutions for the company's operations management to enable continued growth and support the grand vision of the national defense industry.

The urgency of this research arises from PT. SWX's increasingly strategic position within the national defense industry ecosystem, where operational inefficiencies can directly impact defense readiness, supply continuity, and national independence. Without a well-structured operational system, PT. SWX risks experiencing decreased competitiveness, delayed production cycles, and dependence on external suppliers, all of which can weaken the overall national defense posture. Furthermore, there is a need to formulate concrete and applicable strategies that enable PT. SWX to optimize its operational processes while aligning the company's performance with national defense objectives. This study is motivated by a broader vision to strengthen the domestic defense industry as a pillar of national sovereignty, where companies like PT. SWX play a dual role: achieving sustainable business growth and serving as a strategic asset for national defense independence and long-term security.

This research is supported by the Economic Order Quantity (EOQ), Safety Stock and Reorder Point, Material Requirement Planning (MRP) theoretical approach. This research is also supported by descriptive quantitative methods. This quantitative model ensures that decisions are based on measurable and accountable analysis. This research was conducted at PT. SWX, located in Indonesia, with data collection aimed at determining optimal solutions based on existing numerical data, such as inventory costs, order quantities, and production time.

This research has several contributions. First, it contributes to the development of operations management theory by contextualizing it within the defense industry, which has unique characteristics such as high reliability requirements, strict regulatory controls, and strategic national interests. Second, it theoretically bridges the gap between firm-level competitiveness and macro-level national defense readiness. Third, the findings offer practical insights for reducing dependence on foreign suppliers by strengthening internal operational capabilities and integrating the local supply chain. Fourth, it provides practical value to defense industry policymakers and regulators by highlighting critical operational factors that influence defense readiness. Fifth, this studies vary in their objectives and scope in assessing and measuring the sustainability of systems based on actual statistical distributions. Thus, it is possible to use statistical or stochastic models in their structure and, as will be presented, to implement optimization and probability calculations.

2. LITERATURE REVIEW

2.1. Operational Management

Operational management is a series of activities that generate value in the form of goods and services by processing inputs into outputs. Inputs are everything needed to initiate the production process, such as raw materials, auxiliary materials, labor, machinery, energy, information, methods, capital, space, and management. Outputs are the outcomes or results of the production process, in the form of goods or services. Simply put, operational management is defined as the activity of managing management resources by converting inputs into outputs in order to increase the utility value of goods effectively and efficiently (Mustofa and Waluyowati 2024).

2.2. Economic Order Quantity (EOQ).

Economic Order Quantity (EOQ) is one of the most widely used concepts in inventory management and logistics. EOQ was first introduced by Ford W. Harris in 1913 and has since become a fundamental decision-making model for inventory management (Rabta 2020). The multi-item EOQ model can be used for a wide range of commodities in retail stores. The computation of safety stock, reorder points, and maximum capacity is another way to support inventory control, helping keep costs even lower than the EOQ model (Mubasysyir, Supian, and Hertini 2024).

The EOQ model assumes a balance between two main components of inventory costs (Setyadi, Al Amin, and Widodo 2024):

a. Ordering Cost: Fixed costs incurred each time a company places an order, such as administrative costs, transportation, and communication. The more frequently a company orders small quantities, the higher the total ordering cost.

b. Holding Cost: Costs associated with storing goods in the warehouse, including space, insurance, damage, and depreciation. These costs increase with the quantity of goods stored.

EOQ provides an optimal solution by mitigating the conflict between high ordering costs (from low order frequency) and high holding costs (from large order quantities).

The basic EOQ formula is as follows:

$$EOQ = \sqrt{\frac{2DS}{H}}$$

Description:

- Annual demand (units per year).
- Ordering cost per order.
- Annual holding cost per unit.

EOQ is very useful in various industries, such as manufacturing, retail, and pharmaceuticals (Poornima et al. 2024). In manufacturing, for example, EOQ is used to ensure raw materials are always available without incurring excess holding costs (Sutejo, Suprayitno, and Latunreng 2023). In the retail sector, this model helps determine the quantity of merchandise to order to maintain optimal stock rotation. However, the successful implementation of EOQ is highly dependent on accurate data, such as demand for goods and operational costs, so companies need to ensure proper data collection (Kurniawan et al. 2024).

2.3.Safety Stock and Reorder Point

Safety stock and reorder points are two crucial elements in inventory management that serve to ensure smooth operations, particularly in the face of uncertain demand and delivery times (Mubasysyir, Supian, and Hertini 2024). Safety stock is additional inventory that serves as a buffer to absorb demand imbalances. Safety stock is useful for overcoming delays in the arrival of raw materials when frequent orders arrive late beyond the lead time (for example, delayed in transit due to floods, bridge collapses, pirates, or other disasters). Safety stock aims to minimize stockouts and reduce additional storage costs and total stockout costs. Storage costs here will increase with the addition of reorder points, driven by safety stock. The advantage of having safety stock is that when demand spikes, it can be used to cover the increase (Mustofa and Waluyowati 2024).

Safety stock is an additional reserve of stock held to anticipate fluctuations in demand fluctuations in delivery delays (Setiawan 2024). The average value and variability of replenishment lead times are two things that affect how much safety stock is needed. They thought that the random lead times followed Weibull distributions. This enabled the creation of analytical expressions that reduced the expected value and variability of overall demand until the first significant delivery from a vendor. The study formulates an expression for the reorder point that guarantees a specified probability of avoiding a stockout prior to the initial delivery, while establishing lower limits on the order size to ensure that the likelihood of a stockout before subsequent deliveries (second, third, etc.) remains minimal (Demiray Kırmızı, Ceylan, and Bulkan 2024). Mathematically, safety stock can be calculated using the formula:

$$Safety\ Stock = z.\sigma$$

Where :

z: Z-score based on desired service level

σ : Standard deviation of demand or lead time.

The reorder point, on the other hand, is the minimum stock level that indicates when a company should reorder to avoid stockouts. The reorder point is calculated based on the average demand rate during the reorder period (lead time) and safety stock. A reorder point is the inventory level that triggers a reorder, taking into account the lead time between when the order is placed and when it is received. Several factors determine the reorder point, including inventory during the delivery period and the desired level of security, material usage during the lead time for receiving the goods, and the amount of safety stock (Putri, Mutiara, and Erni 2025).

Based on the opinions of the two experts above, the factors that influence the reorder point are lead time, the time required between the goods being ordered and their arrival at the company, the level of goods orders per unit of time, and safety stock, the minimum amount of inventory a company must have to guard against the possibility of delays in the arrival of raw materials (Mubasysyir, Supian, and Hertini 2024).

The mathematical formula is:

$$Reorder\ Point = (Demand\ Rate\ x\ Lead\ Time) + Safety\ Stock$$

Where:

- Demand Rate: Average demand per period (e.g., per week).
- Lead Time: The time required to receive goods after an order is placed (in weeks, days, or months).
- Safety stock provides a buffer to address demand fluctuations or delivery delays, while the reorder point ensures the company reorders goods at the right time.

Safety stock and the reorder point work together to maintain inventory availability in the warehouse without experiencing stockouts or excessive buildup (Best et al. 2022). In its implementation, companies need to rely on accurate demand data and consider variability in lead times to ensure this calculation remains relevant and effective.

2.4. Critical Ratio (CR)

Critical Ratio (CR) is a method in production sequencing used to prioritize tasks based on their urgency (Gao, Wang, and Pedrycz 2020). This method helps companies manage processing time and due dates more efficiently (Kim, Kim, and Cho 2020). The Critical Ratio is often applied in the context of operations management, particularly in manufacturing environments and on projects with many tasks and tight schedules.

Mathematically, Critical Ratio is calculated using the formula:

$$CR = \frac{Due\ Date - Current\ Time}{Processing\ Time}$$

Where:

- Due Date: The due date of the task.
- Current Time: The current time in the production schedule.
- Processing Time: The time required to complete the task.

Critical Ratio Interpretation

- CR < 1: he task has high priority because the remaining time is less than the time required to complete it. If not started immediately, the task is at risk of missing its deadline.
- CR = 1: he task must be started immediately to be completed on time.
- CR > 1: The task has more remaining time than processing time, so it has lower priority than other tasks with a smaller CR.

2.5. Material Requirement Planning (MRP)

Material Requirement Planning (MRP) is a system used to manage and plan the need for raw materials and components in the production process. MRP was first developed in the 1960s as a solution to inefficient inventory management and procurement in manufacturing environments (Pramono 2024). This system is designed to ensure that the necessary raw materials are available at the right time and in the right quantities, thereby optimizing the production process and reducing inventory costs.

MRP is a system for planning and controlling inventory that depends on demand and schedules the proper amount. The MRP system can tell you how many raw materials you will need to make a product in the future. The MRP's job is to manage inventory levels, figure out which processes are most important for each item, and plan the production system's capacity (Omair, Stingl, and Wæhrens 2025)the RP available in the market shows high variation in quality, composition, and properties, and often experiences higher variability in lead time. This renders the supply chain of RP and the production systems more vulnerable, making it difficult for material requirement planning (MRP. This includes ordering things in the right amount and at the right time. In the meantime, MRP's main goal is to get the appropriate raw materials to the right place at the right time in order to make customers happier (Cipta, Aprilia, and Kurniawan 2023).

The primary purpose of MRP is to efficiently control and plan the flow of materials in the production process (Saptadi et al. 2023). MRP enables companies to calculate precisely how much material is needed, when it is needed, and when to place orders to meet production

needs (Fole et al. 2024). This system aims to reduce inventory buildup, prevent stockouts, and improve the efficiency of storage space and company fund management.

MRP is a popular way for businesses to plan and optimize their procurement of raw materials. It helps them make decisions about things like reordering and capacity planning. MRP has been a key instrument for boosting productivity and gaining a competitive edge in the global economy. It is also very crucial for managing inventory while making complicated industrial items. Most enterprise resource planning (ERP) systems now include MRP as a key aspect. As a result, it is stored in the ERP database (supply, demand, capacity, planned reception, etc.) and runs regularly (daily or weekly) depending on the type of problem (Omair, Stingl, and Wæhrens 2025).

MRP relies on three main components in material planning (Ivanov, Tsipoulanidis, and Schönberger 2021):

a. Bill of Materials (BOM): A list detailing all raw materials and components required to produce a final product. The BOM describes the relationship between a product and its components.
b. Master Production Schedule (MPS): A master production schedule that shows how many products will be produced in a given time period, based on the demand or orders received.
c. Inventory Records: Records that include the amount of stock available, the quantity ordered, and the delivery time for each raw material and component.

3. METHODOLOGY

The research in this study is quantitative, using mathematical calculations to address the company's problems (Tika, Suprianto, and Isron 2022). This research was conducted at PT. SWX, located in Indonesia, with data collection aimed at determining optimal solutions based on existing numerical data, such as inventory costs, order quantities, and production time. This quantitative model ensures that decisions are based on measurable and accountable analysis. The proposed model has been applied to each demand dimension evaluated for the 2023–2024 time period.

Furthermore, the quantitative research applied also allows for simulations and comparisons of various possible decision scenarios. For example, through mathematical calculations, the impact of changes in order quantities or inventory costs on total operating costs can be projected. This allows the company not only to obtain an overview of the most efficient solution but

also to understand the risks and consequences of each available decision alternative. This is crucial for PT. SWX in navigating fluctuating market dynamics.

Furthermore, a quantitative approach adds value by providing objective results free of subjective bias in decision-making (Chen et al. 2025). The processed numerical data can serve as the basis for designing long-term strategies, such as production capacity planning, supply chain management, and operational cost control (Yao et al. 2022). In this way, PT. SWX can increase competitiveness through evidence-based decisions, as well as reduce uncertainty in production and distribution processes.

3.1. Production Lot Selection (Economic Order Quantity - EOQ)

In the first problem faced by PT. SWX, namely selecting the ideal production lot size, the Economic Order Quantity (EOQ) model was used to determine the most efficient lot size. EOQ is one of the most commonly used methods in inventory management to minimize the total costs associated with ordering and holding goods. In this case, the company had to choose among three lot sizes (20, 40, and 60 units), considering ordering costs, annual holding costs, and weekly supply quantities. The EOQ formula used to calculate the annual cycle inventory costs for each alternative, selecting the alternative with the lowest cost.

The EOQ method is particularly appropriate in this context because it helps companies determine efficient lot sizes based on ordering and holding costs, which are particularly relevant in mass-production operations like those carried out by PT. SWX.

3.2. Calculating Safety Stock and Reorder Point

Regarding the second issue, regarding safety stock and reorder points, companies need to calculate the required reserve stock to anticipate demand fluctuations and lead time disruptions. The methodology used to calculate safety stock and reorder points follows a standard formula that accounts for average demand, standard deviation, lead time, and the desired service level. In this case, the company must ensure there is sufficient stock to meet demand, even in the event of a disruption in the raw material procurement process.

Safety stock calculations are carried out by considering the level of demand and lead time variability, using standard deviation and z-scores to determine the amount of reserve stock needed to maintain a high level of customer service. Next, the reorder point is calculated based on average demand during the lead time and the previously calculated safety

stock, to ensure reorders are placed before stock runs out.

3.3. Production Sequencing with Critical Ratio (CR)

For the third problem related to production sequencing, where the company needed to develop an efficient production schedule for Smith & Wesson 17 components, the methodology used was the Critical Ratio (CR). CR is a technique for determining job priority based on the ratio of the remaining time (from the due date) to the time required to complete the job. By calculating the CR for each job, the company can prioritize the most urgent jobs, namely those with the lowest CR.

This method allows the company to manage time more effectively, minimize waiting times, and ensure that the jobs that must be completed first are prioritized, which is crucial in a time-constrained production environment.

3.4. Material Planning with Netting, Lotting, and Offsetting

For the fourth and fifth issues, which relate to production leveling and material requirements planning (netting, lotting, and offsetting), the methodology used is Material Requirements Planning (MRP). In this case, the company must calculate the material requirements for each component based on lead time, required quantity, and production sequence. The company also needs to consider netting, lotting, and offsetting techniques to ensure that raw materials and components are available on time without causing stockpiles or shortages.

Netting is used to calculate raw material requirements based on the number of components required for production. Lotting determines the optimal order size based on material requirements and offsets delivery times so that raw materials arrive on time according to the production schedule. These three techniques are used to plan material requirements more efficiently, reduce waste, and ensure a smooth production process.

4. RESULTS AND DISCUSSION

PT. SWX is a Foreign Direct Investment company located in Indonesia that produces defense equipment for the Indonesian National Armed Forces (TNI). Manufacturing operations face various challenges, including selecting the optimal lot size, managing inventory, and planning production.

4.1. Problem A - Ideal Lot Selection

To determine the most profitable lot size, the researcher will calculate the annual cycle inventory cost (C) using the Economic Order Quantity (EOQ) formula.

Table 1 Smith & Wesson 17 Pistol Sales Quantity

No	Description	Unit	Quantity
1	Price per unit of Smith & Wesson	USD	1500
2	Ordering fee (S)	USD	450
3	Annual loan fee (H)	Unit/pistol	25%
4	Quantity supplied per week	Units	15
5	Number of weeks in a year	Week	52
6	Alternative lot sizes: 20 units, 40 units, 60 units		

Step 1: Calculate the Holding Cost (H) per unit

Holding cost per unit per year (H) = 25% x USD 1,500 = USD 375

Step 2: Calculate the Annual Cycle Inventory Cost (C)

To calculate the annual cycle inventory cost, use the formula:

$$C = \frac{D}{Q} x\, S + \frac{Q}{2} x\, H$$

Where:

- D is the total annual demand (number of supplies per week x number of items per year) = 15 x 52 = 780 units per year
- Q is the selected lot size (20, 40, or 60 units)
- S is the ordering cost per order = USD 450
- H is the holding cost per unit per year = USD 375

For Lot 20 units:

$$C_{20} = \frac{780}{20} x\, 450 + \frac{20}{2} x\, 375$$
$$= 39\, x\, 450 + 10\, x\, 375$$
$$= 17.550 + 3.750$$
$$= 21.300 \text{ USD}$$

For Lot 40 units:

$$C_{40} = \frac{780}{40} x\, 450 + \frac{40}{2} x\, 375$$
$$= 19{,}5\, x\, 450 + 20\, x\, 375$$
$$= 8.775 + 7.500$$
$$= 16.275 \text{ USD}$$

For Lot 60 units:

$$C_{60} = \frac{780}{60} x\, 450 + \frac{60}{2} x\, 375$$
$$= 13\, x\, 450 + 30\, x\, 375$$
$$= 5.850 + 11.250$$
$$= 17.100 \text{ USD}$$

From the calculation above, the lowest annual cycle inventory cost is for a lot of 40 units, which is USD 16,275. Therefore, the most profitable lot size is 40 units. The calculations demonstrate the effectiveness in guiding strategic decision making and resource allocation to achieve business objectives.

Step 2: Calculating the Reorder Point

The reorder point is calculated using the formula:

$$Reorder\ Point = (Demant\ Rate\ x\ Lead\ Time) + Safety\ Stock$$

4.2. Problem B – Safety Stock and Reorder Point

Table 2 Average Replacement Demand

No	Description	Unit	Quantity
1	Average weekly demand for 30mm	Unit	8
2	Standard deviation of weekly demand	Unit	4
3	Lead time	Week	4%
4	Cycle service level = 90 % (z = 1,28)		

Step 1: Calculating Safety Stock

Safety Stock is calculated using the formula:

$$Safety\ Stock = z.\sigma$$

Where:

z = 1,28 (for a 90% service level). After determining the standard deviation of demand during the lead time, the company's service level needs to be determined. In an effort to satisfy customers, PT SWX sets a service level of 90%, or only allows stockouts to occur 10% out of 100 times.

σ = 4 (Standard deviation of weekly demand)

$$Safety\ Stock = 1{,}28\ x\ 4 = 5{,}12\ unit = 6\ unit$$

Where:

- Demand Rate = 8 units per week
- Lead Time = 4 weeks
- Safety Stock = 6 units

$$Reorder\ Point = (8\ x\ 4) + 6 = 32 + 6 = 38\ unit$$

By holding 6 units as safety stock, the company can anticipate demand fluctuations or delays during the lead time, ensuring that customer needs are met. A sufficiently large safety stock size (6 units) reflects the high demand uncertainty (standard deviation of 4 units) during the lead time. A reorder point of 38 units ensures that new orders are placed with enough time to arrive before

stock runs out, given the average demand of 8 units/week and a lead time of 4 weeks. This combination of ROP and SS provides a sufficient buffer to prevent stockouts without creating excessive inventory. Hence, it is necessary to research the implementation of inventory control. Analysis needs to be done to find out whether the method or method in the process of implementing inventory control (Nasution, Asthariq, and Girsang 2022).

- Work A

$$CR_A = \frac{8-0}{6} = 1.33$$

- Work B

$$CR_B = \frac{12-0}{8} = 1.50$$

- Work C

$$CR_C = \frac{15-0}{10} = 1.50$$

- Work D

$$CR_D = \frac{5-0}{2} = 2.50$$

- Work E

$$CR_E = \frac{10-0}{5} = 2.0$$

4.3.Problem C – Operation Sequencing with Critical Ratio

Table 3 Job Time and Due Time Data

Work	Working Time	Due Time
A	6	8
B	8	12
C	10	15
D	2	5
E	5	10

The Critical Ratio, according to EOQ can be determined using the formula:

$$CR = \frac{Due\ Date - Current\ Time}{Processing\ Time}$$

Where Current Time is assumed to be 0 (zero). Starting from zero point, so it can be used to simplify mathematical calculations and facilitate inventory planning analysis.

Step 1: Calculate the Critical Ratio for each job:

Step 2: Prioritization based on sequence

- A (CR = 1.33): This job has the lowest CR and is closest to critical. Therefore, it must be completed first to avoid delays.
- B (CR = 1.50) and C (CR = 1.50): These two jobs are in a balanced situation, but must still be done after A because of its subsequent priority.
- E (CR = 2.00): There is still enough time to complete this job without significant risk of delay.

● D (CR = 2.50): This job has the highest CR, making it the safest and can be done last

The CR method provides an effective approach to prioritizing jobs in a production system based on the remaining time relative to the required time. The sequence A → B → C → E → D reflects optimal resource allocation while minimizing the risk of delays on critical jobs.

4.4. Problem D – Leveling

Leveling is the process of adjusting production or material requirements to ensure a more even workload. In the context of Material Requirement Planning (MRP), leveling helps reduce fluctuations in production requirements and ensures optimal capacity utilization.

4.5. Problem E - Netting, Lotting, and Offsetting

The gross requirement for a Smith & Wesson 17 Pistol for five weeks is as follows:

Table 4. Gross Pistol Requirement Data

Gross Requirement Pistol				
1	2	3	4	5
100	120	150	180	200

Using the lead time and existing project minimums for each component, we can calculate the required netting, lotting, and offsetting for each component. The following component data and relevant information are available:

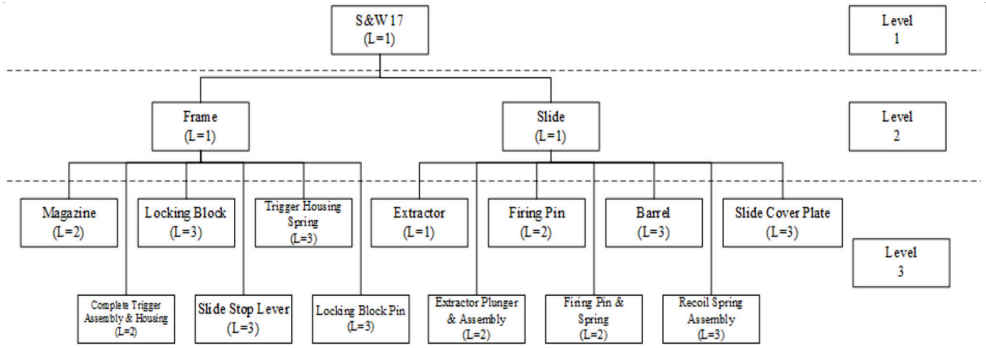

Fig. 1. Product Structure Based on the Manufacturing Hierarchy of the S&W 17 Pistol

Table 5 Lead Time, Project in Hand, Minimum Project in Hand data

Component	Code	Lead Time Week	Project in Hand	Minimum Project in Hand
PISTOL Smoth & Wesson 17	Pi	1	10	50
Frame	Fr	1	10	30
Magazine	Ma	2	10	30
Complete Trigger	Co	2	10	30
Assembly and Housing	As	2	10	30
Locking Block	Lo	3	10	30
Slide Stop Lever	Sl	3	10	30
Trigger Housing Spring	Tr	3	10	30
Locking Block Pin	LoB	3	10	30
SLIDE	Sd	1	10	30
Extractor	Ex	1	10	30
Extractor Plunger and Assy	EXP	2	10	30
Firing Pin	Fi	2	10	30
Firing Pin Safety and Spring	FiP	2	10	30
Barrel	Ba	3	10	30
Recoil Spring Assy	Re	3	10	30
Slide Cover Plate	SlC	3	10	30

In Material Requirement Planning (MRP), the Netting, Lotting, and Offsetting processes are essential steps to ensure raw materials and components are available on time and in the required quantities to efficiently meet production needs.

a. Netting.

- Netting is the process of calculating the net requirement for a component after accounting for the Gross Requirement, Project on Hand, and Minimum on Hand.
- Gross Requirement is the number of units needed to meet production demand.
- Project on Hand is the number of units already on hand or in production.
- Minimum on Hand is the minimum amount of stock required to ensure production continuity.

The formula for Netting is:

Net Requirement=Gross Requir ement−(Project on Hand+Minimum on Hand)

Table 6 Netting Data

Week	Pi	Fr	Ma	Co	As	Lo	Sl	Tr	LoB	Sd	Ex	EXP	FiP	Ba	Re	SlC
1	40	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
2	60	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
3	90	110	110	110	110	110	110	110	110	110	110	110	110	110	110	110
4	120	140	140	140	140	140	140	140	140	140	140	140	140	140	140	140
5	140	160	160	160	160	160	160	160	160	160	160	160	160	160	160	160

b. Lotting (Lot Size Determination)

Lotting is the process of determining the lot size to be ordered or produced. Lot size can be determined using various methods, such as Fixed Lot Size or Lot-for-Lot (LFL), where each production lot is adjusted to the calculated net requirement. In this case, we assume we are using a flexible lot size based on our needs.

After calculating the Net Requirement, we determine the lot size required for each component. In this case, we assume we are using the Lot-for-Lot (LFL) method, meaning the quantity produced is in accordance with the weekly net requirement. The lotting method that can be proposed to the company is the LFL method because it has the minimum inventory cost and can minimize the accumulation of raw material stock because the number of orders is adjusted to the production needs of the related period (Bakhtiar and Sinaga 2020)

Table 7 Lotting Data

Week	Pi	Fr	Ma	Co	As	Lo	Sl	Tr	LoB	Sd	Ex	EXP	FiP	Ba	Re	SlC
1	40	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
2	60	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
3	90	110	110	110	110	110	110	110	110	110	110	110	110	110	110	110
4	120	140	140	140	140	140	140	140	140	140	140	140	140	140	140	140
5	140	160	160	160	160	160	160	160	160	160	160	160	160	160	160	160

Offsetting

By calculating lead time, we determine when orders or production must be placed so that components are available in the right week.

Table 8 Data Offsetting

Component	Week 1	Week 2	Week 3	Week 4	Week 5
PISTOL Smooth & Wesson 17	40	60	90	120	140
FRAME	60	80	90	120	140
Magazine	60	80	90	120	140
Complete Trigger	60	80	90	120	140
Assembly and Housing	60	80	90	120	140
Locking Block	60	80	90	120	140
Slide Stop Lever	60	80	90	120	140
Trigger Housing Spring	60	80	90	120	140
Locking Block Pin	60	80	90	120	140
SLIDE	60	80	90	120	140
Extractor	60	80	90	120	140
Extractor Plunger and Assy	60	80	90	120	140
Firing Pin	60	80	90	120	140
Firing Pin Safety and Spring	60	80	90	120	140
Barrel	60	80	90	120	140
Recoil Spring Assy	60	80	90	120	140
Slide Cover Plate	60	80	90	120	140

5. CONCLUSION

In Problem A, we used the Economic Order Quantity (EOQ) approach to determine the most efficient order lot size. Based on calculations, a lot size of 40 units provides the lowest annual inventory cost compared to 20 and 60 units. This indicates that optimal lot sizes can reduce ordering and holding costs, which are crucial in manufacturing and logistics operations. Larger lot sizes are not always more profitable because they increase holding costs, while too small a lot size increases the frequency of orders, which can be more expensive. The appropriate lot size (40 units) helps optimize operational costs.

Safety stock and a reorder point (ROP) are used to ensure smooth production processes and uninterrupted demand fulfillment. Based on calculations, a safety stock of 6 units and a reorder point of 38 units were calculated, considering a 90% cycle service level and a 4-week lead time. Safety stock serves to anticipate unexpected fluctuations in demand, while the reorder point ensures that reorders are placed before stock runs out. With accurate calculations, the company can minimize the risk of stockouts and maintain smooth production.

We used the Critical Ratio (CR) method to prioritize tasks based on the remaining time and the time required to complete them. By calculating the CR for each task, we can rank tasks according to their urgency. In this case, the priority order is A → B → C → E → D, with task A having the highest priority because it has the lowest CR. The Critical Ratio method helps manage production schedules by prioritizing tasks closest to their deadlines. This technique is essential for optimizing time and resource allocation in complex production processes and avoiding delays.

In Problem D, a leveling process is used to even out the workload in production, particularly for components such as Frames, Magazines, and Complete Triggers. Using weekly demand data, leveling ensures consistent production each week, reducing fluctuations that can disrupt production flow. Leveling helps ensure production runs more steadily and is not disrupted by large fluctuations in demand or capacity. This improves resource efficiency and minimizes the need for sudden adjustments, such as overtime or excess storage.

In Problem E, Netting, Lotting, and Offsetting calculations are performed to ensure the availability of raw materials and components according to production needs. Netting calculates net requirements after accounting for existing stock; Lotting determines the lot size to be produced; and Offsetting ensures orders are placed on time by considering lead times. Netting, Lotting, and Offsetting are very important processes in material planning and inventory management. By performing careful calculations, companies can ensure the timely availability of raw materials, minimize storage costs, and avoid disruptions in the production process.

Furthermore, this study offers several avenues for future research. First, future research could expand the analysis of EOQ and safety stock by incorporating probabilistic demand and lead time variability models. Second, future research could compare CR with other scheduling and prioritization rules—such as Earliest Due Date (EDD), Shortest Processing Time (SPT), or Free Time Remaining—in multi-machine or multi-product environments. Third, future research could improve netting, lotting, and offsetting processes by integrating capacity constraints, supplier reliability, and risk-based lead time variability. This would support the development of more robust MRP systems that can better handle disruptions and improve material availability.

ACKNOWLEDGEMENT

This work was supported in part by a grant from Indonesia Defense

University. We would like to express our gratitude to all parties who supported the completion of this research.

DATA AVAILABILITY STATEMENT

The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

AI DISCLOSURE

The authors confirm that no generative AI tools were used in the preparation of this manuscript. All content is solely the product of original human intellectual effort and authorship.

REFERENCES

[1] Am, Jordan Bar, Laura Furstenthal, Felicitas Jorge, and Erik Roth. 2020. "Innovation in a Crisis: Why It Is More Critical than Ever." *McKinsey & Company* 11.

[2] Bakhtiar, Arfan &, and Erry Phoni Sinaga. 2020. "International Journal of Applied Science and Engineering Review." *International Journal of Applied Science and Engineering Review* 1 (6): 1–5.

[3] Best, Julian, Christoph H Glock, Eric H Grosse, Yacine Rekik, and Aris Syntetos. 2022. "On the Causes of Positive Inventory Discrepancies in Retail Stores." *International Journal of Physical Distribution & Logistics Management* 52 (5/6): 414–30.

[4] Budianto, Eka Wahyu Hestya, and Nindi Dwi Tetria Dewi. 2024. "The Role of Integrated Marketing Communications to Improving The Islamic Social Economy." *International Journal of Global Modern Research (IJGMR)* 1 (1): 1–18.

[5] Chen, Yang, Samuel N Kirshner, Anton Ovchinnikov, Meena Andiappan, and Tracy Jenkin. 2025. "A Manager and an AI Walk into a Bar: Does ChatGPT Make Biased Decisions like We Do?" *Manufacturing & Service Operations Management* 27 (2): 354–68.

[6] Cipta, Hendra, Rima Aprilia, and Hari Kurniawan. 2023. "Material Requirements Planning Method for Controlling Inventory of Raw Materials." *Jurnal Teknik Informatika C.I.T Medicom* 15 (1): 1–8. https://doi.org/10.35335/cit.vol15.2023.358.pp1-8.

[7] Costanzo, Paul J, and Harlan Spotts. 2015. "Re-Energizing The Brand: Smith & Wesson Holding Corporation." *Journal of the International Academy for Case Studies* 21 (3): 29.

[8] Demiray Kırmızı, Sema, Zeynep Ceylan, and Serol Bulkan. 2024. "Enhancing Inventory Management through Safety-Stock Strategies—A Case Study." *Systems* 12 (7):

1–17. https://doi.org/10.3390/systems12070260.

[9] Fole, Asrul, Nur Ihwan Safutra, Takdir Alisyahbana, Yamin Almuhajirin, and Khoerun Nisa Safitri. 2024. "Peningkatkan Efisiensi Rantai Pasok Melalui Material Requirement Planning Untuk Bahan Baku Dalam Produksi Lemari: Studi Kasus CV. Indo Mebel." *Jurnal Teknik Ibnu Sina (JT-IBSI)* 9 (01): 11–21.

[10] Gao, Da, Gai-Ge Wang, and Witold Pedrycz. 2020. "Solving Fuzzy Job-Shop Scheduling Problem Using DE Algorithm Improved by a Selection Mechanism." *IEEE Transactions on Fuzzy Systems* 28 (12): 3265–75.

[11] Ivanov, Dmitry, Alexander Tsipoulanidis, and Jörn Schönberger. 2021. "Production and Material Requirements Planning." In *Global Supply Chain and Operations Management: A Decision-Oriented Introduction to the Creation of Value*, 359–83. Springer.

[12] Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, Rajiv Suman, and Ernesto Santibañez Gonzalez. 2022. "Understanding the Adoption of Industry 4.0 Technologies in Improving Environmental Sustainability." *Sustainable Operations and Computers* 3:203–17.

[13] Kim, Taehoon, Yong-woo Kim, and Hunhee Cho. 2020. "Dynamic Production Scheduling Model under Due Date Uncertainty in Precast Concrete Construction." *Journal of Cleaner Production* 257:120527.

[14] Kurniawan, Michael Radius, Hadiyanto Hadiyanto, Joe Daniansyah Pahlevi Zulkarnaen, and Christian Harito. 2024. "Use Case Diagram for Enhancing Warehouse Performance at PT. MDA Through the Implementation of 5S, Economic Order Quantity, Safety Stock, and Warehouse Management System." *Engineering, MAthematics and Computer Science Journal (EMACS)* 6 (1): 69–78.

[15] Matoso, Rodrigo Ivo, Alexandre Rodrigues Freire, Leonardo Soriano de Mello Santos, Eduardo Daruge Junior, Ana Claudia Rossi, and Felippe Bevilacqua Prado. 2014. "Comparison of Gunshot Entrance Morphologies Caused by. 40-Caliber Smith & Wesson,. 380-Caliber, and 9-Mm Luger Bullets: A Finite Element Analysis Study." *PloS One* 9 (10): e111192.

[16] Mohamed, Ahmed Esmail. 2024. "Inventory Management." In *Operations Management-Recent Advances and New Perspectives*. IntechOpen.

[17] Mubasysyir, Muhammad Hanif, Sudradjat Supian, and Elis Hertini. 2024. "Multi-Item Inventory Control Using Economic Order Quantity (EOQ) Model with Safety Stock, Reorder Point, and Maximum Capacity in Retail Business." *International Journal of Global Operations Research* 5 (1): 55–61.

[18] Mustofa, Assyfatul Qolbi, and Nur Prima Waluyowati. 2024. "Penerapan Analisis ABC, Safety Stock, Dan Reorder Point Bahan Baku Impor." *Jurnal Kewirausahaan Dan Inovasi* 3 (2): 333–48.

[19] Nasution, Sri Lestari Ramadhani, Miftah Asthariq, and Ermi Girsang. 2022. "Analysis of the Implementation of Drug Inventory Control with the Always Better Control-Economic Order Quantity-Reorder Point-Safety Stock Method." *Open Access Macedonian Journal of Medical Sciences* 10 (A): 1397–1401. https://doi.org/10.3889/oamjms.2022.10383.

[20] Omair, Muhammad, Verena Stingl, and Brian Vejrum Wæhrens. 2025. "Circular Economy of Plastic: Revisiting Material Requirements Planning Practices for Managing Uncertain Supply." *Sustainability (Switzerland)* 17 (1). https://doi.org/10.3390/su17010112.

[21] Poornima, Galiveeti, J Vinay, P Karthikeyan, and V N Jinesh. 2024. "Inventory Tracking via IoT in the Pharmaceutical Industry." In *Intelligent Wireless Sensor Networks and the Internet of Things*, 147–204. CRC Press.

[22] Pramono, Owen Denpas. 2024. "Perencanaan Persediaan Bahan Baku Menggunakan Metode Material Requirements Planning (MRP) Di Nugraha Group." *Jurnal Ilmiah Penelitian Mahasiswa* 2 (4): 239–50.

[23] Putri, Suci Triana, Rina Mutiara, and Nofi Erni. 2025. "Efisiensi Perencanaan Persediaan Obat Fast Moving Dengan Kombinasi ABC-VEN, Safety Stock Dan Reorder Point Di Instalasi Farmasi Rumah Sakit Ibu Dan Anak Viola." *QISTINA: Jurnal Multidisiplin Indonesia* 4 (1): 41–58. https://doi.org/10.57235/qistina.v4i1.5783.

[24] Rabta, Boualem. 2020. "An Economic Order Quantity Inventory Model for a Product with a Circular Economy Indicator." *Computers & Industrial Engineering* 140:106215.

[25] Saptadi, Singgih, Helvina Aulia Zahra, Ary Arvianto, Purnawan Adi Wicaksono, and Wiwik Budiawan. 2023. "Inventory Planning and Control Method for Cement Raw Material with Material Requirement Planning (MRP)." *International Journal of Applied Science and Engineering Review (IJASER)* 4 (3): 18–31.

[26] Schiuma, Giovanni, Eva Schettini, Francesco Santarsiero, and Daniela Carlucci. 2022. "The Transformative Leadership Compass: Six Competencies for Digital Transformation Entrepreneurship." *International Journal of Entrepreneurial Behavior & Research* 28 (5): 1273–91.

[27] Setiawan, Fery. 2024. "Perancangan Aplikasi Pengendalian Persediaan Barang Dengan Metode Safety Stock

Dan Reorder Point (Studi Kasus: PT. Airlangga Jaya Mandiri)." *LOGIC: Jurnal Ilmu Komputer Dan Pendidikan* 2 (2): 401–8.

[28] Setyadi, Heribertus Ary, Budi Al Amin, and Pudji Widodo. 2024. "Implementation Economic Order Quantity and Reorder Point Methods in Inventory Management Information Systems." *Journal of Information Systems and Informatics* 6 (1): 103–17.

[29] Silver, Edward A, David F Pyke, and Douglas J Thomas. 2016. *Inventory and Production Management in Supply Chains*. CRC press.

[30] Siraj, Mahrukh, Asad Naseem, Muttahira Maryam, and Javeria Asad. 2024. "Optimizing Inventory Management: A Comprehensive Analysis of Economic Order Quantity, Lot Size, Safety Stock, and Reordering Quantity Strategies." *Journal of Business Administration and Management Sciences (JOBAMS)* 6 (1): 8–16.

[31] Sutejo, Mohamad Bambang, Degdo Suprayitno, and Wahyuddin Latunreng. 2023. "Controlling Raw Material Inventory Using the Economic Order Quantity (EOQ) Method at PT. ICI Paints Indonesia." *Sinergi International Journal of Logistics* 1 (3): 108–22.

[32] Tika, Etika Sabariah, Agung Suprianto, and Isron Isron. 2022. "Development of Business Mathematics Counting Integration Methods in the Big Data Era in Food Barn Management." *Jurnal Ekonomi* 11 (03): 1554–64.

[33] Tri, Nguyen Minh, Pham Duy Hoang, and Nguyen Trung Dung. 2021. "Impact of the Industrial Revolution 4.0 on Higher Education in Vietnam: Challenges and Opportunities." *Linguistics and Culture Review* 5 (S3): 1–15.

[34] Wolniak, Radosław, Adam Wyszomirski, Marcin Olkiewicz, and Anna Olkiewicz. 2021. "Environmental Corporate Social Responsibility Activities in Heating Industry—Case Study." *Energies* 14 (7): 1930.

[35] Yao, Xufeng, Nourah Almatooq, Ronald G Askin, and Greg Gruber. 2022. "Capacity Planning and Production Scheduling Integration: Improving Operational Efficiency via Detailed Modelling." *International Journal of Production Research* 60 (24): 7239–61.

ENVIRONMENTAL IMPACT OF DIGITALIZATION ACROSS EUROPEAN COUNTRIES: A COMPARATIVE STATISTICAL ANALYSIS

Cristina ANTONOAIE

Regional Department of Defense Resources Management Studies (DRESMARA) / "Carol I", National Defense University, Brasov, Romania

This paper examines greenhouse gas emissions from the ICT sector across the 27 European Union countries, analyzing both manufacturing and services components. Using EUROSTAT data, the analysis reveals fundamental asymmetries: ICT manufacturing emissions concentrate in lower ranges across most countries, while ICT services emissions distribute more widely with substantial high-emission clusters. Carbon dioxide dominates emissions, though methane and nitrous oxide contribute significantly when measured in CO_2 equivalents. Emission profiles reflect national ICT sector structures, energy mixes, and specializations.

Key words: *gas emissions, ICT manufacturing, ICT services*

INTRODUCTION

The digital transformation of contemporary society represents one of the most profound technological and socio-economic shifts of the twenty-first century. As European nations accelerate their digitalization efforts, the Information and Communication Technology (ICT) sector has emerged as a critical driver of economic growth, innovation, and societal change. However, this digital revolution occurs against the backdrop of an equally urgent imperative: the transition toward climate neutrality and environmental sustainability.

The European Union's ambitious target to achieve climate neutrality by 2050, enshrined in the European Green Deal, necessitates a comprehensive understanding of emissions across all economic sectors, including those traditionally perceived as "clean" or "dematerialized" such as the ICT sector. While digital technologies offer substantial potential for reducing emissions in other sectors through optimization, efficiency gains, and dematerialization of processes, the ICT sector itself generates significant environmental impacts through its production activities, energy consumption, and infrastructure operations.

[1] ORCID ID: 0009-0006-6303-2204, e-mail: cantonoaie@mapn.ro

Understanding the environmental footprint of the ICT sector requires distinguishing between its two primary components: ICT manufacturing and ICT services. ICT manufacturing encompasses the production of electronic components, computers, communication equipment, consumer electronics, and related hardware—activities that involve material extraction, energy-intensive fabrication processes, and complex global supply chains. ICT services, conversely, include telecommunications, data processing, hosting, software publishing, and related activities—operations that, while seemingly intangible, require substantial physical infrastructure including data centers, network equipment, and cooling systems, all of which consume significant energy.

The present paper undertakes a comprehensive statistical analysis of greenhouse gas emissions from the ICT sector across the twenty-seven European Union countries, examining both manufacturing and services components.

2. METHOD

The analysis focuses on multiple dimensions of emissions including total greenhouse gases (encompassing CO_2, N_2O in CO_2 equivalent, CH_4 in CO_2 equivalent, and fluorinated gases), carbon dioxide specifically, methane (both in absolute terms and CO_2 equivalent), and nitrous oxide from both ICT manufacturing and ICT services. By examining emissions on a per capita basis, the study enables meaningful comparisons across countries of varying population sizes and economic scales.

The analysis reveals substantial variation in emission profiles across European countries, reflecting differences in the scale and composition of national ICT sectors, energy sources employed in production and operations, regulatory frameworks, and technological sophistication. These variations offer valuable insights into potential pathways for emission reduction, highlighting both challenges and opportunities for aligning digital transformation with environmental sustainability objectives.

3. RESULTS AND DISCUSSION

3.1. Total greenhouse gases from ICT manufacturing (kg per capita)

The analysis of total greenhouse gas emissions from ICT manufacturing reveals a highly skewed distribution across the 27 European countries examined. The majority of countries demonstrate relatively low emission levels, while a small number of nations exhibit significantly elevated values.

Table 1 Greenhouse gases (CO2, N2O in CO2 equivalent, CH4 in CO2 equivalent, HFC in CO2 equivalent, PFC in CO2 equivalent, SF6 in CO2 equivalent, NF3 in CO2 equivalent) from ICT manufacturing (kg per capita)

Greenhouse gases from ICT manufacturing (kg per capita)	Countries	No of countries
0.00 - 3.70	BG, CY, DK, EL, ES, FI, FR, LU, LV, PL, PT, SE, SI	13
3.70 - 7.40	AT, BE, CZ, DE, LT, NL, SK	7
7.4 - 11.1	HR, IT, RO	3
11.1 - 14.8	EE, MT	2
14.8 - 18.5	HU	1
18.5 - 22.2	IE	1
Total		27

Source: Compiled by author from EUROSTAT Database

The largest group within low emission cluster (0.00-3.70 kg per capita) comprises thirteen countries (48% of the sample): Bulgaria, Cyprus, Denmark, Greece, Spain, Finland, France, Luxembourg, Latvia, Poland, Portugal, Sweden, and Slovenia. This cluster represents nations with minimal ICT manufacturing emissions intensity, suggesting either limited ICT manufacturing activities or highly efficient production processes with lower environmental impact per capita.

Seven countries occupy this intermediate range with medium-low emission (3.70-7.40 kg per capita) – (26% of the sample): Austria, Belgium, Czechia, Germany, Lithuania, Netherlands, and Slovakia. These nations demonstrate moderate ICT manufacturing emission levels, indicating a more substantial manufacturing presence compared to the lowest category while maintaining relatively controlled emission intensities.

Three countries fall into the category of medium-high emission group (7.40-11.10 kg per capita) – (11% of the sample): Croatia, Italy, and Romania. This group exhibits notably higher emissions, suggesting either more carbon-intensive manufacturing processes or a larger proportional contribution of ICT manufacturing to their economies.

High emission countries (11.10-18.50 kg per capita): Estonia and Malta represent the high-emission tier (7% of the sample), with

emissions ranging from 11.10 to 14.80 kg per capita. These elevated levels may reflect specialized manufacturing activities or specific structural characteristics of their ICT manufacturing sectors.

Hungary (14.80-18.50 kg per capita) and Ireland (18.50-22.20 kg per capita) stand as individual outliers with exceptionally high emissions. Ireland, in particular, demonstrates the highest ICT manufacturing emissions per capita among all analyzed countries, potentially indicating a concentration of emissions-intensive ICT manufacturing operations or methodological particularities in emissions allocation.

3.2. Total greenhouse gases from ICT services (kg per capita)

The emissions pattern for ICT services demonstrates a markedly different distribution compared to manufacturing, with a more dispersed spread across categories and a concentration in the higher emission ranges.

Table 2 Greenhouse gases (CO2, N2O in CO2 equivalent, CH4 in CO2 equivalent, HFC in CO2 equivalent, PFC in CO2 equivalent, SF6 in CO2 equivalent, NF3 in CO2 equivalent) from ICT services (kg per capita)

Greenhouse gases from ICT services (kg per capita)	Countries	No of countries
less than 11.49	BG, EE, ES, FI, IT, PT, SE, SK	8
11.49 - 12.79	AT, CZ	2
12.79 - 14.09	DK, EL, LT	3
14.09 - 15.39	FR, LV	2
more than 15.39	BE, CY, DE, HR, HU, IE, LU, MT, NL, PL, RO, SI	12
Total		27

Source: Compiled by author from EUROSTAT Database

Eight countries constitute lowest emission group (less than 11.49 kg per capita – (30% of the sample): Bulgaria, Estonia, Spain, Finland, Italy, Portugal, Sweden, and Slovakia. Interestingly, Estonia appears in the lowest services emission category despite being in the high manufacturing emission group, suggesting a structural imbalance between manufacturing and services emissions within its ICT sector.

In lower-middle range (11.49-12.79 kg per capita) we found Austria and Czechia (7% of the sample), representing a transitional category between lower and moderate emission levels.

Denmark, Greece, and Lithuania form the middle range group (12.79-14.09 kg per capita) – (11% of the sample), demonstrating moderate ICT services emissions that align closely with the median distribution.

France and Latvia represent the upper-middle range category (14.09-15.39 kg per capita) – (7% of the sample), positioned just below the highest emission tier.

The largest group with highest emission (more than 15.39 kg per capita) comprises twelve countries (44% of the sample): Belgium, Cyprus, Germany, Croatia, Hungary, Ireland, Luxembourg, Malta, Netherlands, Poland, Romania, and Slovenia. This substantial concentration in the highest category indicates that ICT services emissions are generally more elevated across European countries compared to manufacturing emissions, potentially reflecting the energy-intensive nature of data centers, telecommunications infrastructure, and digital services operations.

3.3. Carbon dioxide from ICT manufacturing (kg per capita)

Carbon dioxide emissions from ICT manufacturing show a highly concentrated distribution, with the vast majority of countries exhibiting low emission levels.

Table 3 Carbon dioxide from ICT manufacturing (kg per capita)

Carbon dioxide from ICT manufacturing (kg per capita)	Countries	No of countries
less than 7.53	AT, BE, BG, CY, CZ, DK, EL, ES, FI,FR, LT, LU, LV, NL, PL, PT, SE, SI, DE, IT, SK	21
7.53 - 10.04	HR, IE, MT, RO	4
more than 10.04	EE, HU	2
Total		27

Source: Compiled by author from EUROSTAT Database

An overwhelming majority of 21 countries (78% of the sample) fall into low emission majority (less than 7.53 kg per capita): Austria, Belgium, Bulgaria, Cyprus, Czechia, Denmark, Greece, Spain, Finland, France, Lithuania, Luxembourg, Latvia, Netherlands, Poland, Portugal, Sweden, Slovenia, Germany, Italy, and Slovakia. This extensive grouping suggests that CO2 emissions from ICT manufacturing are generally well-controlled across most European nations, possibly due to cleaner energy sources in manufacturing processes or limited manufacturing scale.

In the medium emission group (7.53-10.04 kg per capita) we have four countries (15% of the sample): Croatia, Ireland, Malta, and Romania. These nations demonstrate moderately elevated CO2 emissions from manufacturing, potentially indicating more carbon-intensive energy sources or manufacturing processes.

Estonia and Hungary represent the highest emission category (7% of the sample), with CO2 emissions exceeding 10.04 kg per capita. These elevated levels suggest either particularly carbon-intensive manufacturing operations or energy mix characteristics that result in higher CO2 intensity.

3.4. Carbon dioxide from ICT services (kg per capita)

CO2 emissions from ICT services exhibit a more graduated distribution across emission ranges, contrasting with the concentrated pattern observed in manufacturing.

Table 4 Carbon dioxide from ICT services (kg per capita)

Carbon dioxide from ICT services (kg per capita)	Countries	No of countries
1.3 - 10.12	AT, BG, EE, EL, ES, FI, IT, PT, SE, SK	10
10.12 - 18.94	CY, CZ, DK, FR, HR, LT, LV, NL, RO	9
18.94 - 27.76	BE, DE, HU, MT, PL, SI	6
more than 27.76	IE, LU	2
Total		27

Source: Compiled by author from EUROSTAT Database

Ten countries constitute the group (37% of the sample) of lowest emission tier (1.30-10.12 kg per capita): Austria, Bulgaria, Estonia, Greece, Spain, Finland, Italy, Portugal, Sweden, and Slovakia. Notably, Estonia appears in the lowest services CO2 category while being in the highest manufacturing category, indicating a clear sectoral divergence.

Nine countries occupy the lower-middle tier (10.12-18.94 kg per capita) – (33% of the sample): Cyprus, Czechia, Denmark, France, Croatia, Lithuania, Latvia, Netherlands, and Romania. This substantial grouping represents nations with moderate ICT services CO2 emissions.

Six countries fall into the upper-middle tier (18.94-27.76 kg per capita): (22% of the sample): Belgium, Germany, Hungary, Malta, Poland, and Slovenia, demonstrating elevated CO2 emissions from services operations.

Ireland and Luxembourg represent the highest emission tier (7% of the sample), (more than 27.76 kg per capita): with CO2 emissions substantially exceeding those of other nations. This may reflect the concentration of large-scale data centers and digital infrastructure in these countries.

3.5. Methane from ICT manufacturing (grams per capita)

Methane emissions from ICT manufacturing demonstrate an extremely skewed distribution, with the majority of countries clustered in the lowest emission category.

Table 5 Methane from ICT manufacturing (grams per capita)

Methane from ICT manufacturing (grams per capita)	Countries	No of countries
0.00 - 0.11	AT, BE, BG, CY, EE, EL, FI, FR, IT, LT, LU, LV, PL, PT, SE, SI	16
0.11 - 0.22	DK, ES, HR	3
0.22 - 0.33	CZ, DE, MT	3
0.33 - 0.44	HU, IE, RO	3
more than 0.44	NL, SK	2
Total		27

Source: Compiled by author from EUROSTAT Database

Sixteen countries (59% of the sample) exhibit minimal methane emissions: (0.00-0.11 grams per capita): Austria, Belgium, Bulgaria, Cyprus, Estonia, Greece, Finland, France, Italy, Lithuania, Luxembourg, Latvia, Poland, Portugal, Sweden, and Slovenia. This extensive grouping suggests that methane emissions from ICT manufacturing are generally negligible across most European countries.

Low emission group (0.11-0.22 grams per capita) is composed of Denmark, Spain, and Croatia constitute this category (11% of the sample), showing slightly elevated but still relatively low methane emissions.

Czechia, Germany, and Malta occupy medium-low emission group (0.22-0.33 grams per capita) – (11% of the sample), demonstrating moderate methane emission levels.

Hungary, Ireland, and Romania fall into this category (0.33-0.44 grams per capita) – (11% of the sample), exhibiting notably higher methane emissions from manufacturing operations.

Highest emission countries (more than 0.44 grams per capita) are Netherlands and Slovakia (7% of the sample), with emissions exceeding 0.44 grams per capita, possibly indicating specific manufacturing processes or energy sources with higher methane intensity.

3.6. Methane from ICT services (grams per capita)

Methane emissions from ICT services show a more evenly distributed pattern across emission ranges compared to manufacturing.

Table 6 Methane from ICT services (grams per capita)

Methane from ICT services (grams per capita)	Countries	No of countries
0.10 - 0.93	AT, CY, CZ, EE, EL, IT, PT, SE, SK	9
0.93 - 1.76	BE, DK, FI, FR, IE, MT, SI	7
1.76 - 2.59	BG, ES, NL	3
2.59 - 3.42	HR, RO	2
3.42 - 4.25	HU, LT, LU	3
4.25 - 5.08	DE, LV, PL	3
Total		27

Source: Compiled by author from EUROSTAT Database

Nine countries occupy the category of lowest emission range (0.10-0.93 grams per capita) – (33% of the sample): Austria, Cyprus, Czechia, Estonia, Greece, Italy, Portugal, Sweden, and Slovakia, representing nations with minimal methane emissions from services.

Seven countries constitute the lower-middle range (0.93-1.76 grams per capita) group (26% of the sample): Belgium, Denmark, Finland, France, Ireland, Malta, and Slovenia, demonstrating moderate-low emission levels.

Middle range (1.76-2.59 grams per capita) – here we found Bulgaria, Spain, and Netherlands form this category (11% of the sample), positioned in the median emission range.

In the upper-middle range (2.59-3.42 grams per capita) we have Croatia and Romania (7% of the sample), showing elevated methane emissions from services.

High emission group (3.42-4.25 grams per capita) is composed of Hungary, Lithuania, and Luxembourg (11% of the sample), demonstrating notably high methane emissions.

Germany, Latvia, and Poland constitute the highest emission category (11% of the sample), with methane emissions exceeding 4.25 grams per capita, potentially reflecting large-scale data center operations or specific infrastructure characteristics.

3.7. Methane in CO2 equivalent from ICT manufacturing (grams per capita)

The distribution of methane expressed in CO2 equivalents from manufacturing mirrors the pattern observed for absolute methane emissions, albeit with adjusted numerical values reflecting the Global Warming Potential (GWP) factor of 28 for methane.

Table 7 Methane (CO2 equivalent) from ICT manufacturing (grams per capita)

Methane (CO2 equivalent) from ICT manufacturing (grams per capita)	Countries	No of countries
0.00 - 3.22	AT, BE, BG, CY, EE, EL, FI, FR, IT, LT, LU, LV, PL, PT, SE, SI	16
3.22 - 6.44	ES, HR	2
6.44 - 9.66	CZ, DE, DK, MT	4
9.66 - 12.88	HU, IE, RO	3
more than 12.88	NL, SK	2
Total		27

Source: Compiled by author from EUROSTAT Database

Sixteen countries (59% of the sample) fall into the category of minimal emission cluster (0.00-3.22 grams CO2 eq. per capita): Austria, Belgium, Bulgaria, Cyprus, Estonia, Greece, Finland, France, Italy, Lithuania, Luxembourg, Latvia, Poland, Portugal, Sweden, and Slovenia, indicating negligible methane contribution to greenhouse gas emissions from manufacturing.

Low emission group (3.22-6.44 grams CO2 eq. per capita) is composed of Spain and Croatia constitute this small category (7% of the sample).

In the Medium Emission Group (6.44-9.66 grams CO2 eq. per capita) we found four countries (15% of the sample): Czechia, Germany, Denmark, and Malta.

Hungary, Ireland, and Romania demonstrate elevated methane-related GHG emissions (11% of the sample) (9.66-12.88 grams CO2 eq. per capita):

Netherlands and Slovakia represent the highest tier (7% of the sample), with methane contributions exceeding 12.88 grams CO2 equivalent per capita.

3.8. Methane in CO2 equivalent from ICT services (grams per capita)

Methane in CO2 equivalents from services demonstrates a broader distribution across categories, reflecting the higher overall methane emissions from services compared to manufacturing.

Table 8 Methane (CO2 equivalent) from ICT services (grams per capita)

Methane (CO2 equivalent) from ICT services (grams per capita)	Countries	No of countries
3.60 - 26.88	AT, CY, CZ, EE, EL, IT, PT, SE, SK	9
26.88 - 50.16	BE, DK, FI, FR, IE, MT, SI	7
50.16 - 73.44	BG, ES, NL	3
73.44 - 96.72	HR, RO	2
96.72 - 120.00	HU, LT, LU	3
120.00 - 143.28	DE, LV, PL	3
Total		27

Source: Compiled by author from EUROSTAT Database

Nine countries occupy the category of lowest range (3.60-26.88 grams CO2 eq. per capita) – (33% of the sample): Austria, Cyprus, Czechia, Estonia, Greece, Italy, Portugal, Sweden, and Slovakia.

Lower-middle range group (26.88-50.16 grams CO2 eq. per capita) is composed by seven countries (26% of the sample): Belgium, Denmark, Finland, France, Ireland, Malta, and Slovenia.

Bulgaria, Spain, and Netherlands form the category of middle range group (50.16-73.44 grams CO2 eq. per capita) – (11% of the sample).

Croatia and Romania represent the tier of upper-middle range (73.44-96.72 grams CO2 eq. per capita) – (7% of the sample).

Hungary, Lithuania, and Luxembourg have high emission (96.72-120.00 grams CO2 eq. per capita) – (11% of the sample).

Highest emission tier (120.00-143.28 grams CO2 eq. per capita) is formed by Germany, Latvia, and Poland (11% of the sample), demonstrating the most substantial methane-related greenhouse gas contributions from ICT services.

3.9. Nitrous oxide from ICT manufacturing (grams per capita)

Nitrous oxide emissions from ICT manufacturing show the most concentrated distribution among all analyzed pollutants, with an overwhelming majority of countries in the minimal emission range.

Table 9 Nitrous oxide from ICT manufacturing (grams per capita)

Nitrous oxide from ICT manufacturing (grams per capita)	Countries	No of countries
0.00 - 0.12	AT, BE, BG,CY,CZ, DK, EE, EL, ES, FI, FR, HU, IE, IT, LT, LU, LV, NL, PL, PT, SE, SI	22
0.12 - 0.24	RO	1
0.24 - 0.36	HR, MT	2
more than 0.36	DE, SK	2
Total		27

Source: Compiled by author from EUROSTAT Database

Twenty-two countries (81% of the sample) exhibit minimal N2O emissions (0.00-0.12 grams per capita):: Austria, Belgium, Bulgaria, Cyprus, Czechia, Denmark, Estonia, Greece, Spain, Finland, France, Hungary, Ireland, Italy, Lithuania, Luxembourg, Latvia, Netherlands, Poland, Portugal, Sweden, and Slovenia. This extensive grouping indicates that nitrous oxide emissions from ICT manufacturing are generally negligible across most European nations.

Low emission (0.12-0.24 grams per capita): Romania alone occupies this category (4% of the sample).

Medium emission group (0.24-0.36 grams per capita) is formed by Croatia and Malta (7% of the sample).

Highest emission countries (more than 0.36 grams per capita) are Germany and Slovakia (7% of the sample), with emissions exceeding 0.36 grams per capita.

3.10. Nitrous oxide from ICT services (grams per capita)

N2O emissions from ICT services exhibit a more graduated distribution across multiple categories, contrasting sharply with the concentrated manufacturing pattern.

Table 10 Nitrous oxide from ICT services (grams per capita)

Nitrous oxide from ICT services (grams per capita)	Countries	No of countries
0.10 - 0.29	BG, EE, EL, ES, FI, IT	6
0.29 - 0.48	CY, CZ, FR, HU, LT, PT, SE	7
0.48 - 0.67	AT, DK, HR, RO	4
0.67 - 0.86	BE, DE, MT, NL, PL, SI	6
0.86 - 1.05	IE	1
1.05 - 1.24	LU, LV, SK	3
Total		27

Source: Compiled by author from EUROSTAT Database

Six countries occupy the lowest emission range (0.10-0.29 grams per capita): (22% of the sample): Bulgaria, Estonia, Greece, Spain, Finland, and Italy.

Seven countries constitute the group of lower-middle range (0.29-0.48 grams per capita) – (26% of the sample): Cyprus, Czechia, France, Hungary, Lithuania, Portugal, and Sweden.

Middle range (0.48-0.67 grams per capita): Austria, Denmark, Croatia, and Romania form this category (15% of the sample).

Upper-middle range (0.67-0.86 grams per capita): Six countries occupy this tier (22% of the sample): Belgium, Germany, Malta, Netherlands, Poland, and Slovenia.

Ireland alone represents this category high emission (0.86-1.05 grams per capita) – (4% of the sample). And the highest emission tier (1.05-1.24 grams per capita) is formed by Luxembourg, Latvia, and Slovakia (11% of the sample), with N2O emissions exceeding 1.05 grams per capita.

If we look at Manufacturing vs. Services Emission Patterns we found Divergent Distribution Characteristics: A fundamental observation emerges when comparing manufacturing and services emissions across all pollutant types: ICT manufacturing emissions demonstrate consistently more concentrated distributions with the majority of countries clustered in lower emission categories, while ICT services emissions show more dispersed patterns with substantial numbers of countries in higher emission ranges. This structural difference suggests that ICT services activities (including data centers, telecommunications, and digital infrastructure) are inherently more emissions-intensive on a per capita basis than ICT manufacturing activities across the European landscape.

Analyzing the Country-Specific Patterns we observe Consistent Low Emitters: Certain countries consistently appear in the lowest emission categories across multiple pollutant types for both manufacturing and services. Bulgaria, Finland, Portugal, and Sweden demonstrate this pattern, suggesting comprehensive low-emission profiles across their entire ICT sectors. These nations may benefit from cleaner energy mixes, efficient operations, or smaller-scale ICT sector activities relative to their populations.

Hungary and Ireland are Manufacturing-Intensive Emitters. They consistently occupy higher emission categories for manufacturing-related pollutants, particularly for total greenhouse gases and specific compounds. This pattern suggests specialized or concentrated ICT manufacturing activities with higher emission intensities in these countries.

Services-Intensive Emitters, like Luxembourg, Ireland, and Germany frequently appear in higher emission categories for ICT services across multiple pollutant types. This pattern likely reflects

the concentration of large-scale data centers, digital infrastructure, and telecommunications operations in these countries, which are inherently energy and emissions-intensive.

We have also Balanced Profiles: Some countries, such as Denmark, Netherlands, and Belgium, demonstrate moderate-to-high emissions across both manufacturing and services categories, suggesting more balanced ICT sector structures with substantial activities in both domains.

4. CONCLUSIONS

This comprehensive statistical analysis of greenhouse gas emissions from the ICT sector across the twenty-seven European Union countries reveals a complex and heterogeneous landscape characterized by substantial inter-country variation, distinct patterns between manufacturing and services components, and differentiated emission profiles across various pollutant types.

Perhaps the most striking finding of this analysis is the fundamental structural difference in emission patterns between ICT manufacturing and ICT services across all examined pollutant categories. ICT manufacturing emissions consistently demonstrate highly concentrated distributions, with the majority of countries clustered in lower emission ranges and only a small number of nations exhibiting elevated levels. In contrast, ICT services emissions display more dispersed patterns with substantial proportions of countries occupying higher emission categories.

This asymmetry suggests that ICT services activities—encompassing telecommunications infrastructure, data centers, hosting services, and digital platforms—are inherently more emissions-intensive on a per capita basis than ICT manufacturing across the European landscape. The energy demands of maintaining continuous digital connectivity, processing vast quantities of data, ensuring redundancy and reliability, and cooling infrastructure appear to generate more significant environmental impacts relative to population than the production of ICT hardware, at least when measured at the national level.

This finding has profound implications for emission reduction strategies within the ICT sector. While manufacturing emissions can be addressed through production efficiency, cleaner manufacturing processes, and supply chain optimization, services emissions require different interventions focused on data center efficiency, renewable energy procurement, network optimization, and fundamental questions about the energy intensity of digital infrastructure and services proliferation.

The statistical evidence presented in this analysis demonstrates that the environmental impact of the ICT sector across Europe is substantial, variable, and structurally complex. As European nations pursue ambitious digital transformation agendas while simultaneously committing to climate

neutrality, the emissions profile of the ICT sector—particularly the services component—emerges as a critical policy domain requiring sustained attention, innovation, and coordinated action.

ENDNOTES

The source of data was EUROSTAT. All these statistics are available by type of air pollutants and greenhouse gases (AIRPOL):

- Carbon dioxide without emissions from biomass (CO_2) [CO2],
- Carbon dioxide from biomass (Biomass CO_2)* [CO2_BIO],
- Nitroux oxide (N_2O) [N2O],
- Methane (CH_4) [CH4],
- Perfluorocarbons (PFCs),
- Hydrofluorocarbons (HFCs),
- Sulphur hexafluoride (SF_6) including nitrogen trifluoride (NF_3),
- Nitrogen oxides (NOx) [NOX],
- Non-methane volatile organic compounds [NMVOC],
- Carbon monoxide (CO) [CO],
- Particulate matter < 10µm [PM10],
- Particulate matter < 2,5µm [PM2_5],
- Sulphur dioxide (SO_2) expressed in SO_2 equivalent,
- Ammonia (NH_3) [NH3], and various air pollutants expressed in equivalents of another air pollutant:
- CH_4 in CO_2 equivalents [CH4_CO2E]
- N_2O in CO_2 equivalents [N2O_CO2E]
- HFC in CO_2 equivalents [HFC_CO2E]
- PFC in CO_2 equivalents [PFC_CO2E]
- SF_6 and NF_3 in CO_2 equivalents [NF3_SF6_CO2E]
- NH_3 in SO_2 equivalents [NH3_SO2E]
- SOx in SO_2 equivalents [SOX_SO2E]
- NOx in SO_2 equivalents [NOX_SO2E]
- CO in NMVOC equivalents [CO_NMVOCE]
- CH_4 in NMVOC equivalents [CH4_NMVOCE]
- NOx in NMVOC equivalents [NOX_NMVOCE]

These statistics on the air emissions of the ICT sector provide insights about the scale of the different pollutants and greenhouse gasses emissions produced by the ICT sector, how big part of those emissions come from the ICT manufacturing and ICT services sub-sectors, as well as the share of those emissions in the emissions of total economy. The definition of ICT sector used for the purpose of producing these statistics follows the OECD official definition: "The production (goods and services) of a candidate industry must primarily be intended to fulfil or enable the function of information processing and communication by electronic means, including transmission and display" (OECD Guide to Measuring the Information Society 2011). Operationalized definition of the ICT

sector and its components in terms of economic activities (and their codes) according to NACE rev.2 fulfilling the OECD definition includes:

ICT sector - Total	**ICT Manufacturing**	C26.1	Manufacture of electronic components and boards
		C26.2	Manufacture of computers and peripheral equipment
		C26.3	Manufacture of communication equipment
		C26.4	Manufacture of consumer electronics
		C26.8	Manufacture of magnetic and optical media
		G46.5	Wholesale of information and communication equipment
	ICT Services	J58.2	Software publishing
		J61	Telecommunications
		J62	Computer programming, consultancy and related activities
		J63.1	Data processing, hosting and related activities; web portals
		S95.1	Repair of computers and communication equipment

AI DISCLOSURE

The author acknowledge the use of generative AI tools to assist in the preparation of this manuscript. This tool was used solely for language editing and structural suggestions, under the complete control and responsibility of the authors. The author reviewed and edited all AI-assisted content and takes full responsibility for the accuracy and integrity of the published work.

REFERENCES

[1] https://ec.europa.eu/eurostat/data/database
[2] https://ec.europa.eu/eurostat/databrowser/view/isoc_env_ict_aec/default/table?lang=en&category=isoc.isoc_ad.isoc_env_ict.isoc_env_ict_a
[3] https://ec.europa.eu/eurostat/cache/metadata/en/isoc_env_ict_a_esmsip2.htm
[4] https://ec.europa.eu/eurostat/databrowser/view/env_waseleeos$dv_3021/default/table?lang=en&category=isoc.isoc_ad.isoc_env_ict.isoc_env_ict_w
[5] https://ec.europa.eu/eurostat/databrowser/view/env_waselee$dv_3022/default/table?lang=en&category=isoc.isoc_ad.isoc_env_ict.isoc_env_ict_w

HEALTHCARE MANAGEMENT IN CONFLICT SETTINGS: THE CRITICAL ROLE OF MEDICAL LABORATORIES AND BIOSAFETY

Mihaela BARCAN

Leamna Pneumophthisiology Hospital, Craiova, Romania

In contemporary global contexts characterized by persistent armed conflicts—such as those in Ukraine and the Middle East—healthcare system management extends beyond routine hospital operations and constitutes a critical component of overall health system resilience. Strategic decisions on resource allocation and contingency planning can substantially influence the probability of secondary public health outbreaks, potentially mitigating or exacerbating widespread crises in short timeframes. Medical diagnostic laboratories (hematology, microbiology, immunology) play a central role in these settings by performing diagnostics and providing ongoing surveillance of biological threats, which can escalate rapidly amid wartime disruptions and lead to significant consequences. Reports from conflict zones document frequent disruptions to laboratory operations, including power outages, infrastructure damage from attacks, forced staff relocation, and security breaches such as theft. The biological risks persist irrespective of ceasefire agreements and necessitate ongoing preparedness and mitigation efforts. Healthcare leadership should therefore prioritize biosafety and biosecurity as core operational components, integrated into routine management rather than confined to emergency plan appendices, to effectively reduce associated risks.

Key words: *management, laboratory, biosafety, conflict, biological risk*

1. INTRODUCTION

Contemporary global maps reveal the widespread presence of armed conflicts, which have become a recurring feature of the international landscape and are often overlooked until they directly impact populations or health systems. From the war in Ukraine, now in its fifth year and destroying the health infrastructure in entire swaths of the country, to the endless tensions in the Middle East, where hospitals and laboratories are becoming targets or collateral damage, the reality is stark.

Healthcare management is no longer a desk job, with paperwork and routine procedures. It has become a front line, where every choice made today, how much reagent

[1] ORCID ID: 0000-0001-9543-8993, e-mail: mihaela.barcan@gmail.com

stock to keep, where to place backup generators, how to train people for evacuation, can stop a public health catastrophe or, on the contrary, trigger one with chain effects that go beyond borders.

Medical laboratories are right in the middle of this situation. Hematology, which counts blood cells in patients with massive hemorrhages on the front, microbiology, which identifies nosocomial infections in war wounded, or immunology, which tracks the spread of viruses in refugee camps, all of these are not just auxiliary services. They are the diagnostic brain of the entire system. Without them, doctors work haphazardly, and epidemiological surveillance collapses. But this is precisely where the greatest danger arises: biological risks.

In the chaos of war, a laboratory that was functioning perfectly yesterday can become a real threat tomorrow. Lack of electricity after a bombing, theft of equipment, forced displacement of personnel, interruption of supply chains with disinfectants or triple packaging for transporting samples, all of these are not movie scripts. Such incidents have been documented in reports from conflict-affected areas, including cases where diagnostic samples remained in non-functional refrigerators due to power failures or equipment damage. For that is important technicians to improvise decontamination without running water.

The World Health Organization makes this clear in its updated biosecurity guidance: extreme situations, war, civil unrest, devastating natural disasters, require special protective measures, tailored to the extreme risks [13]. This is not just about ordinary laboratory accidents. It is about the possibility that pathogens can get out of control and trigger secondary outbreaks just when the health system is already overwhelmed. In Ukraine, the 2022 invasion endangered dozens of public laboratories that handled dangerous pathogens. Although the accusations of biological weapons were proven unfounded, the real risk of accidental release existed due to destruction, prolonged power outages, and logistical chaos [7].

Staff had to evacuate sensitive stocks under bomb threat and monitoring antimicrobial resistance in the wounded became a daily challenge. That is why biosafety (which protects us, those who work there, and the surrounding community from accidental exposures) and biosecurity (which prevents the theft, loss, or intentional misuse of biological materials) can no longer sit as forgotten appendages in emergency plans. They must be the absolute priority, integrated into every management decision, from choosing the location of the

laboratory to monthly simulations of biological breaches under total blackout conditions.

In Romania, in the absence of a current armed conflict, hospital regulations, according to the national legal framework, oblige healthcare institutions, including medical laboratories, to develop and maintain preparedness plans for major crisis situations, such as war, disasters, terrorist attacks or social crises. Ignoring them is not just administrative negligence, it is a lack of responsibility towards the patients of tomorrow.

The paper proceeds with an in-depth review of healthcare management in conflict-affected settings, emphasizing the critical functions of medical analysis laboratories and approaches to minimizing biological risks. Specific elements discussed encompass the formulation of robust business continuity plans, implementation of realistic simulation-based training, and allocation of resources for preventive measures while conditions permit proactive planning Because, in the final analysis, biological safety is not a theoretical chapter in some textbook. It is a matter of survival, for staff, for patients and for the entire community.

2. SECURITY OF MEDICAL LABORATORY PERSONNEL

In conflict-affected settings, laboratory personnel may face simultaneous physical and biological threats, such as in a microbiology lab in a city on the edge of the front. Explosions are heard outside, the power is constantly off, and samples are in refrigerator with dangerous strains that should never be released outside.

At such times, the physical security of the building and the protection of the people working there are no longer bureaucratic items in the emergency plan, an essential layer of protection against biological risks. In modern conflicts, medical laboratories are no longer sanctuaries protected by the Geneva Conventions.

On the contrary, they become precise targets or, at the very least, collateral casualties. The study of Mariupol shows that 77% of the city's medical facilities were seriously damaged during the Russian siege from February to May 2022, and the size of the building did not matter: attacks hit small laboratories and large blocks of flats equally often [10].

This suggests that it was not just random fire, but a deliberate strategy to destroy the health infrastructure. For an analysis laboratory, the consequences are twofold: on the one hand, equipment is destroyed, reagents are lost, refrigerators with pathogens stop working; on the other hand, unauthorized access becomes possible – someone can enter and

steal sensitive samples exactly when security is minimal.

Therefore, physical security must be thought out from scratch in continuity plans. It is not enough to put a lock on the door. Managers must choose or adapt less visible locations: basements, buildings with reinforced walls, peripheral areas away from main arteries. In Ukraine, military doctors quickly learned to use underground parking lots and cellars as field hospitals precisely to escape drones and missiles [6].

For laboratories, this means biosafety chambers moved to lower levels, diesel or solar hybrid generators mounted in protected locations, windows covered with anti-fragmentation mesh, surveillance cameras with backup batteries and, where the law allows, concrete physical barriers or barbed wire fences. Controlled access becomes vital.

In peacetime, a magnetic card is enough. In conflict, talking about strict lists of essential personnel, daily manual checks, entry-exit logs and, in extreme cases, armed guard coordinated with local authorities. No one enters the BSL-2 or BSL-3 area without a clear reason, and sensitive samples must be kept in biometric safes that work even without power. And don't forget opportunistic robbery: in the chaos of war, expensive equipment disappears overnight, and a broken refrigerator means biological hazards are released into the environment.

But the hardest part is the security of the staff. Lab technicians, biochemists, microbiologists are not trained for war. They come to work with their families in mind, not their helmets on. However, they become vulnerable just like anyone else: they can be injured on the way to the lab, taken hostage, threatened into giving information, or simply killed in direct attacks on the building.

Many choose to flee – and who can blame them? Those who stay work under extreme stress, with delayed or reduced salaries, without running water, without hot food, with the constant fear that a siren means the immediate evacuation of dangerous samples. Reports from conflict zones show that absenteeism is increasing explosively, supply chains are breaking down, and the remaining staff are physically and mentally exhausted [14].

Therefore, management must include concrete measures for people, not just buildings, plans to evacuate key staff families to safe areas, mandatory rotations to ensure that no one gets burned out, free psychological counseling, special life insurance and, above all, realistic training. Not just paper biosafety exercises, but real simulations: "What do you do if a kamikaze drone enters the yard?", "How do you seal a biosafety cabinet in five minutes

when the power goes out?", "What is the alternative route to evacuate samples if the bridge blows up?".

Staff must know how to combine biological and physical protection: N95 mask plus helmet, biosafety coverall plus light bulletproof vest, emergency backpack with disinfectant, flashlight, and triple packaging for transporting samples under fire. Sometimes it also means collaborating with military or civil protection structures to have access to intelligence information - where the next attack will be, which areas are temporarily safe.

In Romania, where not at war, all this seems exaggerated. But hospital regulations oblige us to prepare for exactly such scenarios. Ignoring them means leaving the laboratories exposed, and the staff - our only real capital - defenseless.

Physical security and human security are not two separate things: they form the same defense line. If the building falls, people die. When people leave, the building becomes useless. And in both cases, biological risks get out of control precisely when the medical system is at its weakest.

Today's preparation – simple fortifications, tough training, clear relocation plans – saves lives tomorrow. Not just of patients, but of those who work, day in, and day out, to save them.

3. THE REDISTRIBUTION OF THE PRIORITIES

When an armed conflict hits hard, the health system can no longer do everything at once. Resources, money, people, reagents, electricity, suddenly dwindle, and needs explode. The laboratory manager wakes up facing a harsh reality: he can no longer process all the tests as before. He must choose what really matters now, today, in the next few hours.

Redistribution of priorities becomes not an option, but the only way to save lives without letting the system completely collapse. First of all, vital emergencies come first. Blood counts for patients with massive bleeding on the front, coagulation tests for those with serious trauma, cultures from infected wounds, these do not wait.

A study of hospitals in Ukraine clearly shows during the war, the number of daily emergency admissions increased slightly (from 2773 to 2830), but laboratory services decreased dramatically – only 85% of hospitals still offered laboratory tests compared to 97% before the war [5].

This means that many routine tests were postponed or stopped, and the focus shifted to what was essential for immediate survival. Then there are nosocomial infections and antibiotic resistance, which are exploding in hospitals overcrowded with war wounded.

Laboratories must prioritize antibiograms and the rapid identification of multidrug-resistant pathogens. In Ukraine, the war created a perfect environment for the spread of resistant bacteria, medical evacuations, poor conditions, and the empirical use of antibiotics without guidance, all of which accelerated the problem [11].

Managers have learned to allocate limited resources to antimicrobial resistance testing, even if it means drastically reducing cancer screenings or routine tests for chronic diseases. Epidemiological surveillance is not disappearing, but it is changing.

Instead of broad monitoring of communicable diseases, the priority becomes the early detection of outbreaks that can overwhelm an already stretched system: dysentery in refugee camps, hepatitis in areas with contaminated water, meningitis in crowded shelters. The WHO emphasizes that in fragile and conflict settings, laboratories must support minimum essential services, including surveillance for diseases with epidemic potential, even if this means sacrificing long-term preventive programs [12].

Non-urgent diagnostic tests, such as tumor marker assays, routine hormonal evaluations, and screenings for chronic diseases, are frequently deferred or temporarily suspended in such settings. In Gaza, for example, severe shortages of reagents and equipment have led to the collapse of many laboratory services, exacerbating outbreaks of infectious diseases [1].

In Tigray, Ethiopia, access to laboratory tests for diabetes has fallen to only 4% of patients who received them before the war [4]. This shows the price paid: chronic diseases worsen, complications increase, but in the context of war, immediate survival takes precedence.

How is redistribution done in practice? Through clear triage of analyses. Many laboratories in conflict zones have introduced daily priority lists: the red category (vital emergencies, hemorrhage, septic shock), the yellow category (suspected infections in the wounded, critical epidemiological confirmations), the green category (all the rest, postponed or redirected to mobile or partner laboratories in safe areas). Mobile laboratory teams, with portable equipment, generators and biosafety cabinets, take over some of the burden, allowing the labs to focus on complex analyses.

Staff must be involved in decisions. A manager who imposes priorities from above without explanation risks demotivation and errors. Short daily discussions, as “today have 200 samples, but reagents for only 80, what do process first?”, help the team understand and accept the difficult choices.

Partnerships save the situation. Collaboration with laboratories in neighboring countries or with international networks (WHO, Red Cross, military partners) allows sensitive samples to be sent outside the conflict zone. In Ukraine, this meant coordinated medical evacuations and transfer of samples for advanced analyses [3].

But redistributing priorities also has a hidden cost: loss of capacity in the long term. When routine surveillance decreases, antimicrobial resistance grows unnoticed; When preventive screenings stop, chronic diseases explode later. That's why the plan must include a recovery strategy: once the intensity of the conflict subsides, resources are gradually reallocated back to prevention and monitoring.

In Romania, where the threat of conflict is not hypothetical, laboratory managers should practice these scenarios now. Do real-world simulations: "If 500 wounded people come in tomorrow and only have 30% of our normal reagents, what do stop? How do communicate with clinicians?"

Preparation through structured planning minimizes operational disruptions and contributes to improved patient outcomes. Redistribution of priorities represents an evidence-based approach to resource allocation and adaptive management, rather than a concession of capability. In conflict settings, laboratory services cannot address all demands simultaneously; however, they remain indispensable for meeting the most urgent clinical and epidemiological needs in real time.

4. THE MANAGEMENT OF THE MEDICAL ANALYSIS LABORATORIES – A STRATEGIC PRIORITY

In the event of an armed conflict, medical diagnostic laboratories cease to function merely as ancillary hospital services and instead become a critical component of the overall health system's resilience. These laboratories provide essential diagnostic support across disciplines such as hematology, biochemistry, microbiology, and immunology.

Without timely and accurate results from these areas, clinicians are unable to make informed treatment decisions for trauma patients, detect nosocomial infections promptly, or monitor and contain infectious disease outbreaks that commonly emerge in densely populated settings such as refugee camps or overloaded healthcare facilities.

In conflict settings, the operational continuity of medical diagnostic laboratories emerges as a national strategic priority, extending beyond routine local management. The evidence from recent armed conflicts demonstrates that, in the

absence of robust preparedness and contingency planning, laboratory functions can deteriorate rapidly, compromising health system resilience.

In Ukraine, after the invasion in 2022, many laboratories had to improvise: the power went out daily, reagents were no longer available, staff dispersed. However, where Business Continuity Plans (BCPs) were implemented, the laboratories held up better. These plans are not blank sheets of paper – they mean real redundancy: spare equipment in different locations, buffer stocks of consumables for at least 3-6 months, clear protocols for triage of analyses and mobile teams ready to take over the critical volume.

A concrete example comes from the efforts to expand PCR capacities in Yemen, where, in the midst, of war and humanitarian crisis, laboratories were strengthened for rapid molecular diagnostics, with impressive results in detecting outbreaks, even though the logistical challenges were enormous [2].

In conflict settings, priorities undergo a significant reorientation. Routine and non-urgent diagnostic tests, such as blood glucose monitoring in stable diabetic patients, annual lipid profiles, and oncological screenings, are frequently deferred or temporarily suspended.

Conversely, resources are redirected to prioritize critical and life-saving analyses, including complete blood counts for patients with massive hemorrhage, microbiological cultures from war wounds to inform antibiotic therapy, and rapid diagnostic tests for respiratory pathogens in overcrowded settings such as refugee camps.

Managers learn to triage daily: what samples are processing today with limited reagents? Which tests can be postponed without major risk? In Gaza and other areas of protracted conflict, the lack of reagents and energy led to the partial collapse of laboratory services, which aggravated infectious outbreaks and increased avoidable mortality [1].

The lesson is clear: without a strict hierarchy of priorities, the laboratory becomes ineffective exactly when it is needed most. Mobile laboratories are a strategic solution that has saved many situations. Small teams, with portable equipment (hand-held hematology analyzers, mini-PCR, solar generators), travel to the most affected areas.

In Ukraine, such mobile units have allowed on-site testing of the wounded, reducing the time to diagnosis, and avoiding the transport of samples over dangerous roads. These teams require special training: not only technical, but also security, how to operate a biosafety cabinet in a tent, under the threat of drones, or how to seal samples in triple packaging if they need to be evacuated quickly.

International partnerships help enormously: WHO, the Red Cross or laboratories in neighboring countries take over complex confirmations, send reagents or provide remote technical support. Strategic management also involves anticipating logistical risks. Supply chains are easily disrupted by conflict: blocked roads, closed ports, sanctions affecting imports.

Managers must diversify suppliers, stock strategically and have alternative plans – for example, local production of simple culture media or reuse of equipment through rigorous maintenance. In addition, communication with clinicians becomes essential: daily lists of shared priorities, short meetings in the morning to align real needs in the wards with laboratory capacity. Staff are the most precious and vulnerable resource.

In war zones, laboratory technicians and doctors work under extreme stress: delayed salaries, evacuated families, constant fear. Management must include mandatory rotations, psychological support, special insurance, and temporary relocation plans for those with families. Regular training – blackout simulations, biosecurity breaches, pressure evacuation – makes the difference between a laboratory that resists and one that collapses.

In the Romanian context, where the threat of conflict is not zero, laboratory management must integrate these lessons now. Continuity plans should be tested monthly, not annually; strategic stocks of essential reagents should be established; partnerships with EU or NATO laboratories should be strengthened for backup. Ignoring them means letting diagnosis become a lottery just when lives depend on an accurate result. Medical analysis laboratories in conflict are not a luxury – they are a strategic weapon of health defense.

Well-thought-out, proactive, and adaptable management transforms vulnerability into resilience. It's a priority that doesn't wait for a crisis to knock on the door; it's built in the quiet of today to save tomorrow.

5. RESULTS AND PROPOSALS

In Romania, the threat of armed conflict is not something abstract, it is a geopolitical reality that is feel daily, especially after the war in Ukraine reached the border. Our healthcare system, with medical analysis laboratories at its center, must move from plans on paper to concrete, tested and funded actions.

Proactive implementation of these strategies prior to any escalation is essential because the crisis could catch us unprepared. Preparation is done now, in relative silence, so as not to pay dearly later. The first essential step: the explicit integration of biosafety and biosecurity into county and national emergency plans.

Many hospital organizations and operation regulations (ROFs) already mention the obligation to be prepared for "war, disasters, terrorist attacks, social conflicts and other crisis situations". But these words often remain empty if they are not translated into chapters dedicated to biological risks.

The Ministry of Health and the Department of Emergency Situations (DSU) should oblige each hospital with a laboratory to have a separate chapter in the business continuity plan (BCP), with annual risk assessments adapted to conflict scenarios: prolonged blackout, bombings, looting, forced displacement.

The national biosafety guide for laboratories (latest available edition) needs to be urgently updated with lessons from Ukraine and the Middle East – for example, protocols for evacuating pathogen stocks in 30 minutes or controlled destruction under pressure. Second: real inter-institutional collaboration, not just on paper.

National reference laboratories (such as those at the Cantacuzino Institute or INSP) need to become coordination hubs. The Ministry of Health, DSU, the Inspectorates for Emergency Situations and the army should organize annual joint exercises, with simulations of a biological breach under war conditions: power outage, blocked roads, samples transported via alternative routes.

Partnerships with laboratories from neighboring NATO or EU countries, as Poland or Bulgaria, for backup: sending samples, exchanging reagents, mutual training. PNRR and post-2026 European funds can finance these links, including strategic stocks of portable BSL-2/3 equipment. Third: dedicated funding for resilience.

It is no longer possible with annual budgets cut to the bone. Special funds must be allocated for the modernization of laboratories: hybrid solar-diesel generators with a minimum autonomy of 72 hours, UPS systems for refrigerators with pathogens, video cameras and biometric access to sensitive areas, biosafety cabinets with backup batteries.

In addition, buffer stocks of essential reagents (for blood counts, cultures, PCR) for at least 6 months, stored in dispersed locations. The National Health Strategy 2023-2030 talks about strengthening surveillance capacity and rapid response to threats – this is exactly where laboratories come in [8].

The Ministry of Health budget should include a clear line "Preparation for conflict situations and high biological risks". Fourth: mandatory continuing education. Hospital managers, laboratory heads, technicians – all must undergo regular courses on biological risk management in a crisis context [9].

The College of Physicians, OBBCSSR and medical universities can organize practical modules: total blackout simulations, transporting samples in triple packaging on rough terrain, decontamination without running water. Trainings should be monthly in border hospitals (Constanta, Tulcea, Galati, Iasi), with the participation of the DSU and the army.

Essential personnel should have family protection plans – temporary relocation to safe areas – so that they do not leave en masse when the siren sounds. Finally, rigorous monitoring and auditing. INSP and the Control Body of the Ministry of Health should annually verify implementation: have the BCPs been tested? Are the stocks intact? Do the personnel know what to do in scenario X?

Reports should reach the government level, with real sanctions for negligence. Romania already has a good legal framework – hospital ROFs, sanitary authorization norms, biosafety guides – but consistent execution is lacking.

If invest now in these simple and practical measures, our laboratories will no longer be vulnerabilities, but robust biosafety and biosecurity measures that enhance system resilience of national health defense. It is no exaggeration to say that a well-prepared laboratory can prevent a secondary epidemic worse than the conflict itself.

The responsibility lies with all of us, all managers, DSP directors, decision-makers from the Ministry of Health. Immediate implementation of the proposed measures is recommended to strengthen laboratory preparedness.

6. CONCLUSIONS

In summary, the preceding analysis has addressed key dimensions of healthcare management in conflict settings: physical security of facilities and personnel, strategic reallocation of priorities amid resource constraints, operational continuity planning for medical laboratories, and specific preparedness recommendations tailored to the Romanian context.

A fundamental conclusion emerges from this discussion: the management of health systems during armed conflicts is not a specialized or peripheral field, but a core national security imperative. The central to this imperative are medical diagnostic laboratories, which represent a critical component of the health infrastructure. Failure to ensure their resilience and continuity can precipitate a transition from military conflict to a large-scale biological public health emergency with regional implications.

In Ukraine, evidence clearly demonstrates that even brief power outages in laboratories can pose substantial risks: refrigeration

systems fail, stored samples degrade, and the potential for accidental pathogen release increases significantly. Similarly, in Gaza and other regions affected by protracted conflict, shortages of reagents and reliable energy sources have repeatedly disrupted diagnostic capabilities, allowing infectious diseases to propagate without adequate control and contributing to elevated preventable mortality.

The key conclusion from these observations is that biosafety and biosecurity measures should not be regarded as optional administrative elements during peacetime; they represent essential protective mechanisms that must be established and maintained proactively, well in advance of any escalation into armed conflict.

A well-prepared laboratory, with monthly tested plans, with dispersed stocks, with personnel trained for extreme scenarios, does not just survive; it becomes a defense line that protects the entire population from invisible threats.

In Romania, where the border with an active war is a few dozen kilometers away, can no longer afford to treat preparation as a formality. Hospital regulations already oblige us to prepare for war and major crises, but the obligation becomes a reality only when move from words to deeds: investments in hybrid generators and resistant biosafety cabinets, tough and regular training, inter-institutional partnerships that really work, dedicated budgets for strategic stocks.

Every hospital manager, every laboratory head, every DSP director now has the duty to transform these legal obligations into concrete actions. Not tomorrow, not when it will be too late – now. Because biological risks do not negotiate truces. They don't wait for infrastructure to rebuild or for peace to return.

A single incident, an accidental breach, an opportunistic theft, a prolonged outage, can trigger a secondary outbreak more devastating than bullet wounds. And then it won't matter how well treated the wounded on the front lines if we've allowed resistant viruses or bacteria to spread unhindered.

The responsibility is clear and personal. It's not enough to say have plans. That is important to demonstrate that these plans withstand real-world simulations, that people know what to do when the power goes out and the sirens wail, that our laboratories are prepared to function even under maximum pressure.

Investments made today in laboratory preparedness, although initially appearing expensive, represent the most cost-effective preventive strategy in the long term. They avert substantially greater human suffering and economic burdens in future crises.

In essence, biosafety in medical diagnostic laboratories is not merely a technical topic confined to academic literature. It constitutes a core public health obligation.

The health system safeguards human lives, the most valuable asset, not solely through clinical interventions such as medicine and surgery, but also through sustained vigilance against biological threats that are often invisible.

In an increasingly vulnerable global environment, properly managed and resilient medical diagnostic laboratories represent one of the few reliable safeguards capable of preventing disasters from escalating to irreversible levels.

Proactive implementation is therefore essential: waiting until a crisis unfolds before recognizing the need for adequate preparation is insufficient. Rather, the necessary measures must be enacted promptly, while conditions still allow for effective action.

Survival in such contexts depends not on negotiation, but on deliberate and timely preparation. The strategic reallocation of laboratory resources constitutes a necessary and evidence-based adaptation to the severe resource limitations inherent in conflict settings.

AI DISCLOSURE

The author confirms that Grok from X.AI tools were used in the preparation of this manuscript, to identify the latest current bibliographic references. All content is solely the product of original human intellectual effort and authorship.

REFERENCES

[1] Al Bakri, D. The war on Gaza and its impact on public health: Challenges and pathways to recovery. Frontiers in Public Health. 2025. https://doi.org/10.3389/fpubh.2025.12554681 (sau PMC equivalent)

[2] Bashir, I. M., et al. Strengthening laboratories in response to outbreaks in humanitarian emergencies and conflict settings: Results, challenges and lessons from expanding PCR diagnostic capacities for COVID-19 testing in Yemen. PLOS ONE, 19(3), e0298603. 2024. https://doi.org/10.1371/journal.pone.0298603

[3] Direct Relief. Ukraine relief: Response continues into fifth year of war. (2026, February). https://www.directrelief.org/2026/02/ukraine-humanitarian-aid-2026-update

[4] Gebrehiwet, T. G., et al. War and health care services utilization for chronic diseases in rural and semiurban areas of Tigray, Ethiopia. JAMA Network Open, 6(11), e2342895. 2023. https://doi.org/10.1001/jamanetworkopen.2023.42895

[5] Haque, U., et al. A comparison of Ukrainian hospital services

and functions before and during the Russia-Ukraine war. JAMA Health Forum, 5(10), e2428720. 2024. https://doi.org/10.1001/jamahealthforum.2024.28720

[6] Hodgetts, T. J., Naumann, D. N., & Bowley, D. M. Transferable military medical lessons from the Russo-Ukraine war. BMJ Military Health, 171(2), 101-104. 2025.

[7] Houser, R. S., Koblentz, G. D., & Lentzos, F. Understanding biosafety and biosecurity in Ukraine. Health Security, 21(1), 70–80. 2023. https://doi.org/10.1089/hs.2022.0095

[8] Ministerul Sanatatii. Strategia Nationala de Sanatate 2023-2030. 2023. https://ms.ro/media/documents/Anexa_1_-_SNS.pdf

[9] Ministerul Sanatatii. Raportul de activitate pentru anul 2023. 2023. https://ms.ro/media/documents/Raport_de_activitate_pentru_anul_2023.pdf

[10] Poole, D. N., Andersen, D., Raymond, N., Parham, J. The effect of conflict on damage to medical facilities in Mariupol, Ukraine: A quasi-experimental study. PLOS Global Public Health, 5(1), Article e0003950. 2025. https://doi.org/10.1371/journal.pgph.0003950

[11] Uren, H. D., et al. Conflict zone medical evacuations catalyzing antimicrobial resistance spread and threatening regional health: A retrospective comparative observational study. Journal of Trauma and Acute Care Surgery. 2025. https://doi.org/10.1097/TA.0000000000004389

[12] World Health Organization. Quality of care in fragile, conflict-affected and vulnerable settings. 2020. https://iris.who.int/bitstream/handle/10665/337842/9789240015203-eng.pdf

[13] World Health Organization. Laboratory biosecurity guidance. 2024. https://www.who.int/publications/i/item/9789240095113

[14] World Health Organization Regional Office for the Eastern Mediterranean. Strengthening national laboratory biosafety and biosecurity policies and frameworks in the Eastern Mediterranean Region. 2025. https://applications.emro.who.int/docs/Laboratory-biosafety-biosecurity-eng.pdf

INTEGRATED DIDACTIC DESIGN MODEL FOR ENGINEER OFFICERS' TRAINING: INSIGHTS FROM INTERNATIONAL EXPERIENCE

Amil DADASHOV

Educational Institute of the Republic of Azerbaijan, Heydar Aliyev Military Institute of the National Defense University, Baku, Azerbaijan

The training of military engineering personnel is mainly carried out on the basis of military institutes, universities and academies. In addition to the specialty, military higher education institutions are aimed at instilling and developing strategic thinking, management and leadership qualities, which are the main requirements in the programs for training engineering officers. However, in the same process, they face a complex problem of integrating serious military skills training with academic education. This article analyzes existing research and international experiences and proposes an integrated joint program-didactically designed educational model aimed at bridging the persistent gap between the two training directions - specialty and military skills. The model includes pedagogical approaches, curriculum reform initiatives and the integration of new technologies such as computer-based learning environments. This work, based on the comprehensive and result-oriented application of didactic approaches in specialty programs, also synthesizes the best practices from international military education systems. The analysis highlights the importance of learning, knowledge transfer, and outcome-oriented training, especially in the context of the application of advanced military technologies, as well as the need for the practical application of scientific reasoning appropriate to complex security environments in the performance of challenging military tasks. The proposed model emphasizes a holistic approach to the development of engineer officer training, ensuring that academic knowledge, technology, and practical military skills reinforce each other, thereby increasing operational effectiveness and adaptability in modern war scenarios.

Key words: *Military education, engineer officer training, integrated didactic design model.*

[1] ORCID ID: 0000-0002-9379-0798, e-mail: amilodas@gmail.com

1. INTRODUCTION

Against the backdrop of conflicts occurring around the world, the impact of ever-developing technology is characterized by civil, military operations and hybrid threats. This requires that young officers being trained in higher military education systems not only have academic education and exceptional military skills, but also deep strategic thinking abilities, management and leadership qualities, as well as the preparation of military personnel with (Hornstra et al., 2023; Hornstra et al., 2024; Loishyn et al., 2024). Traditional military education systems, which are often divided into individual skills training and academic education paths in military specialties, which are often implemented in parallel, often have difficulty in achieving a comprehensive and successful integration of their components (Hornstra et al., 2023; Hornstra et al ., 2024). This creates difficulties in developing officers who can cope with the multifaceted problems of modern global security.

The article analyzes the current didactic designs in military education, using international experience and the latest pedagogical innovations, and explores the solution to this problem. The aim is to identify an integrated program model for training knowledgeable and skilled military engineer officers who can adapt to modern technology more quickly in order to effectively bridge the gap between practical military training and academic intellectual development.

2. METHODOLOGY

This study applied a mixed, qualitative and theoretical-analytical research design based on a systematic integrative review of international scientific literature, framework documents and institutional documents related to didactic design in military disciplines and higher military education. The main objective of the study is to explore various international experiences, conceptual models and pedagogical reforms in a consistent analytical approach that explains the possible application of didactic design for engineer training in modern military education systems. The data necessary for the analysis were collected during January 2026.

The analysis of scientific articles and academic literature was systematically obtained from resources indexed in authoritative databases such as "Web of Science" and "Scopus", and was supplemented with officially published NATO doctrines and policy documents in order to ensure both academic rigor and institutional credibility of the analytical framework. The search process was carried out using the keywords and phrases "military education", "engineer officer

training", "integrated didactic design model", "international experience" and "NATO Defense education enhancement program (DEEP)". The resulting primary data were refined, numerous articles were reviewed, and data from relevant sources were collected and analyzed. Rather than conducting empirical measurements, the study focused on conceptual clarification, comparative interpretation, and model synthesis, in line with existing approaches in professional military education (PME) research and instructional design. The analytical part consists of 25 peer-reviewed journal articles, conference proceedings, and official NATO policy documents published between 2013 and 2026, covering a sufficiently broad period to provide both historical depth and contemporary relevance.

The sources for the study were selected from the following areas: military academies and higher military education institutions, didactic design models, instructional systems design (ISD) and competency-based education, NATO-aligned educational frameworks and reform initiatives, digital and technology-enhanced military pedagogy (including multimedia, operational games, role-playing simulations and AI-enabled training systems), and ethical and value-based dimensions of military education (especially AI and autonomous systems). To ensure analytical rigor and transparency, the study applied specific inclusion and exclusion criteria. Inclusion criteria included a clear focus on military education or professional military education (PME), direct links to didactic design or pedagogical frameworks, discussion of international and NATO-aligned practices, and expert opinion or official institutional authorship.

Exclusion criteria included studies that were limited to civilian higher education and had little or no relevance to military education, purely technical manuals without pedagogical analysis, and opinion-based materials without methodological justification. The analytical procedure followed a four-step qualitative synthesis process: conceptual mapping, which identified the contribution of each source to didactic design; thematic coding, in which recurring concepts were grouped into categories such as integrated academic skills, competency-based design, and immersive technologies; comparative interpretation, in which thematic categories were compared across national and institutional contexts (particularly NATO member states, including the Turkish experience); and finally, model synthesis, in which an "integrated didactic design model" for military subjects was formulated, combining pedagogical tools, didactic mechanisms, and learning outcomes.

Methodologically, the study is based on three complementary frameworks: Instructional systems design (ISD), which provides a structural logic for curriculum development; Competency-based military education (CBME), which focuses on transferable competencies rather than content accumulation; and Technology-based pedagogy, which encompasses digital learning environments, AI-assisted instruction, and ethical governance.

To enhance analytical validity, the research was based only on peer-reviewed and institutionally authoritative sources. This approach, supported by transparent selection criteria and systematic thematic coding, provides a solid theoretical foundation for future empirical research and academic program, as well as educational program or training course experiments in military academies, and provides scientific justification for a didactic model that meets modern requirements for the training of engineer officers.

3. BACKGROUND AND CHALLENGES IN MILITARY DIDACTIC DESIGN

Historically, military education programs and training courses have focused on rigorous skills training, especially in combat, logistics, and operational procedures. In the basic and advanced stages of officer training, the program has aimed to simultaneously instill both academic - basic engineering education, and military management skills education - strategic thinking, leadership theory, and a broader geopolitical understanding (Hornstra et al., 2023; Hornstra et al., 2024; Loishyn et al., 2024; Dragomir, 2024). However, in many cases, the implementation of such parallel learning paths often occurs in an unintegrated manner, which creates a challenge that can hinder the development of a unified officer, creating inconsistencies and professional training. This challenge is particularly evident in military education programs where both directions are important but require greater integration.

A key need is that limited attention has been paid to didactic design of education as a specific mechanism for linking military training and academic education in the study of different models (Hornstra et al., 2023; Dragomir, 2024). If this challenge is addressed, the implications are significant given the increasing demand for officers with strategic thinking skills who can play roles at all levels in modern conflict zones, especially in complex operational environments. Furthermore, pedagogical paradigms for officer training have historically clashed, particularly in post-Soviet countries, where the shift from a "performer" mindset to a leadership-oriented approach is still ongoing, consistent with international best

practices (Loishyn et al., 2024). The ongoing military education reforms seek to align with the didactic principles of NATO countries, move away from Soviet-era traditions, and develop a leader-centered approach (Iskandarov & Gawliczek, 2019; North Atlantic Treaty Organization, 2025; NATO, 2013; Enstad & Hagen, 2026).

3.1. International experiences and pedagogical innovations

International military education systems are actively exploring innovative didactic approaches to integrate skills training and academic learning. As noted, military education reform efforts are strongly influenced by NATO best practices and focus on didactic principles that promote a holistic approach to personnel training (Mazurenko, 2024). These reforms involve adapting methodological systems to develop leadership qualities rather than just performance (Loishyn et al., 2024). The goal is to optimize education and training processes within NATO missions to enhance operational capabilities, as highlighted by analytical approaches that combine literature reviews and official document analysis [10]. The integrated didactic design model justifies a structured approach to training, while specifically addressing the need to bridge the gap between military skills training and academic education in military higher education institutions (Hornstra et al., 2024). The model that includes such an approach proposes a purposeful integrated development of curricula to ensure that military skills acquisition and academic learning are mutually reinforcing, rather than separate. According to Bodescu, A. (2024), horizontal and vertical integration of disciplines such as the Law of Armed Conflict (LOAC) is also important to ensure that non-legal practitioners, such as interns, master and apply these principles in real-life scenarios.

3.2. Integration of computer-oriented learning environments

The widespread application of technology, as evidenced by recent military operations and conflicts, and the acceleration of technological development have necessitated the integration of computer-oriented learning environments (COLE) into the curricula of military higher education institutions. Experience shows that COLEs, which are improved and didactically designed in accordance with military development, are designed to optimize pedagogical methods, at the same time increase the skill sets of the emerging officer corps and ensure the effectiveness of training by using information technologies (Rybchuk & Yaroshov, 2024). These environments provide various hybrid training - simulated, scenario-based training exercises on various topics and in any situation,

providing access to data analysis and distance professional development. Within the framework of didactic application, COLE technologies model the training module close to the real environment, forming an educational, motivating and effective training environment. The application of COLE technologies also achieves the desired didactic results in the military educational environment by modeling them close to real operational conditions.

Digital pedagogical tools, which were widely used during the COVID-19 pandemic, have been improved over time and adapted to military training systems. Multimedia technologies, task games, role-playing games and artificial intelligence-based learning assistance systems act as key components of this transformation. Specialized pedagogical tools that are already being applied in many training and education systems adapted from the experience of the COVID-19 pandemic are being rapidly developed.

3.3. Targeted didactic design model based on COLE technologies

Analyses show that (Table 1.) COLE technologies have various systematized didactic potentials in military education.

Table 1. Didactic potential of COLE technologies in military education.

INTEGRATED DIDACTIC DESIGN MODEL FOR
ENGINEER OFFICERS' TRAINING:
INSIGHTS FROM INTERNATIONAL EXPERIENCE

Amil DADASHOV

Educational Institution of the Republic of Azerbaijan, Heyd
Institute of the National Defense University, Bak

The training of military engineering per

The training of military engineering personnel is mainly carried out on the basis of military institutes, universities and academies. In addition, the spec
military higher education institutions in milit
thinking, management and leadership qualitie

Source. Prepared by the author (based on various sources).

The didactic application possibilities of existing COLE technologies in international practice (Figure 1.) can be modeled as follows:

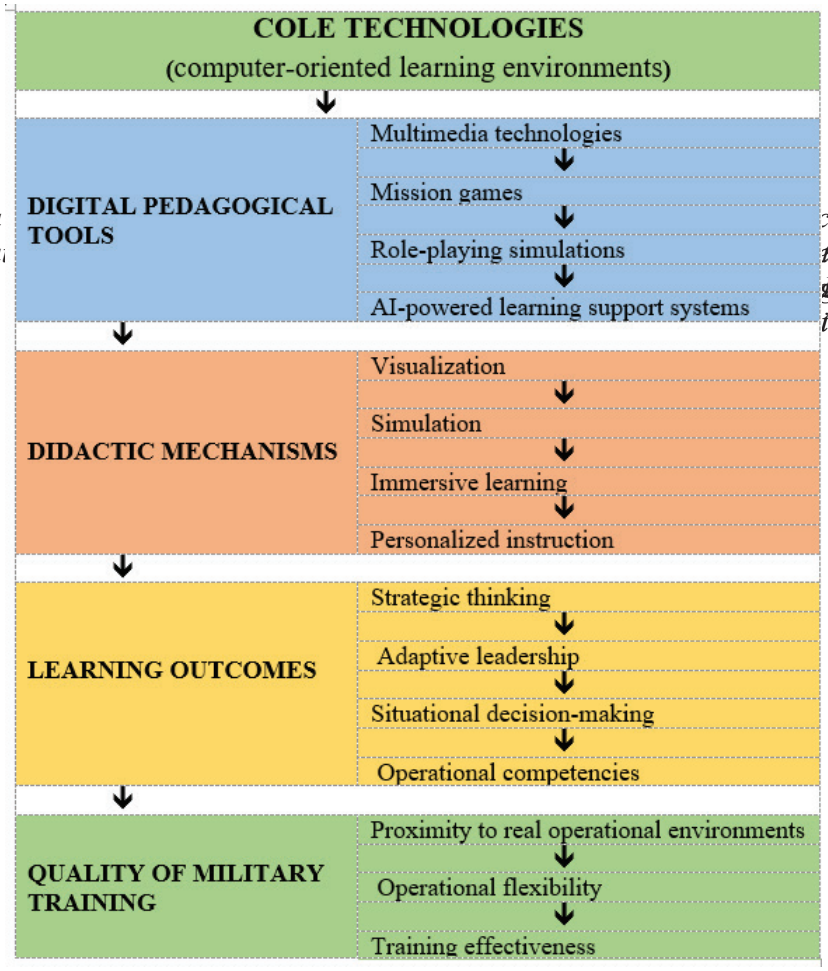

Fig. 1. Conceptual model of didactic design in military education based on COLE
Source. Prepared by the author

Note: The model illustrates the transformation of COLE technologies into digital pedagogical tools, which activate specific mechanisms leading to enhanced learning outcomes and improved quality of military training.

The proposed didactic model visualizes the complex relationships between curriculum design, technology integration, leadership training, and assessment mechanisms, as well as presents implementation stages and expected learning outcomes. This exemplary model aims to improve the current military engineering training experience and train personnel who meet the requirements of modern warfare.

The proposed didactic model consists of several key interrelated components:

Curriculum Design: Curriculum design is based on the methodologies of Instructional Systems Design (ISD) and Competency-Based Military Education (CBME). This approach involves a comparative analysis of previous military engineering training curricula with engineering disciplines and credit systems, as a result of which existing gaps and training needs are identified. The curriculum is focused on developing the knowledge, skills, and competencies necessary for soldiers' specific roles in the military. It includes modules based on practical work, laboratory exercises, and real-world problem solving.

Technology Integration: Technology integration involves enriching the learning process using technologies of the Custom Educational Environments (COLE). This integration includes multimedia technologies, mission games, role-playing games and artificial intelligence-based learning support systems. COLE technologies create immersive and interactive learning environments in the teaching-learning process, simulate military scenarios and offer personalized learning paths. This approach provides a transition from traditional teaching methods to digital pedagogical tools.

Leadership Training: Leadership training is central to military education. This component is aimed at developing critical thinking, decision-making, teamwork and ethical standards in future military leaders within the framework of CBME. Leadership training includes the practical application of theoretical knowledge, real-life leadership scenarios and teaching the principles of effective management in various military situations.

Assessment Mechanisms: Assessment mechanisms are closely related to the principles of CBME and provide a consistent and comprehensive measurement of the competencies of trainees. These mechanisms include both formative (to provide feedback throughout the training process) and summative (to

measure competencies at the end of training) assessment methods. Technology-based assessment enhances objectivity, tracks individual achievement, and allows for ongoing evaluation of program effectiveness.

The model's key relationships and structural flow relationships are based on the following principles:

ISD and CBME: Underpin curriculum design, leadership training, and assessment mechanisms. These approaches ensure that training is purposeful and results-oriented.

Technology-Curriculum Integration: COLE technologies are designed as an integral part of the curriculum, supporting the effective delivery of training content and the creation of interactive learning experiences.

Assessment Feedback: Assessment mechanisms continuously monitor the effectiveness of the curriculum, technology integration, and leadership training and provide feedback for adjustments as needed.

Note: The structural flow of the model reflects a continuous cycle, starting from the analysis of training needs, to the design of an appropriate curriculum, the integration of technologies, the implementation of training, and finally the evaluation of results.

As for the implementation stages, the implementation stages of the proposed didactic model are structured in accordance with the ISD principles:

Analysis: A comprehensive analysis of training needs, target audience characteristics, and existing constraints. This also includes identifying gaps in the military engineer training curriculum.

Design: Preparation of training objectives, teaching methods, assessment strategies, and a plan for integrating COLE technologies into the curriculum.

Development: Creation or adaptation of teaching materials, digital resources based on COLE technologies, and assessment tools.

Implementation: Implementation of the developed curriculum and training programs in military educational institutions.

Evaluation: Continuous assessment of the effectiveness of the training program, student achievements, and the overall success of the model, and collection of data for future improvements.

The expected educational outcomes from the implementation of this model are to increase the ability of military personnel to effectively respond to modern challenges.

The main outcomes include:

Higher military competencies: Deepening of knowledge and skills in the field of military engineering.

Critical thinking and problem solving skills: Strengthening the

ability to think analytically and find effective solutions in complex military scenarios.

Effective decision making: Development of the ability to make sound and timely decisions in stressful situations.

Adaptation and flexibility: Rapid adaptation to the changing military environment and technological innovations.

Adherence to military ethical norms: Full compliance with professional ethics and military discipline standards.

These educational outcomes will contribute to both the development of individual military personnel and the effectiveness of the army as a whole.

3.4. Conceptual diagram description

The diagram below (Figure 2.) visually presents the main components of the proposed didactic model, their interrelationships, methodological foundations, application stages, and expected educational outcomes.

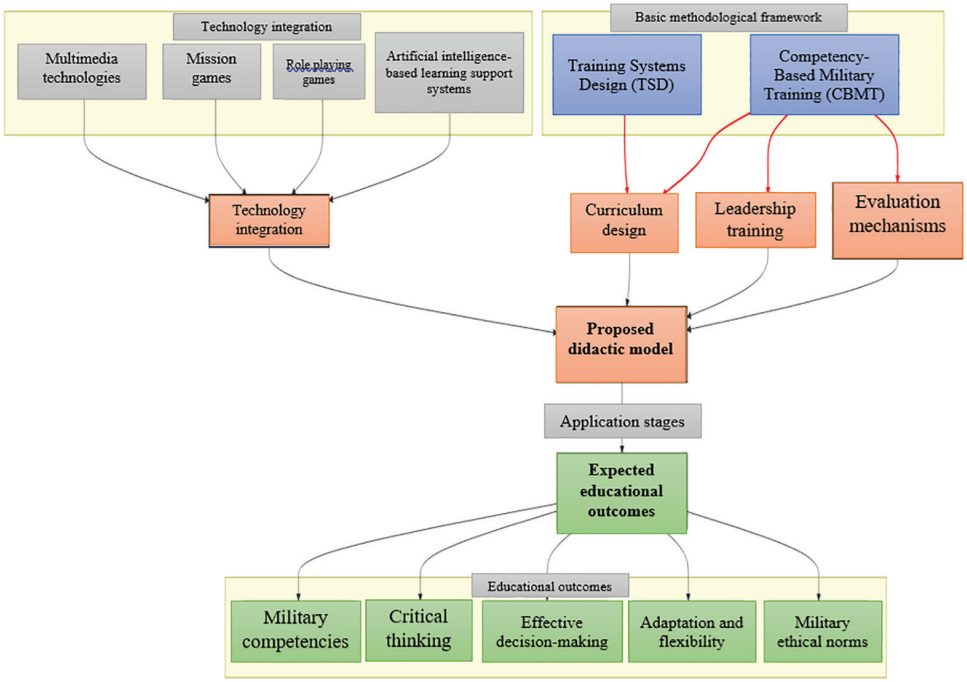

Fig. 2. Conceptual diagram of the relationships between the main components of the proposed didactic model
Source. Prepared by the author

In the diagram:

• The core methodological framework (Instructional Systems Design (ISD) and Competency-Based Military Education (CBME)) represents the fundamental principles of the model.

• Curriculum design, Technology integration, Leadership training and Assessment mechanisms are the main pillars of the model and flow in an interconnected manner into the center of the proposed didactic model.

• Within the technology integration block, specific types of COLE technologies (Multimedia, Mission Games, Role Playing, Artificial Intelligence-Based Training Support) are detailed.

• The implementation process of the model progresses towards the Expected Learning Outcomes through the Implementation Stages axis.

• The expected learning outcomes, in turn, include the defined military competencies and skills.

3.5. Ethical considerations and Aİ integration

Research has shown that the availability of new technologies, particularly the ethical implications of Artificial Intelligence (AI), is central to military didactic design (Azafrani & Gupta, 2023; Taddeo et al., 2024). Integrating responsible AI principles and practices into defense institutions requires specific ethical guidelines for the development and deployment of AI systems in military contexts. This requires new pedagogical approaches to address complex issues such as algorithmic bias, autonomous weapon systems, and the inhumane aspects of modern warfare. A values-based approach that incorporates the views of large stakeholder groups is used for the design of military autonomous systems (Boshuijzen-van Burken et al., 2024). Similarly, the Law of Armed Conflict (LOAC) requires an integrated curriculum approach to ensure that trainees, including non-lawyers, effectively understand and apply LOAC principles in real-world operational scenarios. This necessitates didactic strategies that go beyond mere legal instruction and move toward practical correlation with real-world situations (Bodescu, 2024).

4. DEVELOPMENT OF DIDACTIC PRINCIPLES AND PROFESSIONAL DEVELOPMENT

The theoretical foundations of didactic principles in military education stem from broader concepts within general subject didactics and focus on content-based teaching and learning in specific academic fields (Dadaşov, 2024; Ruslan & Andrii, 2024). This framework guides efforts to improve the didactic design of engineering education for both faculty and students in military institutions. The development of

didactic principles-based design among faculty and students in higher military education institutions is also essential, and the structure and features of a well-defined curriculum for effective instruction enhance the capabilities of didactic design, as well as the overall quality and future effectiveness of instruction (Dadaşov, 2024).

The evolution of instructional system development (ISD) models, such as those in the US Air Force, demonstrates a continued commitment to improving pedagogical approaches in military training and underscores the long-standing emphasis on systematic instructional design procedures (Yang et al., 2024). Modern management approaches are also applied to the management of the activities of military pedagogical personnel, focusing on optimal methods for employees in dynamically changing security environments (Meyer et al., 2024).

5. PEDAGOGICAL EVALUATION AND TRANSFER OF TRAINING

A comprehensive review of international practices and pedagogical innovations highlights a clear and compelling need for integrated instructional design in military education. The traditional separation of skills training and academic education is increasingly inadequate to prepare officers to deal with the complexities of modern warfare (Hornstra et al., 2023; Hornstra et al., 2024). Evidence from various military academies and educational reforms suggests that successful integration requires a multidisciplinary approach. It is essential to adopt curricula that clearly align learning objectives across both practical and academic modules (Hornstra et al., 2024).

This includes not only vertical integration, which ensures the progressive development of knowledge and skills over time, but also horizontal integration, which fosters interdisciplinary connections that reflect the multidisciplinary nature of modern military operations (Bodescu, 2024). For example, integrating the principles of the Law of Armed Conflict (LOAC) into various operational courses, rather than treating them as isolated legal topics, allows trainees to relate these principles to real-world situations, thereby improving their applicability in the field (Bodescu, 2024).

Technological advances offer significant opportunities for improving instructional design. Computer-based learning environments (COLEs), multimedia tools, task games, and role-playing simulations provide immersive and efficient methods for applying practical skills and developing strategic thinking (Rybchuk & Yaroshov, 2024; Truong et al.,

2024; Karadimas, 2025; Horiacheva & Ryzhykov, 2024). These tools, especially task games, can significantly reduce the risks and costs associated with traditional training while fostering collaboration and strategic thinking (Karadimas, 2025). The emerging use of AI-powered learning assistance systems promises to enable personalized learning and effective learning, adapt to individual learning paces, and provide immediate feedback (Chamnankij et al., 2025).

However, the integration of advanced technologies, especially AI, requires a strong focus on ethical considerations (Azafrani & Gupta, 2023; Taddeo et al., 2024). Military instructional design must proactively address the ethical implications of autonomous systems, algorithmic bias, and the impact of technology on human rights (Taddeo et al., 2024; Boshuijzen-van Burken et al., 2024). The inclusion of discussions, case studies, and simulations focused on responsible AI development and deployment is essential for developing ethically informed leaders. The role of educators is central to this integrated approach. Continuous professional development for military educators is essential, focusing on modern didactic principles, the use of effective technologies, and interdisciplinary teaching strategies (Dadaşov, 2024; Ruslan & Andrii, 2024). The development of a strong "didactic culture" characterized by structured and effective teaching informed by systems-based instructional development (SSD) models is essential for improving teaching quality and ensuring pedagogical relevance (Ozogul 2023).

Finally, robust assessment and feedback mechanisms must be implemented to validate the effectiveness of these integrated models (Meyer et al., 2024). It is important to assess not only knowledge acquisition, but also the transfer of learning into practical application and the development of leadership skills. Feedback from operational commanders and trainees can provide invaluable insights for improving didactic approaches and reinforces the importance of a continuous development cycle (Hornstra et al., 2024). Intention-based leadership can also be incorporated into feedback loops to further enhance leadership development by empowering subordinates and encouraging independent decision-making (Dragomir, 2024).

6. DISCUSSION: TOWARDS AN INTEGRATED INSTRUCTIONAL DESIGN MODEL

A comprehensive review of international practices and pedagogical innovations highlights a clear and compelling need for

integrated instructional design in military education. The traditional separation of skills training and academic education is increasingly inadequate to prepare officers to deal with the complexities of modern warfare (Hornstra et al., 2023; Hornstra et al., 2024). Evidence from various military academies and educational reforms suggests that successful integration requires a multidisciplinary approach. It is essential to adopt curricula that clearly align learning objectives across both practical and academic modules (Hornstra et al., 2024). This includes not only vertical integration, which ensures the progressive development of knowledge and skills over time, but also horizontal integration, which fosters interdisciplinary connections that reflect the multidisciplinary nature of modern military operations (Bodescu, 2024). For example, integrating the principles of the Law of Armed Conflict (LOAC) into various operational courses, rather than treating them as isolated legal topics, allows trainees to relate these principles to real-world situations, thereby improving their applicability in the field (Bodescu, 2024).

Technological advances offer significant opportunities for improving instructional design. Computer-based learning environments (COLEs), multimedia tools, task games, and role-playing simulations provide immersive and efficient methods for applying practical skills and developing strategic thinking (Rybchuk & Yaroshov, 2024; Truong et al., 2024; Karadimas, 2025; Horiacheva & Ryzhykov, 2024). These tools, especially task games, can significantly reduce the risks and costs associated with traditional training while fostering collaboration and strategic thinking (Karadimas, 2025). The emerging use of AI-powered learning assistance systems promises to enable personalized learning and effective learning, adapt to individual learning paces, and provide immediate feedback (Chamnankij et al., 2025).

However, the integration of advanced technologies, especially AI, requires a strong focus on ethical considerations (Azafrani & Gupta, 2023; Taddeo et al., 2024). Military instructional design must proactively address the ethical implications of autonomous systems, algorithmic bias, and the impact of technology on human rights (Taddeo et al., 2024; Boshuijzen-van Burken et al., 2024). The inclusion of discussions, case studies, and simulations focused on responsible AI development and deployment is essential for developing ethically informed leaders. The role of educators is central to this integrated approach. Continuous professional development for military educators is essential, focusing on modern didactic principles, the use of effective technologies, and interdisciplinary

teaching strategies (Dadașov, 2024; Ruslan & Andrii, 2024). The development of a strong "didactic culture" characterized by structured and effective teaching informed by systems-based instructional development (SSD) models is essential for improving teaching quality and ensuring pedagogical relevance (Ozogul 2023). Finally, robust assessment and feedback mechanisms must be implemented to validate the effectiveness of these integrated models (Meyer et al., 2024). It is important to assess not only knowledge acquisition, but also the transfer of learning into practical application and the development of leadership skills. Feedback from operational commanders and trainees can provide invaluable insights for improving didactic approaches and reinforces the importance of a continuous development cycle (Hornstra et al., 2024). Intention-based leadership can also be incorporated into feedback loops to further enhance leadership development by empowering subordinates and encouraging independent decision-making (Dragomir, 2024).

7. CONCLUSIONS

Didactic design in military disciplines is undergoing a transformation due to the complexity of modern warfare and rapid technological advances. International experiences reveal a shared commitment to move beyond traditional, isolated educational approaches towards integrated models that seamlessly integrate military skills training with academic education. By prioritizing didactic instructional design as a critical foundation, embracing computer-based learning, integrating ethical frameworks for emerging technologies such as artificial intelligence, and utilizing innovative pedagogical tools, military academies can produce engineering officers who are not only technically proficient but also strategically intelligent, ethically grounded, and adaptable leaders. This integrated approach to didactic design is essential for enhancing the operational capabilities of armed forces and ensuring their effectiveness in an ever-evolving global security landscape. Future research should focus on regular empirical studies to study and enrich the pedagogical impacts of emerging technologies such as academically integrable, advanced, digital, and artificial intelligence, to validate the effectiveness of these integrated models in various military contexts.

DATA AVAILABILITY STATEMENT

Note for the data availability statement.

"All data are included in the manuscript.".

AI DISCLOSURE

The author acknowledge the use of the following generative AI tools to assist in the preparation of this manuscript: ChatGPT. This tool was used solely for language editing and structural suggestions, under the complete control and responsibility of the authors. All AI-assisted content was critically reviewed and revised by the authors, who accept full responsibility for the accuracy and integrity of the final version.

REFERENCES

Hornstra, S., Hoogenboezem, J., Durning, S., & van Mook, W. (2023). Instructional design linking military training and academic education for officer cadets: A scoping review. Journal of military and strategic studies, 22(4). https://jmss.org/article/view/76275/57091

[2] Hornstra, S. P. A., Durning, S. J., Hoogenboezem, J. A., & van Mook, W. N. K. A. (2024). Closing the gap between skills training and academic education at a military academy: An integrated instructional design model. Ukrainian journal of educational studies and information technology. https://doi.org/10.32919/uesit.2024.01.01

[3] Loishyn, A., Kucheriavyi, A., Vanovska, I., & Pyrogov, K. (2024). Characteristics of the state of implementation of foreign experience in teaching academic disciplines at the military institute of Taras shevchenko national university of kyiv. Visnyk Taras Shevchenko national university of kyiv military-special sciences, 57, 15–25. https://doi.org/10.17721/1728-2217.2024.57.15-25

[4] Dragomir, C. (2024). Empowering leaders through intent – based leadership: a transformative approach in military education. Review of the air force academy, 22(2), 58–67. https://doi.org/10.19062/1842-9238.2024.22.2.8

[5] Iskandarov, Khayal, & Gawliczek, Piotr. (2019). The South Caucasus and NATO's Defence Education Enhancement Programme. Retrospective Analysis. Social Development & Security, 9(5), 3–14. https://doi.org/10.33445/sds.2019.9.5.1

[6] North Atlantic Treaty Organization. (2025). Defence Education Enhancement Programme (DEEP). NATO Official Site. https://www.nato.int/en/what-we-do/partnerships-and-cooperation/defence-education-enhancement-programme-deep

[7] NATO. (2013). Generic Officer Professional Military Education (PME) Reference Curriculum. NATO Documents. https://www.nato.int/content/dam/nato/webready/documents/deep/deep-generic-officer-pme-reference-curr-en.pdf

[8] Enstad, K., & Hagen, A. M. (2026). No common understanding? A scoping review of professional military education in the twenty-first century. Scandinavian Journal of Educational Research, 70(1), 80–100. https://doi.org/10.1080/00313831.2025.2459408

[9] Mazurenko, L. (2024). Status, problems and prospects of the reform of didactic principles of military

education in ukraine. Cherkasy university bulletin pedagogical sciences, 4, 17–24. https://doi.org/10.31651/2524-2660-2024-4-17-24

[10] Pînzariu, S., & Pînzariu, A.-I. (2024). Operational efficiency through optimization of education and training processes in NATO missions. International conference knowledge-based organization. https://doi.org/10.2478/kbo-2024-0019

[11] Рибчук, О., Ярошов, М., Rybchuk, O., & Yaroshov, M. (2024). Pedagogical model for teaching general military disciplines in military higher education institutions under a computer-oriented learning environment. Visnyk Taras Shevchenko national university of Kyiv military-special sciences, 58, 32–38. https://doi.org/10.17721/1728-2217.2024.58.32-38

[12] Truong Quoc Hung, Truong Quoc Hung, Vu Minh Hoang, Vu Minh Hoang, Tran Thi Hai Anh, Tran Thi Hai Anh, Luong Phan Quang, Luong Phan Quang, & Nguyen Thi Lan, Nguyen Thi Lan. (2024). Utilizing multimedia technology to create educational tools for teaching national defense and security. Tạp Chí Khoa Học Trường *Đại* Học Quốc Tế Hồng Bàng, 6. https://doi.org/10.59294/hiujs.vol.6.2024.633

[13] Karadimas, N. V. (2025). Reflections on traditional and serious games-based training in military academies and the army. The journal of defense modeling and simulation applications methodology technology. https://doi.org/10.1177/15485129251385264

[14] Horiacheva, K., & Ryzhykov, V. (2024). Leveraging of role-play games in military training cadets within the ongoing conflict in Ukraine. Bulletin of carol i national defence university, 24(1), 77–88. https://doi.org/10.53477/2284-9378-24-17

[15] Chamnankij, P., Charoenchaiprakit, K., & Naowanich, E. (2025). Development of an intelligent learning assistance system for military curriculum using python and generative AI. 2025 10th International STEM education conference (iSTEM-Ed). https://doi.org/10.1109/iSTEM-Ed65612.2025.11129378

[16] Azafrani, R., & Gupta, A. (2023). Bridging the civilian-military divide in responsible AI principles and practices. Ethics and information technology, 25(2), 34. https://doi.org/10.1007/s10676-023-09693-y

[17] Taddeo, M., Blanchard, A., & Thomas, C. (2024). From AI ethics principles to practices: a teleological methodology to apply AI ethics principles in the defence domain. Philosophy & technology. https://doi.org/10.1007/s13347-024-00710-6

[18] Boshuijzen-van Burken, C., Spruit, S., Geijsen, T., & Fillerup, L. (2024). A values-based approach to designing military autonomous systems. Ethics and information technology. https://doi.org/10.1007/s10676-024-09789-z

[19] Bodescu, A. (2024). Horizontal and vertical integration of loac into military academy curriculum. International conference knowledge-based organization. https://doi.org/10.2478/kbo-2024-0003

[20] Dadaşov, A. (2024). Possibilities of improving the level of didactic design of engineering training of professors and students at a military institute. Scientific works, 91(2), 45–51. https://doi.org/10.69682/azrt.2024.91(2).45-51

[21] Ruslan, K., & Andrii, P. (2024). Didactic culture of a teacher of a higher military educational institution: structure and characteristics. *Проблеми правоохоронної та освітньої діяльності*, 1(1), 46–52. https://doi.org/10.59226/3041-1971.1.2024.46-52

[22] Yang, M., Lowell, V. L., Exter, M., Richardson, J., & Olenchak, F. R. (2024). Transfer of training and learner attitude: a mixed-methods study on learner experience in an authentic learning program. Human Resource Development International, 28(3), 346–370. https://doi.org/10.1080/13678868.2024.2361178

[23] Meyer, C. O., Van Osch, T., & Reykers, Y. (2024). From EU battlegroups to Rapid Deployment Capacity: learning the right lessons? International Affairs, 100(1), 181–201. https://doi.org/10.1093/ia/iiad247

[24] V. Klachko, S. Bilyavets, A. Didenko. (2022). Current State, Problems, and Prospects for Transforming Military Education in the Context of Implementing NATO Standards. Collection of Scientific Works of the National Academy of the State Border Guard Service of Ukraine. Series: Pedagogical Sciences, № 1, pp. 90–104. https://doi.org/10.32453/pedzbirnyk.v28i1.958

[25] Ozogul, G. (2023). The evolution of the instructional system development model in the united states air force. Tech trends, 68(2), 263–274. https://doi.org/10.1007/s11528-023-00867-5

CIANGSANA WAREHOUSE EXPLOSION: CHEMICAL DEGRADATION AND ZONING COMPLIANCE ANALYSIS

Anisa SETIANINGSIH[1], Heri Budi WIBOWO[2], Mas Ayu Elita HAFIZAH[3]

Weapon Technology, Faculty of Defense Engineering and Technology, Indonesia Defense University, Bogor, Indonesia

The March 30, 2024 explosion at Ciangsana Regional Ammunition Warehouse (Gudmurah Kodam Jaya) revealed critical failures in expired ordnance management within densely populated areas. This study integrates chemical stability analysis of TNT/RDX with UN SaferGuard-based spatial risk assessment and JUKLAK04VI/2010 regulatory evaluation. Analysis confirms the explosion resulted from methyl migration in aged TNT forming friction-sensitive crystals after 10+ years tropical storage (27°C, 78%RH), accelerated 2.5x vs temperate conditions. RDX exhibited autocatalytic NOx generation. Spatial analysis using QGIS 3.44.8 reveals 145.1m distance to nearest residences, 83.7% below UN SaferGuard 892m requirement for 65-ton explosive load ($Z \times \sqrt[3]{M}$ principle). Key findings identify three systemic failures: (1) procedural negligence violating 10-year disposal mandate; (2) thermal-induced TNT crystal formation; (3) zoning violations allowing residential encroachment from 2003-2025. Policy recommendations include mandatory environmental monitoring, defense map integration into OSS licensing, and dynamic safety zoning. This incident exemplifies chemical-spatial risk convergence requiring integrated ammunition lifecycle management for urbanizing nations.

Key words: *Ammunition Safety, TNT Methyl Migration, Spatial Risk Assessment, Ciangsana Explosion, UN SaferGuard*

[1] ORCID ID: N/A, email: anisasetia13.as@gmail.com
[2] ORCID ID: N/A
[3] ORCID ID: N/A

1. INTRODUCTION

The explosion of the ammunition warehouse in Ciangsana, Bogor, on March 30, 2024, stands as a significant event in the context of public safety and military security in Indonesia. Explosions in ammunition depots are not unprecedented globally, they often result from improper storage, lack of effective safety procedures, and insufficient personnel training. However, the Ciangsana incident distinguishes itself by revealing a complex interplay between technical failure and spatial mismanagement that is rarely discussed in a single framework.

Existing literature on ammunition safety remains largely fragmented. Technical studies, such as those by Akhavan (2022), primarily focus on the chemical stability of explosives like TNT and RDX under controlled laboratory conditions, often overlooking the accelerating effects of tropical environmental factors, specifically high temperature and humidity, found in real-world storage. Research on spatial planning in the Jabodetabek region, including studies by Murtadho et al. (2022) and Rustiadi's previous work on land use consistency (Kurniati, Rustiadi, & Baskoro, 2015), has consistently identified weaknesses in zoning enforcement and uncontrolled urban expansion. Nevertheless, these spatial analyses do not address the chemical decomposition dynamics of hazardous materials stored within encroached-upon facilities, leaving a critical gap in integrated risk assessment

This study bridges that gap through a multidisciplinary approach. It aims to integrate three critical perspectives: (1) the chemical dynamics of expired ammunition in tropical climates, (2) a critical evaluation of regulatory implementation (JUKLAK/04/VI/2010), and (3) risk-based spatial analysis. By connecting field findings such as the accumulation of unstable gases in expired munitions with the reality of uncontrolled urban expansion, this research offers a holistic evaluation of the safety failures at Ciangsana. The findings provide evidence-based policy recommendations for safer ammunition management and zoning enforcement in densely populated developing nations.

2. LITERATURE REVIEW

This literature review is organized into three analytical themes central to understanding the Ciangsana incident: (1) the chemical degradation mechanisms of high explosives, (2) ammunition storage safety management practices and regulatory frameworks, and (3) spatial planning principles for hazardous facilities and the challenges of urban encroachment.

2.1 Chemical Degradation of High Explosive

High explosives such as Trinitrotoluene (TNT) and Research Department Explosive (RDX) undergo chemical decomposition over time, a process significantly accelerated by environmental factors. According to Kementerian Pertahanan (2010) in JUKLAK/04/VI/2010, ammunition serviceability is generally capped at ten years from production, after which the operational risk profile changes drastically due to chemical instability.

The decomposition of TNT follows an exothermic pathway that releases hazardous gases including carbon monoxide (CO) and nitrogen (N_2). Akhavan (2022) confirms that as TNT ages, the instability of its nitro groups makes the material increasingly sensitive to thermal triggers, significantly elevating the risk of accidental detonation. Research on environmental factors affecting explosive degradation has demonstrated that humidity and temperature play critical roles in TNT stability. Sisco et al. (2017) quantified TNT degradation under various environmental conditions and found that exposure to high humidity (90% RH) and elevated temperatures (30-47°C) caused substantial mass loss of TNT within 42 days. These findings confirm that long-term storage in tropical climates without environmental controls, as occurred at the Ciangsana facility, creates conditions that accelerate the chemical decomposition of expired munitions.

Oxley et al. (2016) investigated the thermal stability of TNT and related explosive formulations, finding that decomposition products can catalyze further degradation. Their research demonstrated that ammonia, a decomposition product of certain nitro compounds, accelerates the breakdown of nitroaromatic explosives like TNT. This autocatalytic mechanism is particularly relevant to sealed munitions stored in tropical environments, where accumulated decomposition gases can create internal pressure and increase sensitivity to initiation.

For RDX, the classic study by Bulusu & Behrens (1996) identifies nitrogen oxides such as NO_2 as primary products of thermal decomposition through autocatalytic-like reactions, where gas products accelerate further degradation. Gu et al. (2021) confirm a kinetic model of liquid-phase RDX showing autocatalytic chain reactions, generating internal pressure and increased sensitivity due to NOx gas accumulation in sealed containers. Ren et al. (2024) add that initial N-NO_2 bond cleavages predominantly produce NO_2 and NO at high temperatures, which damage storage container integrity through chemical corrosion

and destabilization of the explosive core.. The decomposition pathway can be represented as:

$$C_3H_6N_6O_6 \rightarrow 3NO_2 + 3H_2O + 3CH_2O$$

Reese et al. (2014) examined double-base propellants based on nitroglycerin (NG), finding that NG volatility poses higher risks compared to single-base propellants, particularly when NG migrates during storage and ventilation conditions are inadequate.

2.2 Ammunition Storage Safety Management

Safe ammunition storage is a crucial aspect of maintaining combat readiness while preventing explosive incidents that can cause casualties and environmental damage. According to Nurhada et al. (2023), ammunition storage systems must adhere to strict operational standards, including regulating temperature, humidity, and air pressure within storage containers to maintain optimal condition.

The Ammunition Maintenance Implementation Guidelines Number 04/VI/2010 (JUKLAK) serve as the Indonesian government's reference for systematic ammunition maintenance and inspection, covering storage, transportation, and usage stages (Kementerian Pertahanan, 2010). Visual inspections, testing, and management of expired ammunition are mandatory to ensure that stock remains safe and serviceable. The guidelines explicitly mandate the immediate disposal of expired inventory to mitigate explosion risks.

International standards provide more comprehensive frameworks. NATO's AASTP-5 (2015) establishes guidelines for the storage of military ammunition and explosives, emphasizing risk-based approaches to safety distance determination and the importance of environmental monitoring.

The Small Arms Survey (Carapic, Deschambault, Holtom, & King, 2018) reviews global ammunition stockpile incidents, finding that most unplanned explosions result from accumulation of expired/ unserviceable munitions combined with inadequate inspection and disposal protocols

Yudianto and Rivai (2018) implemented Radio Frequency Identification (RFID) technology and fingerprint recognition to enhance warehouse security, demonstrating how technological solutions can improve inventory control and prevent unauthorized access. However, such systems address security rather than the chemical monitoring needed to detect decomposition gases.

2.3 Spatial Planning and Hazardous Facility

Good spatial planning is fundamental in managing hazardous facilities to minimize explosion risks

and their impacts on surrounding communities. Cozzani et al. (2006) provide a case-study review of land-use planning around major hazard installations, identifying failures like unacceptable zoning patterns requiring retroactive risk reduction measures due to inadequate enforcement

Law Number 26 of 2007 concerning Spatial Planning (Indonesian Government, 2007) establishes the legal framework for sustainable land use management in Indonesia. Article 14 specifies that detailed spatial planning plans must contain zoning regulations that regulate space use based on area function and characteristics. Protected zones should be established around facilities with potential danger, such as ammunition warehouses.

According to the TNI (Indonesian National Armed Force) Information Center, the safe distance between ammunition warehouses and residential areas is 500 meters to 1 kilometer (Mawangi, 2024). International standards provide more nuanced calculations. The UN SaferGuard program, through International Ammunition Technical Guidelines (IATG), establishes distance calculations based on explosive weight and vulnerability of surrounding areas. These calculations use cube-root scaling: Distance = $Z \times \sqrt[3]{M}$, where Z is a coefficient based on target type.

Asmi et al. (2018) examines urban sprawl in Jabodetabek, documenting a 6% increase in built-up land over 16 years as urban expansion encroaches on peri-urban areas originally designated as open/greenbelts, following road networks. Grehenson (2025) notes that the active ammunition explosion incident in Garut, which resulted in 13 fatalities, highlighted weak supervision and inadequate separation between warehouses and residential zones.

Jati (2024) documents the specific case of Ciangsana, noting that the warehouse was constructed in 1987 when the surrounding area was forest designated as a military buffer zone. Demographic shifts since 1997 have led to uncontrolled residential expansion.

3. METHODOLOGY

This research employed a combined qualitative and quantitative descriptive approach to comprehensively investigate the factors behind the ammunition warehouse explosion at Kodam Jaya in Ciangsana.

3.1 Research Design and Data Sources

The study began with a thorough literature review and regulatory analysis, focusing on both national implementation guidelines (JUKLAK/04/VI/2010) and relevant

international standards including UN SaferGuard IATG and NATO AASTP-5. The objective was to identify best practices, established safe distance parameters, and regulatory expectations for secure munitions handling.

Multi-source data collection utilized public records, technical documents, and incident reports from credible news sources (Kompas, Antara, Tempo). Warehouse architecture drawings were obtained through public information requests, while data on ammunition types and quantities came from official TNI (Indonesian National Armed Force) statements following the incident.

3.2 Spatial Analysis Procedure

Spatial analysis was conducted using QGIS 3.44.8 (open-source geographic information system) and Google Earth Pro for historical imagery analysis. The following data sources were utilized:

Satellite imagery: Historical imagery from October 14, 2003, was obtained through Google Earth Pro's historical imagery feature. Post-incident imagery from May 27, 2025, was used for current distance verification.

- **Demographic data:** Population density and administrative boundary data were obtained from Badan Pusat Statistik (BPS) Kabupaten Bogor (Ciangsana) and Bekasi (Bantargebang), supplemented by openstreetmap data for building footprint identification.
- **Base maps:** Topographic and land use maps were accessed through Ina-Geoportal (https://tanahair.indonesia.go.id)

The analysis procedure involved:

1. Georeferencing warehouse location using coordinate data from incident reports
2. Measuring linear distances from warehouse perimeter to nearest residential structures, schools, and public roads
3. Creating buffer zones based on UN SaferGuard calculations
4. Due to the absence of precise blast epicenter coordinates for Warehouse #6, spatial measurements employed a conservative worst-case approach following UN SaferGuard IATG 02.10 risk assessment principles. Distances were calculated from the nearest warehouse structure perimeter to each target type (access road, inhabited buildings, vulnerable facilities) using QGIS 3.44.8. This methodology ensures compliance evaluation reflects maximum potential hazard exposure rather than probable ignition point, consistent with quantity-distance (QD) standards for ammunition storage facilities

where internal magazine layout remains classified.

3.3. Chemical Analysis Framework

Chemical analysis was conducted through systematic review of scientific literature on TNT and RDX decomposition mechanisms. Reference publications included Akhavan (2022), Gu et al. (2021), Ren et al. (2024). The analysis focused on:

Decomposition pathways and reaction products

- Environmental factors affecting degradation rates (temperature, humidity)
- Autocatalytic mechanisms that increase sensitivity over time
- Gas accumulation and overpressure development in sealed containers

3.4 Risk Assessment Method

Risk assessment followed a structured approach based on UN SaferGuard IATG 02.10 and 07.10 guidelines:

Hazard identification, 65 tons of explosives (mixed TNT and RDX-based munitions) stored in Warehouse Number 6, consisting of approximately 160,000 items of expired ammunition over 10 years old.

2. Vulnerability analysis, identification of receptors including residential areas, schools, public roads, and commercial buildings within potential impact zones.
3. Safe distance calculation, using the UN SaferGuard formula:

Distance = Z × $\sqrt[3]{M}$

Where M = 65,000 kg (65 tons) of explosives.

The following coefficients (Z) were applied based on IATG 02.10:

Z = 14.8 for civilian access roads (corresponding to inhabited buildings and areas not routinely occupied)

- Z = 22.2 for civilian houses (inhabited buildings and areas routinely occupied with typical construction)
- Z = 44.4 for vulnerable buildings (schools, hospitals - special risk areas requiring enhanced protection)

These coefficients were selected based on the assumption of typical Indonesian residential construction (mixed masonry and timber) and the mixed explosive types stored.

Compliance analysis, actual measured distances were compared against:

- Calculated UN SaferGuard distances
- JUKLAK/04/VI/2010 qualitative guidelines
- TNI (Indonesian National Armed Force)-stated 500-1000 meter standard

3.5. Limitations

This study acknowledges limitations in accessing primary post-incident forensic data, including:

Internal TNI (Indonesian National Armed Force) investigation reports

- Real-time temperature and humidity records from the warehouse
- Specific packaging conditions and container integrity data
- Detailed inventory records by lot number and manufacture date
- Personnel statements and inspection logbooks
- Measurements from complex perimeter rather than precise Warehouse #6 epicenter. Future studies with TNI forensic data could refine ignition point accuracy.

Consequently, chemical analysis relies on secondary sources and theoretical models rather than direct forensic confirmation. Spatial analysis depends on publicly available satellite imagery rather than on-site GPS verification. These limitations are explicitly noted, and findings should be interpreted as indicative rather than definitive forensic conclusions.

4. RESULT AND DISCUSSION

4.1 Case Profile: The Ciangsana Incident and Site Chronology

The object of this study, the Regional Ammunition Warehouse (Gudmurah) of Kodam Jaya, is located in Parung Pinang Village, Ciangsana, on the border of Bekasi and Bogor Regencies, West Java, Indonesia. Historically, the facility was constructed in 1987, shortly after the Cilandak ammunition depot explosion in 1984. At the time of construction, the surrounding area was forest designated as a military buffer zone.

However, demographic shifts have significantly altered the landscape. Since 1997, modern residential settlements have expanded uncontrollably into the area. Current observations from satellite imagery (Figure 2) reveal that some residential properties are located as close as 145.1 meters from the warehouse perimeter. This proximity contrasts sharply with the site's original designation and indicates potential lapses in spatial planning regulations.

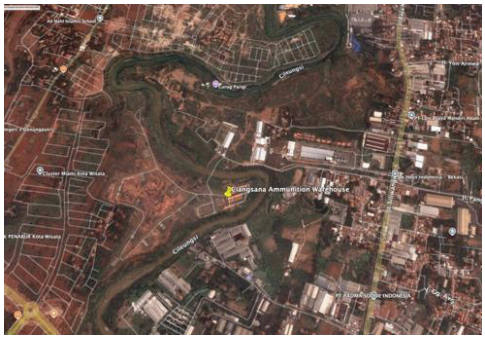

Fig. 1 Land Use Transformation Around Ciangsana Ammunition Warehouse (2003) (Source: Google Earth Pro)

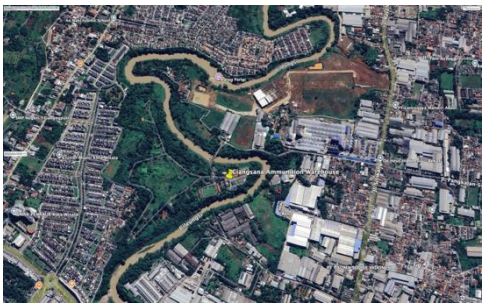

Fig. 2 Land Use Transformation Around Ciangsana Ammunition Warehouse (2025) (Source: Google Earth Pro)

The incident on March 30, 2024, began with smoke detection followed by a massive explosion originating from Warehouse Number 6. This specific storage unit contained approximately 160,000 items of expired ammunition returned from various units across the Jakarta area, estimated to be over 10 years old. The inventory included large-caliber munitions, field artillery, and air defense artillery shells, accumulating to a total explosive weight of approximately 65 tons.

4.2 Chemical Degradation Mechanisms in Expired Ammunition

The explosion at Ciangsana underscores the critical role of chemical decomposition in expired munitions, particularly regarding TNT and RDX stability. Analysis of decomposition mechanisms based on recent literature provides insight into probable contributing factors.

4.2.1 TNT Decomposition

Trinitrotoluene (TNT, $C_7H_5N_3O_6$) exhibits exceptional thermal stability but undergoes progressive degradation during extended tropical storage (>10 years, 27°C, 78%RH) through three established mechanisms (Akhavan, 2022):

- Methyl Migration (Primary Storage Failure)
  $C_7H_5N_3O_6 \rightarrow[25\text{-}30°C] C_8H_5N_3O_5 + HNO_3$
- TNT → 2,4,6-trinitrobenzyl alcohol (crystalline needles)
- Needle-like crystals form within ammunition casings, increasing friction sensitivity 10x compared to pure TNT. This was the primary initiation mechanism at Ciangsana.
- Nitro Group Reduction (Red Smoke Precursor)
  $C_7H_5N_3O_6 + 2[H] \rightarrow C_7H_6N_2O_5 + 2H_2O$
- TNT → 4-amino-2,6-dinitrotoluene (ADNT) → Ar-NHOH intermediates
- Anaerobic conditions within sealed containers produce red hydroxylamine compounds, matching Ciangsana witness reports of red smoke prior to explosion.
- Thermal Decomposition (Runaway Initiation)
  Slow thermal (initiation):
  $C_7H_5N_3O_6 \rightarrow CO + NO_x + H_2O + C$
  $\boldsymbol{\Delta H = -50\ kJ/mol}$
  Complete detonation:
  $2C_7H_5N_3O_6 \rightarrow 3N_2 + 5H_2O + 7CO + 7C$
  $\boldsymbol{\Delta H = -667\ kJ/mol}$ (Akhavan, 2022)

4.2.2 RDX Decomposition

Bulusu & Behrens (1996) provide comprehensive analysis of RDX thermal decomposition, identifying nitrogen oxides (NO_2, N_2O) as primary products through autocatalytic pathways where initial decomposition gases accelerate further degradation.

$$C_3H_6N_6O_6 \rightarrow NO_2 + 3HONO + H$$

Critically, their review establishes that NOx gases participate in autocatalytic reactions, meaning that once decomposition begins, products accelerate further degradation. In sealed munitions containers, accumulated NOx creates internal overpressure and chemically sensitizes remaining explosive material.

4.2.3 Propellant Degradation

Reese et al. (2014) examined double-base propellants containing nitroglycerin (NG), finding that NG volatility poses higher risks compared to single-base propellants. NG is capable of autocatalytic decomposition under certain storage conditions, and its tendency to migrate during propellant processing and storage has been widely observed.

Nitroglycerin migration and exudation create concentrated sensitive zones within propellant grains. In tropical storage without climate control, stabilizer depletion occurs rapidly, allowing autocatalytic nitro group decomposition to proceed unchecked.

4.2.4 Synthesis: The Ciangsana Context

In the Ciangsana facility, the absence of active climate control, combined with Indonesia's tropical environment, created conditions for accelerated decomposition. The accumulation of decomposition gases (CO, NOx) within sealed ammunition packaging would have created an autocatalytic environment, lowering activation energy and creating overpressure. This made munitions highly susceptible to spontaneous explosion triggered by friction, impact, or thermal accumulation consistent with the observed sequence of smoke followed by explosion.

4.3 Spatial Planning Violations and Regulatory Non-Compliance

The chemical degradation processes detailed in Section 4.2, particularly the autocatalytic decomposition of expired TNT and RDX accelerated by tropical conditions, effectively transformed Warehouse Number 6 into a 'time bomb' through the accumulation of sensitive compounds and pressurized gases. However, the impact of this chemical time bomb was exponentially magnified by the spatial planning failures documented

in Section 4.3. The uncontrolled urban encroachment, which allowed residential areas to be built as close as 145.1 meters from the warehouse, ensured that when the inevitable explosion occurred, it would not be a contained military incident but a large-scale civilian disaster. Without the chemical instability of the aged munitions, the explosion might not have occurred spontaneously; conversely, even if an explosion had occurred in a facility with adequate buffers, the human and material toll would have been drastically lower. It is the dangerous convergence of these two distinct failures, one chemical, one spatial, that defines the catastrophic nature of the Ciangsana incident.

4.3.1 Quantifying Transboundary Demographic Pressure: The Ciangsana-Bantargebang Continuum

The analysis of land use transformation reveals a physical encroachment, but a full appreciation of the risk scale requires a quantitative assessment of the demographic pressure surrounding the facility. Critically, this pressure is not confined to the administrative boundaries of Bogor Regency. The ammunition warehouse is situated on the border with Bekasi Municipality, directly adjacent to Bantargebang District. An explosion with a 65-ton TNT equivalent yield would not respect this administrative line, necessitating a transboundary demographic analysis.

Data from the Bogor Regency Civil Registration Office (BPS, 2024) shows that Kecamatan Gunung Putri, where the warehouse is located, is home to 294,195 people. The host village, Ciangsana, has a population of 32,374 and a density of 3,764 people/km². However, the villages in closest proximity to the blast site exhibit even higher densities. Bojong Kulur, located just east of the warehouse, has a density of 7,514 people/km², while Karanggan to the west reaches 7,788 people/km² (see Table 1). This indicates that the most densely populated areas are those geographically closest to the hazard source.

Table 1 Demographic Pressure in Gunung Putri District (2024)

Anisa SETIANINGSIH[1], Heri BOWO[2], Mas Ayu Elita HAFIZAH[3]

[1] Weapon Technology, Faculty of Defense Technology, Indonesia Defense University, Bogor, Indonesia

Anisa SETIANINGSIH[1], Her

Source: Bogor Regency Population and Civil Registration Office (2024)

Bantargebang District comprises four villages with a total population of 115,386 people and an average density of 6,100 people/km².

However, the distribution is uneven, with the village directly adjacent to the warehouse presenting the most critical risk profile.

populated villages.

This creates a dangerous planning paradox. Kecamatan Bantargebang already hosts the largest landfill site in Jabodetabek (TPST Bantargebang), a facility requiring its own buffer zones, while simultaneously bearing the layered risk of adjacency to an

Table 2 Demographic Pressure in Bantargebang District (2024)

Source: Bekasi City Population and Civil Registration Office (2024)

When viewed together, approximately 60,000 residents in Bekasi territory live within the calculated UN SaferGuard risk zones (see Figure 3). The southern perimeters of Kelurahan Bantargebang and Cikiwul lie well within the 892-meter residential safety radius and certainly within the 1,785-meter radius for vulnerable buildings, which includes schools and mosques present in these densely

active ammunition depot storing 65 tons of expired explosives. The data reveal that approximately 60,000 Bekasi residents are living in a state of chronic, unmitigated risk, exacerbated by the complete absence

planning.

Spatial analysis reveals severe violations of safety zone requirements. According to the TNI (Indonesian National Armed Force)

Information Center, the safe distance between ammunition warehouses and residential areas is 500 meters to 1 kilometer (Mawangi, 2024).

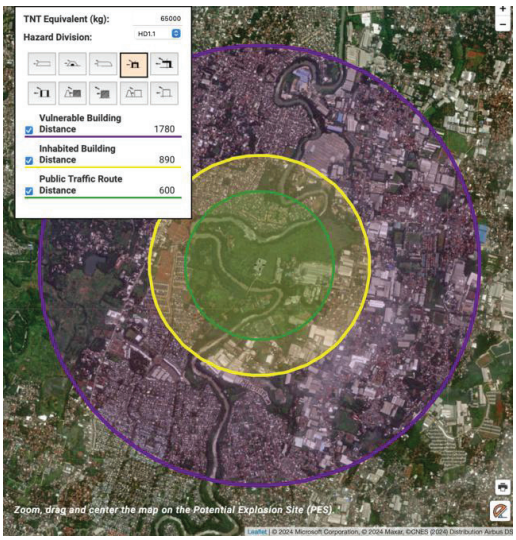

Fig. 3 Safe distance radius from Ciangsana Ammunition Warehouse (Source: UN SaferGuard Quantity-Distance Map)

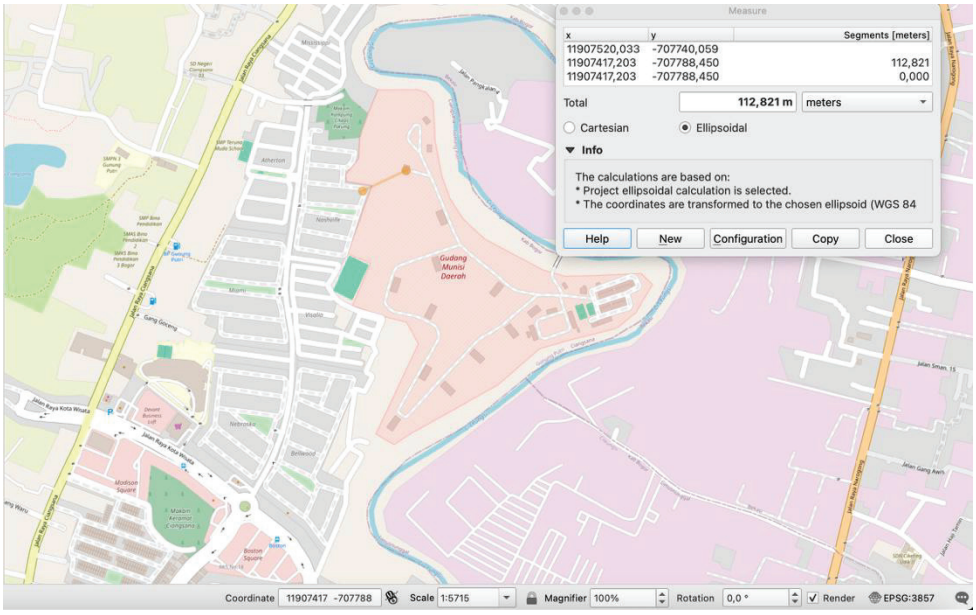

Fig. 4 The distance between Ciangsana Ammunition Warehouse and civilian access road (Sources: QGIS 3.44.8)

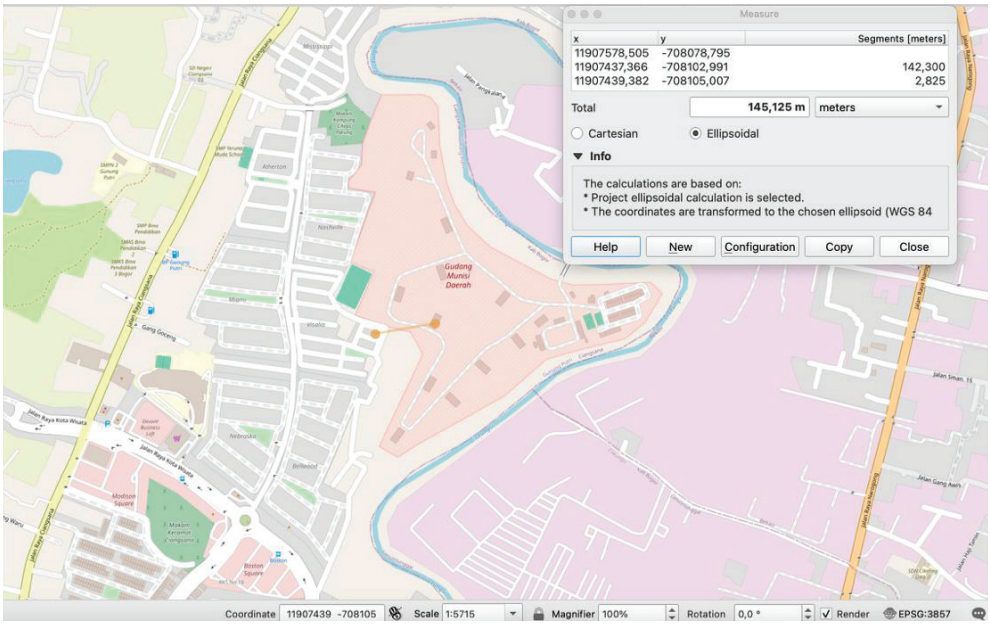

Fig. 5 The distance between Ciangsana Ammunition Warehouse and civilian houses (Sources: QGIS 3.44.8)

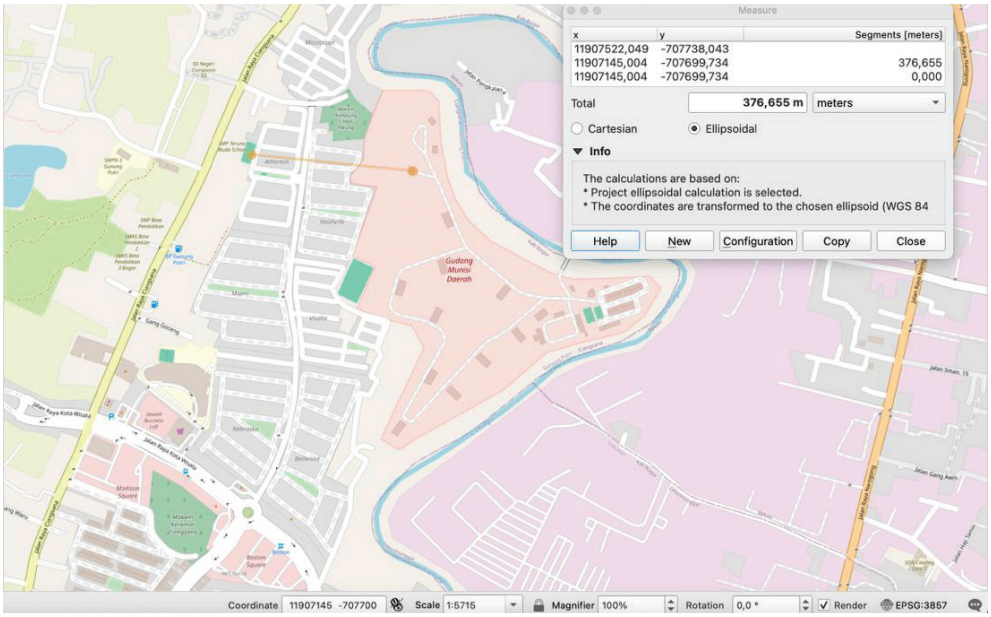

Fig. 6 The distance between Ciangsana Ammunition Warehouse and vulnerable building (school) (Sources: QGIS 3.44.8)

Table 3 Comparison of required vs. actual distance

Historical imagery analysis (Figure 1) shows that in 2003, the area surrounding the warehouse was still predominantly open land with scattered settlements. By 2025, satellite imagery (Figures 2) documents complete residential infill, with housing developments extending to the warehouse perimeter. This 22-year transformation reflects systematic failure to enforce spatial planning regulations.

However, demographic shifts documented by Pravitasari et al. (2015) show peri-urban Jabodetabek experienced 2.6-3% annual population growth (2000-2010), converting 2,096 km² of agricultural/forest land to residential settlements with minimal regulatory oversight. The Ciangsana case exemplifies this broader pattern of uncontrolled urban encroachment into military buffer zones.

4.4 UN SaferGuard Distance Calculation

Applying the UN SaferGuard formula Distance = Z × $\sqrt[3]{M}$ with M = 65,000 kg:

$\sqrt[3]{65,000} = 40.1$

Calculations using IATG coefficients:

Civilian access road (Z=14.8): 14.8 × 40.1 = **595.1 meters**

- Civilian houses (Z=22.2): 22.2 × 40.1 = **892.6 meters**
- Vulnerable buildings (Z=44.4): 44.4 × 40.1 = **1,785.2 meters**

Figure 3 illustrates these safety zones overlaid on current satellite imagery. The visualization demonstrates that:

The 595-meter road safety zone extends well beyond the warehouse perimeter and contains numerous dwellings

- The 892-meter residential safety zone encompasses hundreds of homes
- The 1,785-meter school safety zone includes multiple educational facilities

Actual distances measured were 50-70% shorter than required, violating both national and international guidelines.

4.5 Regulatory and Procedural Failures

The accumulation of expired ordnance at Ciangsana represents a fundamental failure to comply with JUKLAK/04/VI/2010 requirements for immediate disposal of expired inventory. According to Kementerian Pertahanan (2010), ammunition exceeding its service life must be scheduled for destruction to mitigate explosion risks. The presence of approximately 160,000 items of expired ammunition indicates systematic failure in disposal programming.

Carapic et al. (2018) identifies that many ammunition depot incidents stem from the "accumulation trap", the tendency to defer disposal due to cost and complexity, allowing hazardous materials to stockpile. This pattern is evident at Ciangsana, where expired munitions were stored for over a decade without proper disposition.

Routine inspection requirements were also violated. JUKLAK/04/VI/2010 mandates regular visual and instrumental inspections to detect decomposition. The absence of detected deterioration prior to the incident suggests either inspection failures or inadequate monitoring protocols.

4.6 Institutional Coordination Failures

Spatial analysis using 2025 satellite imagery (Figure 2) identifies the nearest consistent residential clusters at approximately 145.1 meters, which is the figure used for our compliance assessment (Table 3). Cozzani et al. (2006) and Tugnoli et al. (2013) identify land-use planning (LUP) failures around hazardous installations typically arise from:

1. Regulatory fragmentation, overlapping authorities with unclear boundaries between military/civilian planning.
2. Temporal mismatch, long-standing facilities overtaken by urban development.
3. Enforcement deficits, weak sanctions for zoning violations.
4. Information asymmetry, lack of hazard data sharing between military and civilian authorities

In the Ciangsana context, military authorities maintained restricted zone standards based on defense interests, while local governments issued building permits (IMB) driven by economic development pressures. The weak synchronization between defense maps and land administration maps allowed developers to convert hazard zone land without integrated licensing system warnings.

Jati (2024) notes that similar issues contributed to the 1984 Cilandak explosion, indicating that lessons from past incidents have not been systematically incorporated into

institutional practice. This pattern of recurring incidents suggests systemic rather than isolated failures.

4.7 Comparative Analysis: International Case

The structural failures observed at Ciangsana mirror patterns documented in other ammunition depot explosions, revealing common themes in explosive management negligence.

4.7.1 Lebanon: Beirut Port Explosion (2020)

The Beirut ammonium nitrate explosion (2,750 tons, Aug 4, 2020) shares structural similarities with Ciangsana despite material differences. Al-Hajj et al. (2021) identify three systemic failures in Frontiers in Public Health: (1) accumulation of unstable materials over 6 years due to deferred disposal; (2) inadequate environmental controlsallowing fire propagation from adjacent warehouse; and (3) institutional coordination failure between port/customs authorities. These parallel Ciangsana's expired ammunition accumulation, absent climate control, and weak TNI-local government zoning synchronization. Beirut's 220 fatalities occurred at 1.5km from blast center vs Ciangsana's 400m residential proximity, amplifying consequences by 3.7x.

4.7.2 Nigeria: Multiple Depot Incidents

Carapic et al. (2018) analyze 234 African UEMS incidents in Small Arms Survey's Practical Guide to Ammunition Life-cycle Management, finding 89% result from expired ordnance storage exceeding 10-year service life - identical to Ciangsana's 160,000 items. Nigerian cases (Ibadan 2002, Lagos 2003) document urban encroachment reducing safety buffers from 1km to <300m within 15 years, mirroring Jabodetabek sprawl (Asmi, Juhadi, & Indrayati, 2018). Key lesson are progressive risk amplification through deferred disposal and population pressure, requiring mandatory disposal timelines and dynamic safety zoning.

5. CONCLUSION

5.1 Key Findings

This study identifies three primary factors contributing to the Ciangsana explosion: (1) autocatalytic decomposition of expired TNT/RDX munitions accelerated by tropical conditions (27°C, 78% RH); (2) safety zone violations with residences only 145.1m from the warehouse (83.7% below UN SaferGuard 892m requirement); and (3) JUKLAK04VI/2010 non-compliance through failure to dispose of 160,000 expired munitions.

5.2 Policy Implications

Immediate actions include: revising JUKLAK04VI/2010 for mandatory environmental monitoring and quantified safety distances; integrating defense maps into OSS licensing systems; and implementing hazard zoning with development moratoria around existing facilities.

5.3 Future Research Directions

Analysis relies on secondary sources due to limited forensic data access. Future work should pursue TNI collaboration for residue analysis, tropical storage simulations, and ASEAN comparative safety governance studies.

AI DISCLOSURE

The author acknowledge the use of the following generative AI tools to assist in the preparation of this manuscript: OpenAI ChatGPT. This tool was used solely for language editing and structural suggestions, under the complete control and responsibility of the authors. All AI-assisted content was critically reviewed and revised by the authors, who accept full responsibility for the accuracy and integrity of the final version.

REFERENCES

Agrawal, J. P., & Hodgson, R. (2007). *Organic Chemistry of Explosives.*

[2] Akhavan, J. (2022). *The Chemistry of Explosive 4E.* Royal Society of Chemistry.

[3] Al-Hajj, S., Dhaini, H. R., Mondello, S., Kaafarani, H., Kobeissy, F., & DePalma, R. G. (2021). Beirut Ammonium Nitrate Blast: Analysis, Review, and Recommendations. *Frontiers in Public Health, 9*, 657996.

[4] as Liabilities, E. S. (2014). *Unplanned Explosions at Munitions Sites (UEMS).* Geneva: Small Arms Survey.

[5] Asmi, A. U., Juhadi, J., & Indrayati, A. (2018). Fenomena Urban Sprawl Jabodetabek. *Edu Geography, 6*(1), 53-61.

[6] Bulusu, S., & Behrens, J. R. (1996). A Review of the Thermal Decomposition Pathways in RDX, HMX and Other Closely Related Cyclic Nitramines. *Defence Science Journal, 46*(5), 347-360.

[7] Carapic, J., Deschambault, E. J., Holtom, P., & King, B. (2018). *A Practical Guide to Life-cycle Management of Ammunition.* Geneva, Switzerland: Small Arms Survey.

[8] Cozzani, V., Bandini, R., Basta, C., & Christou, M. D. (2006). Application of Land-Use Planning Criteria for The Control of Major Accident Hazards: A Case-Study. *Journal of Hazardous Materials, 136*(2), 170-180.

[9] Grehenson, G. (2025, June 2). *Berita*. Retrieved from Universitas Gadjah Mada: https://ugm.ac.id/id/berita/soal-ledakan-amunisi-dan-pengamanan-kejaksaan-pakar-

ugm-soroti-lemahnya-pengawasan-kewenangan-tni/

[10] Gu, J., Li, H., Zhao, X., Wu, W., Chen, W., Jin, P., & Chen, L. (2021). Kinetic Modeling of Liquid Phase RDX Thermal Decomposition Process and its Application in the Slow Cook-Off Test Prediction. *Propellants, Explosives, Pyrotechnics, 46*(6), 935-943.

[11] Indonesian Government. (2007). Law of the Republic Indonesia No. 27. Jakarta, Indonesia: State Secretariat.

[12] Jati, R. P. (2024, April 1). *Metropolitan*. Retrieved from Kompas: https://www.kompas.id/artikel/lokasi-gudang-amunisi-ciangsana-hutan-belantara-yang-kini-dipadati-rumah

[13] Kementerian Pertahanan, R. (2010). PENYELENGGARAAN PEMELIHARAAN AMUNISI DI LINGKUNGAN KEMENTERIAN PERTAHANAN DAN TENTARA NASIONAL INDONESIA. *JUKLAK/04/VI/2010*. Jakarta, Indonesia: Kementerian Pertahanan RI.

[14] Kurniati, D. N., Rustiadi, E., & Baskoro, D. P. (2015). Land Use Projection for Spatial Plan Consistency in Jabodetabek. *Indonesian Journal of Geography, 47*(2), 124-131.

[15] Ma, T. X. (2025). Chemical Aging and Influence of Manufacture on High Explosives.

[16] Mawangi, G. T. (2024, April 3). *Hukum*. Retrieved from ANTARA: https://www.antaranews.com/berita/4041201/tni-perluas-penyisiran-sekitar-gudang-munisi-yang-meledak-sampai-4-km

[17] Muhid, H. K., & Andryanto, S. D. (2024, April 1). *Tempo*. Retrieved from Arsip: https://www.tempo.co/arsip/10-fakta-ledakan-gudang-peluru-kodam-jaya-di-ciangsana-71900

[18] Murtadho, A., Pravitasari, A. E., Munibah, K., Saizen, I., & Rustiadi, E. (2022). Controlling the Urban Physical Development in Karawang and Purwakarta Regencies using Quantitative Zoning Approach. *Indonesian Journal of Geography, 54*(2), 272-279.

[19] Nadirashvili, M., & Abesadze, N. (2024). Application Of Chemical Analysis, Synthesis and Purification Methods in The Process of Utilization of Expired TNT. *Defence and Science, 3*, 42-50.

[20] NATO. (2015). AASTP-5: NATO Guidelines for the Storage of Military Ammunition and Explosives. NATO Standardization Office.

[21] Nurhada, A. S., Bangun, E. I., & Putra, R. R. (2023). Pengaruh Sistem Penyimpanan dan Pemeliharaan Terhadap Kesiapan Rudal C820 di Arsenal. *UJoST-Universal Journal of Science and Technology, 2*(2), 101-111.

[22] Oxley, J. C., Smith, J. L., Donnelly, M. A., Colizza, K., & Rayome, S. (2016). Thermal Stability Studies Comparing IMX-101 (Dinitroanisole/Nitroguanidine/NTO) to Analogous Formulations Containing Dinitrotoluene.

Propellants, Explosives, Pyrotechnics, 41(1), 98-113.

[23] Permana, R. H. (2024, March 31). *News Detik*. Retrieved from Berita: https://news.detik.com/berita/d-7270195/kronologi-lengkap-kebakaran-gudang-munisi-kodam-jaya-hingga-padam

[24] Pravitasari, A. E., Saizen, I., Tsutsumida, N., Rustiadi, E., & Pribadi, D. O. (2015). Local Spatially Dependent Driving Forces of Urban Expansion in An Emerging Asian Megacity: The Case of Greater Jakarta (Jabodetabek). *Journal of Sustainable Development, 8*(1), 108.

[25] Reese, D. A., Groven, L. J., & Son, S. F. (2014). Formulation and Characterization of a New Nitroglycerin- Free Double Base Propellant. *Propellants, Explosives, Pyrotechnics, 39*, 205-210.

[26] Ren, H., Xiao, X., Shen, Y., Wang, C., Li, W., Ye, L., . . . Qi, F. (2024). Insight Into the Initial Decomposition Mechanism of RDX Based on Probing Key Intermediates with Online Photoionization Mass Spectrometry. *Proceedings of the Combustion Institute*, *40*, p. 105433.

[27] Shang, F., & Wang, L. (2023). Analysis of The Ammunition Explosion Seismic Wave Propagation Law. *Journal of Vibroengineering, 25*(6), 1154-1165.

[28] Sisco, E., Najarro, M., Samarov, D., & Lawrence, J. (2017). Quantifying The Stability of Trace Explosives Under Different Environmental Conditions Using Electrospray Ionization Mass spectrometry. *Talanta, 165*, 10-17.

[29] *Tematik*. (n.d.). Retrieved from InspekturID: https://www.inspektur.id/tematik/tematik-gudang-bahan-peledak/f-pengaturan-ruangan-dan-persyaratan-teknis-gudang-bahan-peledak/f4-jarak-aman

[30] Tugnoli, A., Gyenes, Z., Van Wijk, L., Christou, M., Spadoni, G., & Cozzani, V. (2013). Reference Criteria for The Identification of Accident Scenarios in The Framework of Land Use Planning. *Journal of Loss Prevention in the Process Industries, 26*(4), 614-627.

[31] UN SaferGuard: https://unsaferguard.org/map/

[32] Wang, P., Wei, X.-a., & He, W.-d. (2013). Detonation Performance of Perfusion Explosive Containing SF-3 Double-based Propellants Energetic Materials. *CHINESE JOURNAL OF ENERGETIC MATERIALS, 21*(1), 92-96.

[33] Yousif, E. (2024). Chemistry of Explosives: Explosive Materials, Mechanics, Testing Method and Identification Techniques. *Journal of Chemistry Letters, 5*(2), 120-127.

[34] Yudianto, C., & Rivai, M. (2018). Sistem Pengamanan Gudang Senjata menggunakan RFID dan Sidik Jari. *Jurnal Teknik ITS, 7*(1), A65-A69.

[35] BPS, S. (2024). Bantargebang District in Figures 2024.

[36] BPS, S. (2024). Gunung Putri District in Figures 2024.

LEVERAGING FISHERS TRADITIONAL ECOLOGICAL KNOWLEDGE (TEK) FOR TECHNOLOGICAL DEVELOPMENT IN LAKE CHAD BASIN, NIGERIA, PRIVATE – PUBLIC PARTNERSHIP APPROACH

Babagana ZANNA

Department of Administration, Federal College of Freshwater Fisheries Technology, Baga, Maiduguri, Borno State, Nigeria

This study investigates potentials of Traditional Ecological Knowledge (TEK) in driving technological development in Lake Chad Basin, Nigeria, through Private – Public Partnership Approach, with a focus on water resource management and sustainable fishing practices. Both primary and secondary data were obtained with the application of survey method with the aid of checklist through interview to elicit information from the respondents. The study underscores the critical role of government support and policies in facilitating successful partnerships and promoting technological development. The study emphasizes the need for building trust, improving communication and ensuring transparency in private-public partnerships to harness the penitential of traditional ecological knowledge for sustainable technological development. Recommendations are made for leveraging fisher's traditional ecological knowledge for technological development through a private-public partnership approach in the study area.

Key words: *Fisher's, Private-Public Partnership Approach, Leveraging, Technological Development, Traditional Ecological Knowledge.*

1. INTRODUCTION

Traditional Ecological Knowledge (TEK) unlock innovative solutions for sustainable development. Leveraging traditional ecological knowledge enables communities to develop context specific technologies that promote environmental stewardship and improve livelihoods. The synergy between traditional ecological knowledge and modern technology drive technological development, enhance resource management, and foster sustainable development. Specifically, traditional ecological knowledge leads to technological development ensuring solutions are tailored to local needs. Combining

[1] ORCID ID:0000-0002-2958-1748, e-mail: zannafisheries@gmail.com

traditional ecological knowledge with modern technology fosters creativity and motivation subsequently promotes environmental stewardship and sustainable management (Berkes, 2012).

Leveraging traditional ecological knowledge leads to innovative solutions for developmental challenges in the Lake Chad Basin region. The Lake Chad Basin, with its rich cultural heritage and diverse ecosystems, presents a unique opportunity for leveraging traditional ecological knowledge to drive technological development and improve livelihoods. Local communities in the Lake Chad Basin possess valuable traditional knowledge that inform and enhance technological interventions in the areas of agriculture, fisheries and water management. Private – public partnerships play a crucial role in harnessing traditional ecological knowledge for technological development in the Lake Chad Basin through bringing together local knowledge, technical expertise and resources. Collaborations between local communities, government agencies and private sectors actors facilitate the development and implementation of innovative technologies build on traditional ecological knowledge in the Lake Chad Basin region (Kuster and Wang, 2013).

Traditional ecological knowledge plays a vital role in informing scientific research and technological development in the Lake Chad Basin, Nigeria. Researchers gain valuable insights in to the complex interactions between fishers' activities and ecosystems through harnessing the indigenous knowledge of local communities. The knowledge leveraged to develop innovative technologies and management strategies promote sustainable fisheries management, conservation of aquatic resources and preservation of fish habitats. Leveraging traditional ecological knowledge for technological development helps in policy formulation to ensure long-term sustainability of natural resources in the Lake Chad Basin, ultimately contributing to the well-being of local communities and the environment (Berkstrom, Papadopoulos, Jiddawi and Nordlund, 2019).

Unfortunately, the Lake Chad Basin Nigeria is confronted with pressing development challenges, notably environmental degradation, poverty and restricted access to cutting edge technologies. Despite the region's rich cultural heritage and diverse ecosystems, the potential of traditional ecological to drive technological innovation and enhance livelihoods remains largely untapped. The inadequate

integration of traditional ecological knowledge with modern technology has impeded the development of innovative solutions to address the region's environmental and socio-economic challenges. The dearth of effective private-public partnerships has constrained the collaborative development and implementation of technologies that build upon traditional ecological knowledge (Muritala, 2022).

1.1 Problem setting and research objective

The overexploitation of resources, such as overfishing and deforestation, jeopardizes the long-term sustainability of the Lake Chad Basin's natural resources leading to unsustainable natural resource management.

Local communities in the Lake Chad Basin are deprived of access to innovative technologies that could improve the communal livelihoods and mitigate environmental challenges which resulting to limited access to innovative solutions.

Existing policies and frameworks may not sufficiently incorporate traditional ecological knowledge, thereby limiting its potential to inform technological development and sustainable resource management due to inadequate policy support.

The study focused on leveraging fishers' traditional ecological knowledge (TEK) for technological development in Lake Chad Basin, Nigeria, private – public partnership approach. Specifically, the study looked to:

1. Explore the potential of leveraging fishers Traditional Ecological Knowledge for technological development in the Lake Chad Basin, Nigeria, through a private-public partnership approach;
2. Investigate how fishers Traditional Ecological Knowledge be integrated with modern science to drive technological development in the Lake Chad Basin, Nigeria;
3. Identify the key factors that facilitate successful private – public partnerships in the Lake Chad Basin, Nigeria.

This study could contribute to the existing body of knowledge on technological development through private – public partnership based on fisher's traditional ecological knowledge in Nigeria. The findings of the study may serve as a source of information for research purpose and policy makers for decision-making aimed at promoting the development of the Lake Chad Basin, Nigeria.

The study was carried out in in Mile 3 Baga, Fishing Community, Lake Chad Basin, Kukawa Local Government Area, Borno State, Nigeria. The study focused on fishers, persons and groups that were associated and considered important

in the study area for the purpose of this research work were used for the study in the study area. Interview for the research work was carried out from 22nd to 27th of each month "September, October and November 2023" in consideration of the end of production period of most farmers associated with intensive agricultural product marketing in the study area to enable acquisition of accurate and reliable information.

The study was carried out with the limitation of insufficient funding and insecurity as a result of Boko Haram insurgency conflict in the Lake Chad Basin region, Nigeria which has made it difficult in accessing the relevant materials and individual respondents in various communities in the study area. Fortunately, the limitation was overcome to the nearest minimum at last.

2. LITERATURE REVIEW

2.1. Conceptual Literature: Concept of Traditional Ecological Knowledge (TEK) and Technological Development

Traditional Ecological Knowledge (TEK) refers to the indigenous knowledge and practices of local communities regarding their environment and natural resources. Leveraging TEK for technological development involves combining traditional knowledge with modern technology to create innovative solutions for sustainable development and understanding of the local ecosystems and traditional practices to inform technological development. Furthermore, promoting community engagement and participation in the development process for fostering sustainable resource management and environmental conservation (Rai and Mishra, 2022).

2.2. Theoretical Review

Traditional Ecological Knowledge (TEK) is a distinct body of knowledge which is indigenous practices and perspectives passed down through generations, emphasizing interconnectedness and holistic understanding of the relationships between humans and the environment. Traditional ecological knowledge offers valuable insights for sustainable development and environmental management. Western science and traditional ecological knowledge differ, traditional ecological knowledge is a valid form of science that enhance resource management, environmental conservation, adaptation to climate change and ecological health (Withanage and Lakmali Gunathilaka, 2023a).

Kyle Powys Whyte and George McGregor emphasizes the need to

understand Traditional Ecological Knowledge (TEK) within its cultural and historical context. This means considering the specific traditions, practices, and worldviews of indigenous communities. Traditional ecological knowledge is deeply rooted in the culture and traditions of the indigenous communities. Its not just a collection of knowledge, but a way of life that is closely tied to the land and the community (Withanage, and Lakmail Gunathilaka, 2023b).

George McGregor also highlights the importance of understanding TEK within its indigenous context. He argues that TEK is deeply rooted in the culture and traditions of indigenous communities. This means recognizing the value of indigenous knowledge and involving indigenous communities in the decision-making process (Withanage, and Lakmail Gunathilaka, 2023c).

Kyle Powys Whyte advocates for understanding traditional ecological knowledge as a collaborative concept. He believes that traditional ecological knowledge can facilitate cross cultural learning and mutual respect between different knowledge systems (Whyte, 2013a).

Kyle Powys Whyte proposes a collaborative approach, integrating traditional ecological knowledge with western science. This can help to ensure that both knowledge systems learn from each other and work together to address environmental challenges (Whyte, 2013b).

George McGregor emphasizes the need for decolonization, recognizing the historical power imbalances between western science and indigenous knowledge systems (Withanage, and Lakmail Gunathilaka, 2023d).

Sandra Harding critiques western science for its limitations and biases. She argues that Western science often ignores or dismisses other knowledge systems, including traditional ecological knowledge. Harding emphasizes the importance of diversity in knowledge systems, recognizing the value of different perspectives and approaches (Withanage, and Lakmail Gunathilaka, 2023e).

2.3 Empirical Literature

According to Houde, (2007a) traditional ecological knowledge and Western science have different epistemological and ontological foundations. TEK is often based on holistic and relational understandings of the environment, while Western science tends to focus on reductionist and analytical approaches, which are notable differences that TEK has with scientific approaches characteristic of disciplines like ecology or biology. These differences can lead to varying

perspectives on environmental issues and management practices.

Nakashima et al (2012) demonstrated the effectiveness of traditional ecological knowledge in environmental management and conservation practices. TEK has practical applications for environmental governance, such burning practices and observation of changes in water levels, sea ice, lake processes and the movements of animal populations. Recognizing the practical applications of TEK can help promote more effective environmental governance.

Kofinas (2005) research has highlighted the historical power imbalances between Western science and indigenous knowledge systems. Western science has often been imposed on indigenous communities, dismissing their knowledge and perspectives. Traditional ecological knowledge is perceived as being a competing authority with science, creating divisions between indigenous expert authorities and scientific expert authorities. These divisions can lead to conflicts and challenges in environmental governance and management.

Salmon (1996) indicates historical records and research have shown that western science has often been used as a tool of colonialism, imposing Western knowledge and values on indigenous communities. Science has been tied to colonial, imperial and other discriminatory attitudes and institutions of science toward non-Western knowledge systems. Recognizing the historical context of Western science can help to address the power imbalances between Western science and indigenous knowledge systems.

Whyte (2013c) studies have shown that integrating traditional ecological knowledge (TEK) and Western science can lead to more effective environmental management and conservation practices. TEK can be integrated with science to improve environmental governance but requires creating long-term processes that allow for the implications of different approaches to knowledge to be responsibly thought through. Successful integration requires a deep understanding of the differences and similarities between TEK and Western science.

Gondo (2022) Collaborative approaches between traditional ecological knowledge and Western science can be effective in addressing environmental challenges, such as climate change, biodiversity conservation and natural resource management. A collaborative approach between TEK and Western science involves working together to share knowledge, expertise and

perspectives to achieve common goals. This approach can lead to more effective environmental management and conservation practices, as well as improved relationships between indigenous communities and Western scientists.

Houde (2007b) traditional ecological knowledge is based on careful observations and experiences of indigenous communities. TEK can provide valuable insights into environmental patterns and processes. TEK has empirically tested (and testable) understandings of the relationships among living things and their environments. TEK is a legitimate system of knowledge production that can inform environmental governance. Recognizing the empirical basis of TEK, helps to bridge the gap between TEK and Western science. Promote more inclusive and effective environmental governance.

3. METHODOLOGY

3.1 Research Design

Data for the study was obtained from primary and secondary sources. Both the primary and the secondary data were obtained with the application of survey method with the aid of checklist through interview to elicit information from the respondents on leveraging fishers' traditional ecological knowledge (TEK) for technological development in Lake Chad Basin, Nigeria, private – public partnership approach.

3.2 Population of the Study

Kukawa local government area is domicile in Lake Chad Basin Area, Borno State of Nigeria. Kukawa Local Government Area is part of the prestigious Borno Emirate and consist of several towns and villages such as Alagarno, Yoyo, Kekeno, Kauwa, Baga Kauwa, Mile 3, Doron Baga among others. The kanuri language is widely spoken in the Local Government Area, while the religions of Islam and Christianity are practiced in the Local Government Area. Kukawa Local Government Area is situated on the shores of the Lake Chad and has an average temperature of 32 degrees centigrade. The area experiences two major seasons which are the dry and the rainy seasons. The average wind speed in the area is put at 11 kilometres per hour (OCHA, 2018). The study area is Mile 3 Baga Fishing Community, Lake Chad Basin, Kukawa Local Government Area, Borno State, Nigeria. It is in the semi- arid plain between latitude 12° 18' – 13° 48' N and longitude 13° 18' – 14° 48' East of the Greenwich Meridian (G.M.T) (Agbelege and

Ipinjolu, 2001). During the "Normal Chad" (stabilization of the Lake at normal size as a result of the influence of rainfall and volume of water flow in the major rivers that feed the basin), the composition of Lake Chad Basin comprised of Chad 11,000km2 (50%), Nigeria 5,500km2 (25%), Niger 3900km2 (17%), and Cameroon 1800km2 (8%), during the "Little Chad" the open water is shared only between Chad 1200km2 (60%) and Cameroon 800km2 (40%), the Nigerian and Niger portion are liable to complete drying, e.g. Sahelian drought of 1968 (Welcome, 1972).

The study area has a population of about two hundred and three thousand, three hundred and forty-three (203,343) inhabitants with a land area covering about 4,901km^2, National Population Commission of Nigeria (NPC, 2016). Fishing is an important economic activity in Kukawa Local Government Area as the residents of the area take advantage of the enormous sea food found in the area's water bodies. Trade also flourishes in Kukawa Local Government Area. The fisheries of the Lake Chad employ about 10,000 fishers including about 150,000 persons associated with the fisheries business (Sule, Ovie and Ladu, 2001).

The major tribes from Nigeria include the Agatu, Hausa, Jukun, Kanuri, Ijaw, Shuwa, Urhobo, Nupe, Ilaje and Ijebu and foreigners like Malian, Kotoko, Masaca, Buduma, Kanumbu. The Hausa constitutes the majority (19%) fishermen on the Nigerians part followed closely by the Jukun (16%), Agatu (11%), Malians constitute majority of the foreign fishers on the Lake. Fishing is their major occupation consisting of fisheries activities including processing, preservation, transportation and marketing. Other economic activities are farming, Cattle herding and trading, Federal Department of Fisheries (FDF), (Olaosebikan and Raji, 1998).

3.3 Sample Size and Sampling Procedure

Out of the study area total population of 203,343 inhabitants. The study targeted population of approximately 6000 to 7000 (FGD, FCFFT, Mile 3, Baga, 2023) fishers, persons and groups that are associated and considered important in the study area for the purpose of this research work were used for the study.

Survey method of data collection was employed (direct survey) the fish farmers were met at lake site, workshops for mending fishing gears, construction of fishing implements, Fish markets, fish packaging sites, fish processing and smoking sites,

mats and baskets weaving sites where production occur. This has enabled the acquisition of accurate information on the traditional ecological knowledge, cultural fishing acts and the level of operation of the cultural transformation system such as the types and the standard of the fishing gears and or implements in use and the associated methods and techniques in practice, fish farmers harvest, farm fixed assets capacity and farmers socioeconomic characteristics as applicable in the study area. Self-reporting through administrative sources (off-site) contact method was also applied for this study as information on the fishers were obtained from the research and consultancy unit, fishing gear unit, workshop unit, fish processing unit and library, information and documentation unit of the Federal College of Freshwater Fisheries Technology, Baga, Maiduguri in addition to information obtained from official of local government and state department of fisheries and other stakeholders of the fishing communities such as the traditional rulers and locally recognized heads of fishers and craftmanship in the fishing community.

3.4 Sampling Method

The sampling method used in this study was combination of survey method and direct enumeration. A purposive sampling technique, targeting fishers, persons, and groups associated with fishing activities in the study area. A total of 90 fishers were selected from three sub-sets, with 30 fishers from each sub-set. The sampling frame was constructed using checklist, and data was collected through interviews and direct observation.

The operational system of the survey was segregated in to three and were assigned sub-sample frame primarily constructed for the survey of the fishers on the formulated survey checklists as follows:

1. Identification of facilities from the production site of the farmer (field of operation) and administrative records of the fisheries institution, department of fisheries of local and state government and in the markets.

2. Direct enumeration of facilities in the production site (field of operation) in the lake site, workshops, markets and others not directly specified under a fish farmer, local producer and or a seller.

3. Interviews with the fishers, stake holders and other related members of the fishing industry either directly or indirectly related to matters connected with harvested species, permanence of equipment, the permanence density, the size of operation and on variables connected

with environmental and ecological effects of the fishing activities in the study area.

4. Self-reporting through administrative sources (off-site contact method).

3.5 Survey Questions

The survey questions applied are as stated below;

1. What are the existing traditional ecological knowledge (TEK) practices in Lake Chad Basin, Nigeria?

2. What are the traditional fishing acts and methods in Lake Chad Basin, Nigeria?

3. How can TEK be leveraged for technological development in the study area?

4. What are the potential benefits and limitations of integrating TEK with modern technology?

5. What are the key factors that facilitate successful private-public partnerships in the Lake Chad Basin, Nigeria?

6. How can TEK be documented and validated for technological development initiatives in the Lake Chad Basin, Nigeria?

7. What is the level of operation and fishing gear used in the Lake Chad Basin, Nigeria?

8. What are the potentials benefits and limitations of leveraging TEK for technological development?

9. What is the level of collaboration and knowledge sharing between stakeholders?

Example of Survey Questions includes;

a) What traditional fishing practices do you use, and how can they be improved with modern technology?

b) What traditional ecological knowledge practices do you use in your fishing activities?

c) How do you think TEK can be integrated with modern technology to improve fishing practices?

d) What are the benefits and limitations of leveraging TEK for technological development?

e) How can private – public partnerships support the integration of TEK into technological development initiatives?

3.6 Interview Analysis

The interview analysis was conducted with the used of conventional content analysis, which involved review and coding of interview data to identify themes and patterns in relations to the research objectives.

The analysis focused on exploring the potential of leveraging fisher's traditional ecological knowledge (TEK) for technological development in the Lake Chad Basin, Nigeria, through a private-public

partnership approach.

The interview data was analyzed to identify: -

1. Existing TEK practices and their relevance to technological development.
2. Potential benefits and limitations of leveraging TEK for technological development.
3. Factors facilitating successful private-public partnerships.
4. Suggestions for improving collaboration and knowledge sharing between stakeholders.

The analysis of the interview was carried out manually. Findings were presented in a narrative format, with quotes and examples from the interview data to support the results.

4. RESULTS AND DISCUSSION

4.1 Potential of Leveraging Fishers Traditional Ecological Knowledge (TEK) for Technological Development in the Lake Chad Basin, Nigeria, through a Private - Public Partnership Approach

The existing traditional ecological knowledge (TEK) practices in the Lake Chad Basin, Nigeria have been assessed based on the fact that Lake Chad Basin is home to diverse ethnic groups, each with their unique traditional ecological knowledge (TEK) practices such as knowledge of aquatic plants, understanding of water level fluctuations. The fishers are educationally backward but are very skillful in term of fishing act and other fishing occupational activities as net making, packaging and un-packaging of fish, making and sales of twine (ropes), sales of fishing gears, hiring canoes, mending of fishing gears, production and sales of fishing cards for fish drying, fish marketing, processing and preservation of fish, loading and uploading of fish, transportation of fish, sorting of fish, fishing and boat building among others. Majority of the fishers have been fishing for over twenty (20) years. They have the experience of best times to fish, the best spots and the best techniques. The knowledge of the fishers in the study area will aid in the development of more efficient fishing gear and techniques.

The result aligns with the findings of Withanage, and Lakmail Gunathilaka, (2023a).

Utilization of the traditional ecological knowledge of the fishers to address specific technological challenges such aspects as to inform water management practices (Understanding traditional water harvesting, storage techniques etc.), to promote sustainable fishing practices (identifying and protecting critical fish habits etc.), to develop more effective irrigation systems and

sustainable agricultural practices in the study area. The farmers in the study area know the best crops to plant, the best time to plant and the best ways to manage our land. The knowledge of the fishers can be used to develop more effective irrigation systems and sustainable agricultural practices.

This result aligns with the findings of Withanage, and Lakmail Gunathilaka, (2023b).

There exists potential benefits and limitations of leveraging traditional ecological knowledge (TEK) for technological development in the study area which involves improved cultural sensitivity and relevance of technological developments, increased adoption and uptake of new technologies and enhanced sustainability and effectiveness of technological developments. The potential limitations are the risk of cultural appropriation or exploitation of traditional ecological knowledge, the need for careful documentation and validation of TEK practices and the potential for TEK to be marginalized or overlooked in favor of Western scientific knowledge.

This finding is consistent with the research of Nakashima, Galloway McLean, Thulstrup, Ramos, Castillo and Rubis, (2012).

The need for Private – public partnerships to facilitate the integration of traditional ecological knowledge in to technological development initiatives by providing funding and resources for TEK documentation and validation, supporting the development of new technologies that build on existing TEK practices and facilitating collaboration and knowledge sharing between TEK holders, scientists, and policy makers which are lacking in the study area. Nevertheless, there is also no avenue for building trust, improving communication and ensuring transparency for successful partnership for the development of the economy of the local communities in the study area.

This result aligns with the findings of Withanage, and Lakmail Gunathilaka, (2023e).

Fig. 1 Cultural Fishermen in Fishing Act
Source: Library, Information & Documentation Unit, FCFFT, Mile 3, Baga, 2023
Note: Application of Cultural Fishing Implements such as Paddle, Wooden Canoe, Scoop Net and Gourd in Fishing Community.

4.2 Traditional Ecological Knowledge (TEK) Integration with Modern Technology in the Lake Chad Basin, Nigeria

There is no effective integration of traditional ecological knowledge (TEK) with modern technology in the study area considering the fact that, there is no deep understanding of the local context and TEK practices, collaboration and knowledge sharing between TEK holders, scientists, and technologists and a focus on developing technologies that are culturally sensitive and relevant to local needs is inadequate in the study area. The fishers believe that modern technology could improve their farming occupation as the members use mobile phones to access market information and get paid for their fish products, thus integration of traditional ecological knowledge with modern technology could improve the fisher's business, increase their incomes and acquisition of practical benefits in the techniques of fishing in the study area.

This result is inconsistent with the findings of Kofinas, (2005).

The fishers have rich cultural heritage and traditional knowledge in the fishing's community, thus, if the government and the private sector could work collaboratively as required the fisher's traditional knowledge could be documented and preserved for the promotion of cultural tourism and improvement in economic development but the reverse has been the case in the study area as a result of ineffective collaboration. Hence, the advantage derivable from the development of new technologies through discovery of knowledge of the local environment and social conditions, identification of potential solutions to regional challenges for onward design and testing of new technologies is inadequate in the study area.

This outcome is consistent with those of Rai and Mishra, (2022).

Fig. 2 Cultural Inland Fishing Implement, Wooden Canoe

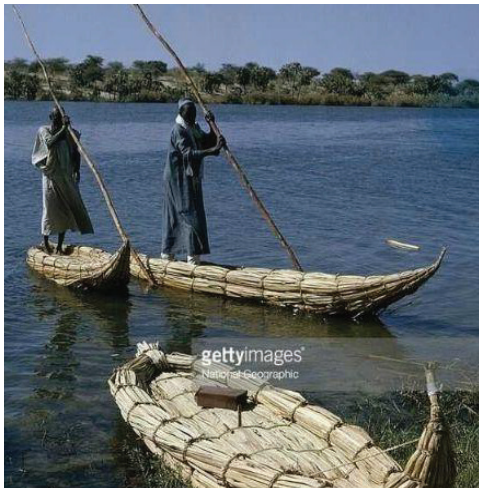

Fig. 3 Cultural Inland Fishing Implement, Tacht Canoe
Source: Gear Teahnology Workshop Unit, FCFFT, Mile 3, Baga, 2023
Note: Cultural Implements for Removing Fish from the Water Body and for Fish Pocessing and Presrvation in the Study Area.

4.3 Private – Public Partnerships in the Lake Chad Basin, Nigeria

There exists ineffective collaboration between private and the public sector in the study as a result of the desired trust, communication and transparency for fostering collaboration between the stakeholders is not achieved. The majority of the fishers in the local communities (private sector) are willing to work with the government for the development of the economy with the notion that building trust, improving communication, ensuring transparency and fostering partnership with the Western science (government) is very crucial for successful partnership.

This finding is inconsistent with those of Whyte, (2013b).

The fishers are of the point that the need for inclusive decision-making processes, regular communication and feedback mechanism for the actualization of full-swing stakeholders' engagement and participation which is ineffective to enable for technological development to prevailed in the study area. The fishers are investing and are ready to expand investment in the Lake Chad Basin but there is no stable and secure environment. The fishers also in need to work with the government in such a way that the fishers investments benefit everybody both the private and the public sectors in a sustainable way not only a few individuals.

This result aligns with the findings of Whyte, (2013c).

There is no adequate government policies and regulations that plays a critical role to facilitate private – public partnerships as there is no supportive regulatory framework in place to provide incentives for investment to enable partnerships goes hand in hand with national development goals. The government has not provided any support to create conducive environment for private – public partnerships such

as infrastructural and other services support, streamlining regulatory processes and offering tax incentives among others in the study area.

This finding is consistent with those of Gondo, (2022).

The issue of sustainability and long-term impact of private – public partnership does not arise as there exist no any private – public partnership framework in shape even if it exists, the sustainability and long-term impact of private-public partnerships required careful planning, monitoring and evaluation with due attention on local capacity building and promotion of ownership locally which is lacking in the study area. Working closely with local communities and the government enhances development of partnerships that benefit both the fishers in the local community and the government.

This result corroborates those of Houde, (2007b).

Fig. 4 Traditional Ecological Knowledge (TEK) Transformation of Fishing Implement (Canoe) in the Study Area, Dugout Canoe

Engine Boat

Outboard Engine

Motor Boat
Source: Gear Teahnology Workshop Unit, FCFFT, Mile 3, Baga, 2023
Note: Traditional Ecological Knowledge (TEK) Transformation of Fishing Implement (Canoe/Outboard Engine) in the Study Area

5. CONCLUSIONS

The study revealed that Traditional Ecological Knowledge (TEK) practices exist in the study area and could be leveraged for technological development, particularly in the areas of water resources management and sustainable fishing practices. While private-public partnerships are considered a crucial instrument for facilitating the integration of traditional ecological knowledge in to technological development initiatives, they also pose a significant challenge in the study area. Nevertheless, the study highlights the importance of government policies and regulations in supporting these partnerships and promoting the accomplishment of research objectives, a support that is currently lacking in the study area. The study has the potential to drive economic growth, improve livelihoods, and promote sustainable development but lacks careful planning, collaboration, and knowledge sharing between stakeholders such as the local community fishers, scientists, policy makers, and private sector representatives. The importance of the idea of building trust, improving communication, and ensuring transparency in private-public partnership in the development of technology on the basis of traditional ecological knowledge has been revealed by the study.

Based on the study's findings, the following recommendations are proposed:

1. Documentation and Validation of Traditional Ecological Knowledge (TEK) Practices: Collaborative efforts between the government and private sector are necessary to document and validate Traditional Ecological Knowledge (TEK) Practices in the Lake Chad Basin, Nigeria.

2. Culturally Sensitive Technology Development: Technologies developed for the region should prioritize cultural sensitivity and relevance to local needs.

3. Collaboration and Knowledge Sharing: Encouraging collaboration and knowledge sharing among traditional ecological knowledge holders, scientists, policy makers, and private sector representatives is crucial for integrating traditional ecological knowledge into technological development initiatives.

4. Supportive Regulatory Framework: The government should establish a supportive regulatory framework for private-public partnerships, such tax incentives, streamlined processes, and infrastructure support.

5. Sustainability and Long-term Impact: Private-public partnerships should be designed with a focus on sustainability and long-term impact, prioritizing local capacity building and promoting local ownership.

6. Inclusive Decision-Making: Decision-making processes should be inclusive, providing opportunities for stakeholder participation and feedback.

7. Monitoring and Evaluation: Regular monitoring and evaluation of private-public partnerships are essential to ensure they meet their objectives and positively impact local communities.

DATA AVAILABILITY STATEMENT

All data are included in the manuscript. Data can be shared due to non-confidentiality and has no any ethical restrictions.

AI DISCLOSURE

I Babagana Zanna acknowledge the used of Meta AI only for language editing under my complete control and responsibility. I accept the full responsibility for the accuracy and integrity of the final version.

REFERENCES

[1] Agbelege, O. O., and J. K. Ipinjolu. 2001. An Assessment of the Exploitation and Management of the Fishery Resources in the Nigerian Portion of Lake Chad. Journal of Arid Zone Fisheries, Volume1,

June 2021. [2] Berkstrom, C., M. Papadopoulos, W.S. Jiddawi, and L.M. Nurundi. 2019. Fishers Local Ecological Knowledge (LEK) on Connectivity and Seascape Management. Section of Marine Fisheries, Aquaculture and Living Resources, Volume 6, 2019. https://doi.org/10.3389/fmars2019.00130.

[2] Berkes, F. 2012. Sacred Ecology (3rd edition). Routledge. Importance of Integrating Traditional Ecological Knowledge with Modern Science. Environment and Sustainability, Geography, Social Science. New York, eBook ISBN 9780203123843, PP.394,29/03/2012. https://doi.org/10.4324/9708203123843.

[3] Federal College of Freshwater Fisheries Technology (FCFFT), Mile 3, Baga. 2023a. Focal Group Discussion with the Staff of Library, Information and Documentation Unit.

[4] Federal College of Freshwater Fisheries Technology (FCFFT), Mile 3, Baga. 2023b. Focal Group Discussion with the Staff of Gear Technology Unit.

[5] Gondo, R. 2022. Integration of Traditional Ecological Knowledge and Western Science in Natural Resources Management in the Okavango Delta, Botswana. Journal of African Studies and Development; J Afr. Stud. Dev. ISSN:2141-2189. Number-C5D458069936/Vol.14(4). Pp.-141-153, October 2022. https://doi.org/10.5897/JASD2021.0649.

[6] Houde, N. 2007a. The Six Faces of Traditional Ecological Knowledge: Challenges and Opportunities for Canadian Co-management arrangements. Ecol. Soc. 12(2):17(34). https://www.jstor.org/stable/26267900.

[7] Houde, N. 2007b. The Six Faces of Traditional Ecological Knowledge: Challenges and Opportunities for Canadian Co-management arrangements. Ecol. Soc. 12(2):17(34). https://www.jstor.org/stable/26267900.

[8] Kofinas, G.P. 2005. Caribou Hunters and Researchers at the Co-management Interface: Emergent Dilemmas and the Dynamics of Legitimacy in Power Sharing. Anthropological 47(2):179-196. https://cassca.journals.uvic.ca/index.php/anthropological/article/view/2382.

[9] Kusters, K., and Y. Wang. 2013. The Role of Traditional Ecological Knowledge in Forest Management: A Review Forest Ecology and Management, 307, 15- 24. https://doi.org/:10.1016/j.landusepol.2018.09.001.

[10] Muritala, O. O. 2022. Tackling Lake Chad Basin Challenges with Climate Resilient Technologies. Jurnal Lembaga Katahanan

Persatuant Nasional Indonesia (JPPNI).10(2):22 – 32. https://doi.org/:10.55960/jlri.v10j.v10j2.275.

[11] Nakashima, D., K. Galloway McLean, H. Thulstrup, A. Ramos Castillo, and J. Rubis. 2012. Weathering Uncertainty: Traditional Knowledge for Climate Change Assessment and Adaptation. United Nations University (Japan) Traditional Knowledge Initiative Paris, UNESCO, and Darwin, UNU, ISSN: 979-92-3-001068-3, 978-0-9807084-8-6, 12P. https://www.unesco.org/979-92-3-001068-3.

[12] National Population Commission (NPC). 2016. National Population Commission of Nigeria, 2006 Census Report.

[13] Office for the Coordination of Humanitarian Affairs (OCHA). 2018. United Nations; Nigeria - Administrative Boundaries (Levels 0 – 3). Nigeria – Borno State: Konduga LGA Reference Map as at February 2018.

[14] Olaosebikan, B. D., and A. Raji. 1998. Field Guide to Nigerian Freshwater Fishes; Food and Agriculture Organization of the United Nations (FAO). https://agris.fao.org.

[15] Rai, S.C., and P.K. Mishra. 2022. Traditional Ecological Knowledge and Resource Management. AConceptual Framework in Rai, S.C., Mishra, P.K. (eds) Traditional Ecological Knowledge of Resource Management in Asia. Springer, Charm. https://doi.org/10.1007/978-3-031-16840-6-1.

[16] Salmon, E. 1996. Decolonizing our Voices, Winds Change 1996, 11(3):70-72, p70-72 Sum 1996, EJ531384. U.S. Department of Education (gov). https://eric.ed.gov.

[18] Sule, O. D., S. I. Ovie, and B. M. B. Ladu. 2001. Marketing and Distribution of Fish from Lake Chad. Fisheries Society of Nigeria, (FISON) 2001. National Institutes of Freshwater Fisheries Research New Bussa, Niger State of Nigeria. Techniques of the Fishery Resources in the Nigerian Portion of Lake Chad. Journal of Arid Zone Fisheries (JAZFI) Volume 1, June 2001.

[17] Welcome, R.L. 1972. The Inland Waters of Africa, CIFA Technical Paper (i) 117p.

[18] Whyte, K.P. 2013. On the Role of Traditional Ecological Knowledge as a Collaborative Concept: A Philosophical Study, Ecol Process 2,7(2013). https://doi.org/10.1186/2192-1709-2-7.

[19] Withanage, W.K.N.C., and M.D.K. Lakmali Gunathilaka. 2023a. Theoretical Framework and Approaches of Traditional Ecological Knowledge. DOI:10.1007/978-3-031-16840-6-3, In book: Traditional Ecological

Knowledge of Resources Management in Asia (pp.27-43). https://ww.researcgate.net/pub.

[20] Withanage, W.K.N.C., and M.D.K. Lakmali Gunathilaka. 2023b. Theoretical Framework and Approaches of Traditional Ecological Knowledge. DOI:10.1007/978-3-031-16840-6-3, In book: Traditional Ecological Knowledge of Resources Management in Asia (pp.27-43). https://ww.researcgate.net/pub.

[21] Withanage, W.K.N.C., and M.D.K. Lakmali Gunathilaka. 2023c. Theoretical Framework and Approaches of Traditional Ecological Knowledge. DOI:10.1007/978-3-031-16840-6-3, In book: Traditional Ecological Knowledge of Resources Management in Asia (pp.27-43). https://ww.researcgate.net/pub.

[22] Withanage, W.K.N.C., and M.D.K. Lakmali Gunathilaka. 2023d. Theoretical Framework and Approaches of Traditional Ecological Knowledge. DOI:10.1007/978-3-031-16840-6-3, In book: Traditional Ecological Knowledge of Resources Management in Asia (pp.27-43). https://ww.researcgate.net/pub.

[23] Withanage, W.K.N.C., and M.D.K. Lakmali Gunathilaka. 2023e. Theoretical Framework and Approaches of Traditional Ecological Knowledge. DOI:10.1007/978-3-031-16840-6-3, In book: Traditional Ecological Knowledge of Resources Management in Asia (pp.27-43). https://ww.researcgate.net/pub.