



**JOURNAL OF
DEFENSE
RESOURCES
MANAGEMENT**

Vol. 16 Issue 2(31)/ 2025

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

- Dr. TEODOR FRUNZETI, Professor - Academy of Romanian Scientists, (Romania)
Dr. WILLIAM D. HATCH, Senior Lecturer, MS - Center for Executive Education (CEE), Naval Postgraduate School, Monterey, CA (USA)
Dr. GRETA KEREMIDCHIEVA, Senior Lecturer and Director of Language Training, Rakovski Defense & Staff College, National Defense Academy, Sofia, (Bulgaria)
CRISTIANA (CHRIS) MATEI, Senior Lecturer - Center for Homeland Defense and Security (CHDS), Naval Postgraduate School, Monterey, CA (USA)
Dr. ETLEVA SMAÇI - Vice Rector and International Affairs Professor - Albanian Armed Forces Academy, Tirana (Albania)
Dr. VLADAN HOLCNER, Professor and Director of the Language Centre, National University of Defense, Brno (Czech Republic)
Dr. PAVEL FOLTIN, Head of Department of Defence Analysis, Center for Security and Military Strategic Studies, National University of Defense, Brno (Czech Republic)
Dr. ADI-MARINEL MUSTAȚĂ - "Carol I" National Defense University (Romania)
Dr. FLORIN-EDUARD GROSARU, Professor - Regional Department of Defense Resources Management, Studies, Brasov, Romania
Dr. CATALIN CIOACA, Associate Professor, Eng. - "Henri Coanda" Air Force Academy (Romania)
Dr. MIRCEA BOSCOIANU, Professor, Eng. - "Transilvania" University, Brasov (Romania)
Dr. ADRIAN POPA, Associate Professor, Eng. - "Mircea cel Batran" Naval Academy, Constanta, (Romania)
Dr. ALEXANDRU BABOS, Associate Professor, - "Nicolae Balcescu" Land Forces Academy Sibiu, (Romania)
Dr. MONICA RAILEANU SZELES, Professor - "Transilvania" University, Brasov (Romania)
Dr. MUSTAFA KEMAL TOPCU, Lecturer - National Defense University (Turkey)
Dr. ALEXANDRU STOICA, Senior Lecturer - "Carol I" National Defense University (Romania)
Dr. BADEADOREL, Professor - "Nicolae Balcescu" Land Forces Academy Sibiu, (Romania)
Dr. CIPRIAN SAU, Senior Scientist, Military Equipment and Technologies Research Agency (METRA) (Romania)
Dr. CONSTANTIN NICOLAE TOADER, Senior Scientist, Research and Innovation Center for CBRN Defense and Ecology (Romania)
Dr. ILEANA TACHE, Professor - "Transilvania" University, Braşov (Romania)

EDITORIAL BOARD

- Editor in Chief:** Dr. CEZAR VASILESCU, Professor habil., Eng. - Regional Department of Defense Resources Management Studies (DRESMARA), Brasov, (Romania)
- Deputy Editor in Chief:** Dr. JOHN T. CHRISTIAN - College of Information and Cyberspace, National Defense University, Washington DC, (USA)
- Executive Editor:** Dr. AURA CODREANU, Associate Professor - Regional Department of Defense Resources Management Studies (DRESMARA), Brasov, (Romania)
- Senior Editors:** Dr. Mitch J. McCARTHY - Defense Resources Management Institute, Naval Postgraduate School, Monterey, California, (USA)
- Dr. David C. EMELIFEONWU - Royal Military College, Kingston, (Canada)
- Dr. Piotr GAWLICZEK - Cuiavian University, Wloclawek (Poland)
- Dr. Cristina ANTONOAIIE, Lecturer - Regional Department of Defense Resources Management Studies (DRESMARA), Brasov, (Romania)

Dr. Livia TATAR (Romania)

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

***DISCLAIMER:** The authors take full responsibility for the contents of their papers (according to the provisions of Law no. 183/2024 on the status of research, development and innovation personnel) and for any copyright infringements. The articles in this journal do not reflect in any way the position of the editorial or advisory boards. No part of this publication may be reproduced, partially or totally, without the prior written permission of the editorial board.*



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 margins 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, left 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: <http://www.jodrm.eu>

PRINTED AT THE MILITARY TECHNICAL PUBLISHING CENTER



CONTENTS

ARTIFICIAL INTELLIGENCE – THE PREMISE OF A NEW REVOLUTION IN MILITARY AFFAIRS	9
<i>Daniel DOICARIU</i>	
FIVE BASIC MILITARY STRATEGIES AND THEIR MODERN IMPLEMENTATION ...	25
<i>Rashad TAHIROV, Sadi SADIYEV, Hikmet HASANOV</i>	
CHARACTERIZING THE MILITARY CAREER OF ARTILLERY OFFICERS AND SERGEANTS IN THE PORTUGUESE ARMY: DETERMINANTS, CHALLENGES AND OPPORTUNITIES	45
<i>Maria DÂMASO, David Pascoal ROSADO</i>	
A NOVEL INSTRUCTIONAL DESIGN MODEL FOR MILITARY ACADEMIES: VALIDITY EVIDENCE FROM GENDARMERIE OFFICER CADETS	59
<i>Steven HORNSTRA, Steven DURNING, Jaap HOOGENBOEZEM, Paul NEELISSEN, Walther VAN MOOK</i>	
THE MILITARY LEADER'S CHALLENGE: ACHIEVING THE BALANCE BETWEEN SUBORDINATES' PERSONAL VALUES AND ORGANIZATIONAL VALUES	93
<i>Cristian DRAGOMIR</i>	
MOTIVATION, COMPETENCE, AND ADAPTABILITY: LEVERAGING CIVILIAN-MILITARY TALENT SYNERGY AS UKRAINE'S STRATEGIC HUMAN RESOURCE ADVANTAGE	105
<i>Arsen BIEKIROV</i>	
PRINCIPLES-BASED LEADERSHIP AND ITS IMPACT ON MILITARY ORGANIZATION EFFECTIVENESS	113
<i>Cristian DRAGOMIR, Lucia BOROTA</i>	
THE IMPACT OF DIGITAL LEADERSHIP IN THE AIRLINE INDUSTRY ON EMPLOYEE PERFORMANCE: AN EMPIRICAL STUDY	123
<i>Salih AYGÜN, Ülkü UZUNÇARŞILI</i>	
NATO'S NEW FORCE MODEL: ADAPTING TO A DYNAMIC SECURITY LANDSCAPE	141
<i>Khayal Iskandarov IBRAHIM, Piotr GAWLICZEK</i>	
BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE FOR ENHANCED INFORMATION SECURITY IN MILITARY COMMUNICATION SYSTEMS	157
<i>Fiodor TIMERCAN</i>	
DIGITAL SHIELD: INTEGRATING HEALTH INTELLIGENCE INTO NATO'S DEFENSE STRATEGY	165
<i>Dimitra BALASKA, Dimitris KARAFERIS, Ioannis REMATISIOS, Yannis POLLALIS</i>	

FOOD SECURITY CONCEPTS: HISTORICAL EVOLUTION AND CURRENT STAETE	191
<i>Vasile SACOVICH, Vitalii CAZACU</i>	
SECURITY CULTURE - A NEED OF THE POPULATION	203
<i>Nicolae CHIMERCUC</i>	
ORGANIZATIONAL RESOURCE MANAGEMENT AND ENVIRONMENTAL SUSTAINABILITY. A TIME-SERIES ANALYSIS OF ICT SECTOR GREENHOUSE GAS EMISSIONS IN ROMANIA (2013-2022).....	215
<i>Cristina ANTONOAIIE, Aura CODREANU</i>	
COMPARATIVE ANALYSIS OF SATELLITE BATTERY TECHNOLOGIES	239
<i>Andrew H. CHUNG, Michael J. BROWN, Robert D. FASS, Clay M. KOSCHNICK</i>	
THE EVOLUTION OF SOCIAL MEDIA PLATFORMS AS INSTRUMENTS OF PROPAGANDA, DISINFORMATION AND MEDIA SUBVERSION IN MODERN CONFLICTS	257
<i>George – Adrian AIONESEI</i>	
KEEPING THE BALANCE BETWEEN ETHICS AND EFFECTIVENESS IN COMMUNICATION	275
<i>Brîndușa Maria POPA</i>	
EXAMINING THE UNITED STATES AIR FORCE FIGHTER AIRCRAFT SUPPLY CHAIN: HOW NATIONAL SECURITY, BUDGETING, AND MANPOWER CHALLENGES IMPACT MISSION CAPABILITY	287
<i>Ciara C. WETZLER, Robert O. WALTON</i>	
THE ENCOURAGEMENT OF ARMS EXPORT IN DEVELOPING COUNTRIES: CAUSALITY ANALYSIS BETWEEN DEFENSE EXPORT, GDP AND DEFENSE EXPENDITURE IN TURKIYE	303
<i>Meliha ENER, Nazan YELKIKALAN, Selen SAVAŞKAN</i>	
SOLUTION OF TASK OPTIMAL PLANNING OF AIR DEFENSE MEANS AGAINST LOW-ALTITUDE AIR TARGETS	319
<i>Arzuman G. GASANOV</i>	
BLUE ECONOMY, MARITIME RESILIENCE, AND A SYMBOL OF SOVEREIGNTY: AN INTEGRATIVE STUDY OF BERHALA ISLAND AS A STRATEGIC DEFENCE POINT	329
<i>Susilawati, Sutanto, Adnan Madjid, Totok Imam Santoso</i>	

ARTIFICIAL INTELLIGENCE – THE PREMISE OF A NEW REVOLUTION IN MILITARY AFFAIRS

Daniel DOICARIU

"CAROL I" National Defense University, Bucharest, Romania

This article is predominantly forward-looking, exploring the possibility of shaping a sixth Revolution in Military Affairs (RMA) by identifying scientific foundations that can support this trend. Although the concept of RMA has been intensively analyzed and exploited in recent decades, the emergence of disruptive technologies, especially in the field of artificial intelligence, raises the possibility of significant transformations not only at the technological level, but also in terms of the doctrines and operational concepts of the armed forces. The interest in artificial intelligence, far from being a novelty in the technological sphere, has reached a level of maturity that justifies analyzing its potential to dominate the future of warfare and "military affairs" as a whole.

Key words: *revolution in military affairs, emerging and disruptive technologies, artificial intelligence, innovation.*

1. INTRODUCTION

Using the term "*revolution*" to describe profound transformations in the military domain is conceptually problematic, as ignoring the temporal dimension of these changes can lead to theoretical confusion. Although the term suggests rapid and radical change, history shows that such transformations in the military often happen over long periods of time, which calls for a critical rethinking of the validity of the concept of "*revolution*" in analyzing military developments.

In the contemporary era, phenomena associated with war

and the impact of technology on the military domain have been conceptualized predominantly through two major analytical frameworks: the "*military revolution*" and the "*revolution in military affairs*" (RMA). These concepts, although related, reflect significant differences in the origin, extent and nature of the changes analyzed.

The concept of "*military revolution*", introduced by Michael Roberts in 1956, has been extensively analyzed by numerous researchers over the past few decades. Although no clear consensus has emerged on the defining features of military

revolution, academic debates have highlighted the analytical potential of this concept in investigating structural, organizational, and technological transformations in the military domain.

Military revolutions are *"changes to the framework of war; recasting societies and states in addition to military organizations"* (Morris: 2024), while RMA requires *"the assembly of a complex mix of tactical, organizational, doctrinal, and technological innovations in order to implement a new conceptual approach to warfare or to a specialized sub-branch of warfare"* (Knox, Murray: 2001, p.26). In other words, revolutions in military affairs represent profound and accelerated transformations in the conduct of warfare, driven by technological, doctrinal, and organizational developments that fundamentally influence how armed forces train, conduct operations, and achieve military objectives.

In the context of emerging and disruptive technologies such as artificial intelligence, autonomous drones, nanotechnologies, or advanced cyber capabilities, it becomes all the more important to critically reevaluate the validity and relevance of using the term *"revolution"*. This approach must take into account the complexity of the processes involved and the danger of oversimplifying historical and

contemporary realities, especially in an era in which technological innovation is constantly redefining the paradigms of armed conflict.

2. RMA FROM THE PERSPECTIVE OF MILITARY ACTIONS

The increasing deployment of high technologies within military structures is not, in essence, a new phenomenon. The concept of *Revolution in Military Affairs*, used as a conceptual alternative to the term *Military-Technical Revolution* (Krepinevich: 2002), refers to a complex process of structural transformation involving significant operational, organizational, and technological changes in the way military actions are conducted. RMA has its origins in doctrinal changes, and its course has been decisively shaped by technological advances. In specific, the combination of systems that collect, process, and transmit information with those that generate and apply military force has led to a profound transformation in how combat is understood and conducted. This close link between technology and doctrine has fundamentally changed both the strategies of action and the current structure of the armed forces.

Theoretical approaches focused on this topic date back to the end of World War II (Murray: 1997, p. 1), but large-scale research began with

the publication of a DoD report in 1992 on the next technical-military revolution, which later became known as the RMA (Bartosiak: 2019, p. 1).

A point of view expressed by Tilford from the US Institute for Strategic Studies stated that RMA represents *"a major change in the nature of warfare brought about by the innovative application of technologies which, combined with dramatic changes in military doctrine, and operational concepts, fundamentally alters the character and conduct of operations"* (Tilford: 1995).

Another point of view accepted in many papers and reports was that of Andrew Marshall, who affirmed that: *"a Revolution in Military Affairs (RMA) is a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts, fundamentally alters the character and conduct of military operations"* (McKittrick et al.: 1998, p. 65).

After thoroughly reviewing the specialized literature, we found that the information presented by MacGregor Knox and Williamson Murray in their publication *The dynamics of military revolution, 1300-2050*, is consistent, arguing that, from 1618 to the present,

humanity has gone through *five military revolutions*. (Knox, Murray: 2001):

- the rise of the modern state and modern military institutions in the 17th century;
- the French Revolution at the end of the 18th century, which combined the forces of nationalism with military power;
- the industrial revolution, which began at the end of the 18th century and provided national armies with modern technology and logistics;
- The World War I, which represented the synthesis of the forces initiated by the French Revolution and the Industrial Revolution;
- the development of nuclear weapons and ballistic missile launch systems towards the end of World War II, which prevented a large-scale war between the superpowers during the Cold War.

Throughout history, states have constantly tried to *"innovate"* in order to consolidate their military superiority. However, what has profoundly transformed the nature of armed conflict over the last two centuries has been not only rapid technological evolution, but also its interaction with operational and organizational changes. The profound technological transformation of

warfare has been the result of a cumulative process, characterized by major progress at different stages in history. From transportation and communication means such as railways, telegraphs, steamships, and rifles (between the Napoleonic Wars and the American Civil War) to the transition to steam-powered armored hulls (late 19th century), each innovation reshaped the way armed conflicts were conducted. Then, the machine gun, aircraft, submarine, and armored vehicles, followed by the internal combustion engine, radio and radar, set the stage for the world conflicts of the 20th century. During and after World War II, nuclear weapons and ballistic missiles totally changed the global strategic balance. Finally, the last decades of the 20th century brought a digital revolution in the military field, through the integration of information technology, microelectronics, lasers, and satellite systems. (Kak: 2000).

An interesting interpretation is provided by Hundley, who argues that an RMA involves a paradigm shift in the nature and conduct of military operations that either renders one or more core competencies of a dominant actor obsolete or irrelevant, or creates one or more new core competencies in a new dimension of warfare, or both (Hundley: 1999. p. 9). The revolution in military affairs involves a profound and systemic change that redefines not

only the means of combat, but also the way of thinking, from the tactical to the strategic level.

The academic community's interest in the concept of RMA has never waned, with a constant search for new technological models that could bring about a new "*revolution in military affairs*". In the paper *A retrospective on a so-called revolution in military affairs, 2000-2020* we find a comparative analysis of the predictions made in the book *Tehnological change and the future of warfare* by the same author, Michael O'Hanlon. Referring to 29 technologies analysed in terms of their revolutionary potential, he highlighted that only computers (hardware and software) met the criteria established in 2000 for revolutionary technologies, and that eight categories would see major advances: "*chemical sensors, biological sensors, radio communications, laser communications, robotics, radio-frequency weapons, nonlethal weapons, and biological weapons*" (O'Hanlon: 2018, p. 1), as shown in Figure 1.

Since we consider O'Hanlon's research results to be of real interest to the present work, in order to anticipate how emerging and disruptive technologies (EDT) in the military field, as well as the time horizon required for further technological developments, we present in Figure 1 the estimates revised in 2018.

Table 1. Estimates of progress in key technologies (O’Hanlon: 2018, p. 6)

Category	Technology	Moderate	High	Revolutionary	Revised, 2018
Sensors	Chemical sensors		X		Moderate
	Biological sensors		X		Moderate
	Optical, infrared, and UV sensors	X			No change
	Radar and radio sensors	X			High
	Sound, sonar, and motion sensors	X			No change
	Magnetic detection	X			No change
	Particle beams (as sensors)	X			No change
Computers and communications	Computer hardware			X	No change
	Computer software			X	No change
	Radio communications		X		Moderate
	Laser communications		X		Moderate
Projectiles, propulsion, and platforms	Robotics		X		Revolutionary
	Missiles	X			High
	Explosives	X			No change
	Fuels	X			No change
	Jet engines	X			No change
	Internal-combustion engines	X			No change
	Rockets	X			No change
	Ships	X			No change
	Armor	X			No change
	Stealth	X			No change

Category	Technology	Moderate	High	Revolutionary	Revised, 2018
Other weapons	Radio-frequency weapons		X		Moderate
	Nonlethal weapons		X		Moderate
	Biological weapons		X		Moderate
	Other weapons of mass destruction	X			No change
	Particle beams (as weapons)	X			No change
	Electric guns	X			No change
	Lasers	X			No change
	Long-range kinetic energy weapons	X			No change

In support of the idea expressed by O'Hanlon, according to which most defense systems require several decades for development, testing and implementation, we illustrate the PATRIOT (*Phased Array Tracking*

Radar to Intercept on Target) surface-to-air missile system, presented in a 1994 article in the USA and which was introduced in the Romanian Army in 2020 (Figure 2).

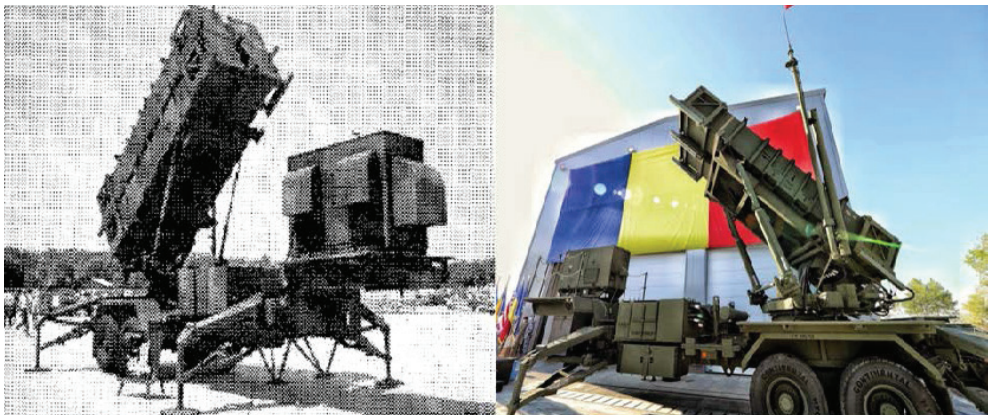


Fig. 1 PATRIOT surface-to-air missile system
(Fitzsimonds, Van Tol: 1994, p. 30; Forțele Aeriene Române: 2020)

The real revolution in military affairs is forcing modern states to use military technological advances to focus on minimizing civilian casualties and collateral damage rather than destroying the enemy. In some cases, this transforms the laws of war designed for totally different types of combat into a political and propaganda weapon in the hands of non-state actors and nations that use asymmetric means of combat (Cordesman: 2014).

Starting from the Revolution in Military Affairs (RMA) from the perspective of military action, it is necessary to identify, from a wide range of emerging and disruptive technologies, those technologies that are of particular strategic relevance in current armed conflicts. Artificial intelligence (AI) stands out as one of the most influential technologies, with a significant and indisputable presence in modern theaters of operations, particularly in the conflicts in Ukraine, Syria, and Iran over the past decade.

3. PERSPECTIVES OF A NEW RMA DETERMINED BY ARTIFICIAL INTELLIGENCE

Every revolution in military affairs has been the result of a combination of several innovations in technology, doctrine and organization. Consequently, Figure 3

shows a complex model of the discovery process in which RMAs are the result of multiple innovations. The innovative stages in this model are as follows (Hundley: 1999, pp. 23-24):

- a new technology (or several new technologies) that enables the use of devices and systems that were not previously possible or anticipated;
- a new device based on this new technology that does something that could not be done before;
- a new system, based on the new device, which performs a military task either much better or much differently than before;
- a new operational concept that describes how the new system is used in a particular type of military situation, performing a particular military task either much better or much differently than before, or performing a new task that did not exist before;
- a new doctrine and a new force structure - a doctrine that defines the principles governing the use of the new system and the force structure that provides the military organization necessary to fully realize its potential.

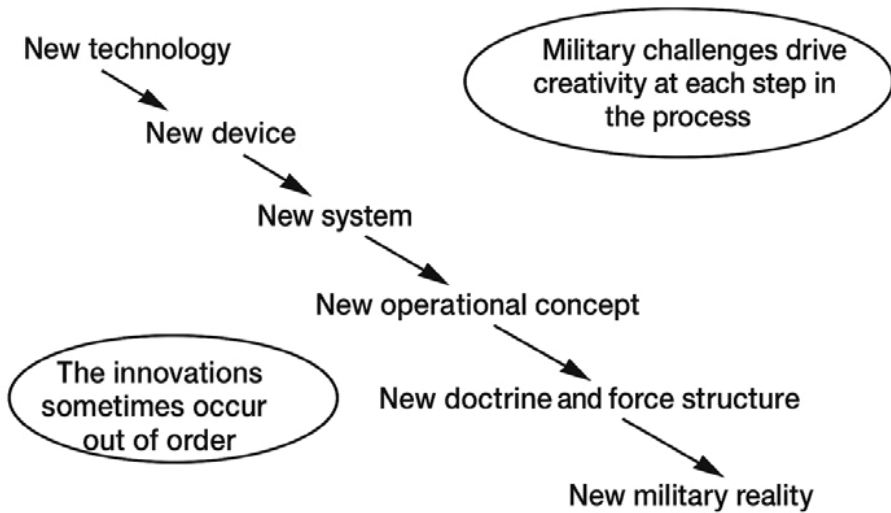


Fig. 2 A model of the RMA process as a result of multiple innovations (Hundley: 1999, p.24)

From the analysis of Figure 3 and the innovative phases listed by Hundley, we observe that unresolved military challenges represent an essential catalyst for innovation in the military transformation process, stimulating the combination of technologies into functional systems and generating the development of operational concepts, doctrines, and force structures. In the absence of such challenges, technological and doctrinal progress is improbable. The RMA process is vulnerable to discontinuities at any phase, from the development of new technology to the adoption of a new military reality. Obstacles such as the absence of an adequate operational concept, cultural resistance to change, or the inability to integrate new devices into coherent systems can block or nullify

the entire transformation process.

In the following, the possibility that technologies currently classified as emerging and disruptive may constitute the premises for triggering a new Revolution in Military Affairs will be examined, with reference to the preconditions theorized by Fitzsimonds and Van Tol (1994, pp. 25-26), namely:

- *technological development* - simply inventing a technology is not enough; practical integration into military systems is also necessary;
- *doctrinal and/or operational innovation* - to exploit the full potential of new systems, new technologies must be integrated into new operational concepts and doctrine;

- *organizational adaptation* - the most profound changes also involve bureaucratic changes and institutional acceptance.

The RMA is a direct result of the convergence of three essential conditions, each amplifying the effect of the others.

The development of new technologies over the last decade has been unprecedented. With regard to the contribution of these new technologies to the development of military capabilities, we may consider this criterion to be fulfilled, with examples including the use of artificial intelligence, autonomous systems, quantum technologies, biotechnology, hypersonic systems, space technology, novel materials and manufacturing, as well as energy and propulsion, and next-generation communications networks (NATO: 2023).

In terms of *doctrine*, the changes that have taken place at NATO, European Union, and national levels have resulted in the development of relevant strategies, programs, and doctrinal documents, including the following:

- NATO's Quantum Technologies Strategy (NATO: 2024);
- NATO's revised Artificial Intelligence Strategy (NATO: 2024);
- NATO Science & Technology Strategy (NATO: 2025);
- A Drone Strategy 2.0 for a Smart and Sustainable

Unmanned Aircraft Eco-System in Europe (EU: 2022);

- Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (EU: 2024);
- National Strategy for the Implementation of 5G Technology (Official Gazette of Romania: 2019);
- National Strategy on Artificial Intelligence 2024-2027 (Official Gazette of Romania: 2024);
- National Strategy in the Field of Quantum Technologies for the period 2024-2029 (Official Gazette of Romania: 2024);
- National Strategy for the Development and Support of Digitalization through Digital Innovation Centers in Romania 2024-2027 (Official Gazette of Romania: 2024).

The constant interest of NATO and the EU in the development of EDT *"as evidenced by both their structural and organizational adjustments, as well as the financial resources committed. Moreover, the stated ambition to engage the private sector and industry is expected to accelerate the achievement of the established objectives"* (Doicariu, Acsinte: 2025, p.259).

The third pillar necessary for establishing a new RMA, *organizational adaptation*, is easier to quantify, given that structural and

organizational changes are often public, and here we refer to the establishment of new structures with duties related to EDT. Thus, there are institutions or bodies such as the Office of the Special Envoy for Critical and Emerging Technology (S/TECh) - USA, the NATO Advisory Group on Emerging and Disruptive Technologies, Defence Innovation Accelerator for the North Atlantic (DIANA) or the Euro-Atlantic Resilience Centre (E-ARC).

An additional argument is NATO's recognition of cyberspace (NATO Summit: 2016) and outer space (NATO Summit: 2019) as distinct operational domains, highlighting the alliance's expansion and adaptation to the new realities of technology, where AI has made its mark, significantly influencing both domains.

An essential question that arises in this context is the following: *What happens when a disruptive technology becomes so advanced and complex that, once integrated into existing combat systems, it fundamentally redefines the battlefield?*

Just as the advent of nuclear weapons radically changed military doctrines and strategies in the 20th century, *I think that artificial intelligence can be expected to generate a profound reassessment of social and institutional structures in all areas of DIME (diplomatic, information, military, economic).*

Intelligence is increasingly emerging as a driver of structural change in the defense sector, directly influencing the way in which operational concepts and current military organization are being redefined. It is not just a disruptive technology, but a strategic tool with significant potential to reshape military practices and thinking.

Artificial intelligence is a "*force*" in the dynamics of current military conflicts, profoundly influencing military capabilities, planning and resource allocation, and the execution of operations. The implementation of AI in defense infrastructure and military equipment is helping to redefine how states manage their national security and conduct combat operations, marking a paradigm shift in the conduct of warfare. Among the areas where AI is exerting a significant influence on modern warfare are the following (Mocanu: 2024, p.532):

- *Autonomous weapons and systems:* AI has a major role in the development of autonomous drones and unmanned vehicles. These systems are capable of performing reconnaissance, surveillance and combat missions without the need for human involvement;
- *Intelligence, Surveillance, and Reconnaissance (ISR):* AI ensures the processing of large volumes of data

- from satellites, sensors, and surveillance platforms, enabling real-time analysis of the enemy, terrain, and potential threats;
- *Cyber warfare*: malware and hacking tools based on artificial intelligence can infiltrate enemy networks, disrupt critical infrastructure, and compromise communications systems (offensive capabilities). Also, machine learning algorithms can detect anomalies in network traffic, anticipate potential vulnerabilities, and automate defensive measures such as neutralizing threats or restricting access (defensive mechanisms);
 - *Decision-making process*: AI can assess complex situations on the battlefield, process multiple data sources, and recommend the best decisions or courses of action;
 - *Predictive analysis*: AI algorithms can process large amounts of data, including historical battle records, weather patterns, and geopolitical information, to predict enemy movements and intentions. In addition, AI systems can forecast the outcomes of military strategies by simulating different battlefield scenarios and enemy reactions;
 - *Automatization of military supply chains*: AI optimizes logistics by managing inventories, forecasting supply demand, and automating the transport and distribution of resources in conflict zones;
 - *Information warfare and psychological operations*: Psychological operations based on artificial intelligence can use social media platforms and news channels for these purposes. Artificial intelligence is also used to identify and combat disinformation campaigns by detecting fake content, deepfakes, and tactics used to manipulate social media.

The war in Ukraine provides an unprecedented operational space where military capabilities integrated with artificial intelligence are continuously tested under real combat conditions. This accelerated exposure drives rapid development of technological solutions, stimulated by the constant need for operational efficiency and adequate responses to ever-changing threats. The rapid implementation of AI solutions has highlighted their ability to act simultaneously as force multipliers, laying the groundwork for a profound transformation in the way military operations are conceived and executed.

One of the essential functions of AI in this context is to create a common operational picture by aggregating and correlating data from multiple sources such as sensors, drones, IT platforms, or mobile devices. This capability gives commanders a better understanding of the battlefield and supports accelerated decision-making.

In addition, AI contributes to the simultaneous management of a large number of assets and resources, thereby facilitating decentralized command and increased tactical agility. This type of technological integration has generated multiple practical initiatives in the Ukrainian army, particularly in the field of drone warfare, where AI optimizes both the target identification process and the execution of strikes with increased precision.

These developments increasingly validate the fact that AI is not just a technological resource, but is capable of redefining the balance between speed, accuracy, and lethality in modern conflicts. The Ukrainian case could represent not only an intermediate stage of a new RMA, but also the beginning of an operational paradigm in which superiority is no longer determined exclusively by volume or technique, but by informational and decision-making efficiency. AI is a fundamental technology for the transition from automated systems to autonomous systems, or systems that can decide

how to achieve a goal, rather than simply executing algorithms programmed by humans (Bondar: 2025, p.1). Achieving total autonomy in the use of artificial intelligence remains, at present, a goal constrained by technological, legal, and ethical factors. The conflict in Ukraine is a key example of the accelerated implementation of artificial intelligence-based technologies in the military domain. The information and experience gained in this context will significantly shape international debates on the use of AI in defense, influencing the evolution of combat doctrines, ethical norms, and global security policies in the next period (Mamediiava: 2025).

A group of researchers from Germany has highlighted a series of ethical considerations specifically formulated for military applications involving the use of artificial intelligence. These principles include (Anneken M. et al.: 2025, 28):

- *traceability*, which involves ensuring the transparency and comprehensibility of the decision-making processes of AI-based systems;
- *proportionality*, which refers to maintaining an appropriate balance between military objectives and the imperative of complying with humanitarian norms;
- *governability*, which emphasizes the importance of maintaining human control

over decisions generated by autonomous systems;

- *responsibility*, according to which responsibility for actions carried out with the help of AI must always lie with the human operator;
- *reliability*, which aims to develop robust, safe, and predictable AI systems in a military context.

These are some of the ethical principles that will form the basis of studies, scenarios, war games, subsequent exercises, and ultimately military combat systems.

As artificial intelligence-based technologies become increasingly integrated into defense systems, the traditional boundaries between the civilian and military domains are blurring. The result is the formation of a new security ecosystem characterized by technological interdependence, strategic flexibility, and an increasingly evident convergence between civilian innovations and their military applications.

Although there have been debates and contradictions regarding the number of military revolutions that have taken place over time, we agree with the statement that *"technology alone is not sufficient to justify the existence of a military business revolution"* (Vlad, Dumitrescu: 2005, p. 60). The authors highlight that the importance of operational

concepts is at least equivalent to that of technological innovation.

A relevant aspect is that, following consultation of the academic databases Google Scholar (2025) and ResearchGate (2025), only one paper was identified that includes the phrase *"the sixth revolution in military affairs"* in its title, namely *The Sixth RMA Wave: Disruption in Military Affairs?* (Raska: 2022), which suggests the novelty and still little explored nature of this concept in the literature.

In an integrated approach, it can be argued that the transformations induced by artificial intelligence contribute to shaping a new wave within the Military Affairs Revolution. The dynamics of these technological developments, correlated with decisions taken at the political-military level, whether anticipatory or reactive, can influence both the operational concepts and the structural characteristics of future armed conflicts.

4. CONCLUSIONS

The transformation of the military is not a singular event, but a continuous, complex, and adaptive process. It should be understood as a permanent evolution, driven by technological advances, doctrinal changes, and organizational restructuring, designed to ensure the efficiency and relevance of the armed forces in a security environment undergoing constant transformation. This perspective, commonly found

in the literature and in institutional discourse on military modernization, emphasizes the progressive and long-term nature of changes in defense.

The accelerated evolution of artificial intelligence technology requires sustained international collaboration to build a regulatory framework capable of balancing innovation with the protection of fundamental human rights. As AI takes on an increasingly important role in the military, governments, international organizations, and defense structures are forced to adapt to a constantly changing reality marked by advanced technologies that can fundamentally transform the nature of conflicts.

AI capabilities in the military context have expanded considerably, from real-time data collection and analysis to the operation of autonomous weapons systems. These advances offer a considerable operational advantage, enabling rapid processing of large volumes of information and a more effective response to threats. However, the integration of these technologies raises serious ethical and legal issues, particularly with regard to responsibility for lethal decisions and compliance with international humanitarian norms.

In this context, the Revolution in Military Affairs is not simply a matter of modernizing equipment, but reflects a profound cultural and conceptual transformation of the military domain. This change aims

to achieve a significant strategic advantage in an increasingly complex security environment marked by digitalization, interconnectivity, and volatility.

Although technological innovation is an essential factor in the transformation of the military domain, it is not, in itself, sufficient to generate revolutionary change. *A Revolution in Military Affairs* only occurs when technology is coherently and effectively integrated into doctrine, organizational structures, and operational concepts. If we accept that military change can be profound even in the absence of an accelerated rhythm, interpreting it as an evolutionary process becomes fully justified.

Based on the results obtained through the analysis of the specialized literature, it can be concluded that the identification of a new Revolution in Military Affairs remains an open topic, especially with regard to the critical arguments concerning the integration of artificial intelligence into combat systems.

As stated in the introduction, I would like to reiterate that this article is forward-looking, aiming to analyze the prospect of artificial intelligence becoming the sixth Revolution in Military Affairs in the future.

In my opinion, the impact of artificial intelligence is expected to trigger at least a new wave of RMA, if not a new RMA altogether, with the only unknown being when this transformation will happen.

REFERENCES

- [1] Bartosiak J., *The Revolution in military affairs*, Geopolitical futures, 2019. Accessed on July 2, 2025. <https://geopoliticalfutures.com//pdfs/the-revolution-in-military-affairs-geopoliticalfutures-com.pdf>
- [2] Cordesman A.H., *The Real Revolution in Military Affairs*, Center for Strategic and International Studies, 2014. Accessed on July 2, 2025. <https://www.csis.org/analysis/real-revolution-military-affairs>
- [3] Doicariu D., & Acsinte A.-I. (2025). *NATO-EU cooperation in response to the challenges of emerging and disruptive defense technologies*. *Journal of Defense Resources Management*, 16(1), 255-268. <https://doi.org/10.64404/JoDRM.2025.1.12>.
- [4] European Union, 2022, *Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe*, Document 52022DC0652. Accessed on July 17, 2025. <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52022DC0652>
- [5] European Union, 2024, *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence*. Accessed on July 17, 2025. <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R1689>
- [6] Fitzsimonds J. R., Van Tol J. M., *Revolutions in Military Affairs*, The Joint Force Quarterly, 1994.
- [7] Forțele Aeriene Române, 2020. Accessed on July 7, 2025. https://www.roaf.ro/?page_id=26602
- [8] Google Scholar, 2025. Accessed on August 4, 2025. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=the+sixth+revolution+in+military+affairs&btnG=
- [9] Hundley R. O., *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us About Transforming the U.S. Military?*, RAND's National Defense Research Institute, Santa Monica, 1999.
- [10] Krepinevich Jr. A. F., *The Military-Technical Revolution A Preliminary Assessment*, CSBA-Center for Strategic and Budgetary Assessments, Washington DC, 2002.
- [11] Kak K., 2000, *Revolution in Military Affairs-An Appraisal*. Accessed on July 9, 2025. https://ciaotest.cc.columbia.edu/olj/sa/sa_apr00kak01.html
- [12] Knox M., Murray W., *The dynamics of military revolution, 1300-2050*, Cambridge University Press, 2001.
- [13] McKittrick J., Blackwell J., Littlepage F., Kraus G., Blachfield R., Hill D., *The Revolution in Military Affairs*, din lucrarea *Battlefield of the Future – 21st Century Warfare Issues*, editori Barry R. Schneider, Lawrence E. Grinter, Air War Collage Studies in National Security, no. 3, 1998.
- [14] Mocanu C., *The Role of Artificial Intelligence in Modern Warfare*, Proceedings 20th International Scientific Conference *STRATEGIES XXI - "Strategic Changes in Security and International Relations"* vol. XX, "CAROL I" National Defence University, 2024.
- [15] Official Gazette of Romania, Part I, No. 551 bis, DECISION No. 429 of June 20, 2019, approving the 5G

- Strategy for Romania*, 2019.
- [16] Official Gazette, Part I No. 730 of July 25, 2024, Decision No. 832/2024 approving the *National Strategy on Artificial Intelligence 2024-2027*, 2024.
- [17] Official Gazette, Part I No. 893 of September 4, 2024, Decision No. 1028/2024 approving the *National Strategy in the field of quantum technologies for the period 2024-2029*, 2024.
- [18] Official Gazette, Part I No. 979 of September 30, 2024, Decision No. 1166/2024 approving the *National Strategy for the Development and Support of Digitization through Digital Innovation Centers in Romania 2024-2027*, 2024.
- [19] Murray W., *Thinking about revolutions in military affairs*, OASD(PA)/DPC, 1997. Accessed on July 2, 2025. <https://apps.dtic.mil/sti/pdfs/ADA354177.pdf>
- [20] Morris J. F., *On the Precipice of a New Era of Warfare? Reflections on Military Revolutions, Past and Future*. Accessed on July 4, 2025. <https://mwi.westpoint.edu/on-the-precipice-of-a-new-era-of-warfare-reflections-on-military-revolutions-past-and-future/>
- [21] NATO, 2023, *Emerging and disruptive technologies*. Accessed on July 15, 2025. https://www.nato.int/cps/en/natohq/topics_184303.htm?selectedLocale=en
- [22] NATO, 2024, *Summary of NATO's Quantum Technologies Strategy*. Accessed on July 15, 2025. https://www.nato.int/cps/en/natohq/official_texts_221777.htm
- [23] NATO, 2024, *Summary of NATO's revised Artificial Intelligence (AI) strategy*. Accessed on July 15, 2025. https://www.nato.int/cps/en/natohq/official_texts_227237.htm
- [24] NATO, 2025, *NATO Science & Technology Strategy*. Accessed on July 15, 2025. https://www.nato.int/nato_static_fl2014/assets/pdf/2025/6/pdf/250605-sto-strategy.pdf
- [25] O'Hanlon M., *A retrospective on the so-called revolution in military affairs, 2000-2020*, Foreign Policy at Brookings, Washington, D.C., 2018.
- [26] Raska M., 2022, *The sixth RMA wave: Disruption in Military Affairs?* Accessed on August 5, 2025. https://www.google.ro/books/edition/Defence_Innovation_and_the_4th_Industrial_Revolution/e-RXEAAAQBAJ?hl=ro&gbpv=1
- [27] ResearchGate, 2025. Accessed on August 4, 2025. <https://www.researchgate.net/search/publication?q=the%2Bsixth%2Brevolution%2Bin%2Bmilitary%2Baffairs&page=2>
- [28] NATO Summit, 2016. Accessed on July 23, 2025. <https://nato.mae.ro/node/435>
- [29] NATO Summit, 2019. Accessed on July 23, 2025. <https://www.mae.ro/node/51012>
- [30] Tilford E. H., *The Revolution in military affairs: prospects and cautions*, Strategic Studies Institute, US Army War College, 1995. Accessed on July 5, 2025. <https://www.jstor.org/stable/pdf/resrep11803.pdf>
- [31] Vlad L. B., Dumitrescu A. T., *Tranziția de la armata modernă la armata postmodernă. Implicațiile tehnologiei militare*, Economic Journal No. 15, 2005.

FIVE BASIC MILITARY STRATEGIES AND THEIR MODERN IMPLEMENTATION

Rashad TAHIROV*, **Sadi SADIYEV****, **Hikmet HASANOV*****

*Colonel, deputy of rector Military Scientific Research Institute,
PHD in Military science and National security

**Dr. PhD. senior advisor of International Military Cooperation
Department,

***Major- general, deputy of rector National Defence University of
Azerbaijan

This article explores the continued relevance and transformation of five foundational military strategies – extermination, annihilation, exhaustion, intimidation, and subversion – within the context of twenty-first-century conflict. While rooted in classical theories of warfare, these strategies have evolved dramatically due to technological advancement, cyber capabilities, and shifting geopolitical dynamics. Extermination, once associated with large-scale battlefield destruction, now manifests through precision drone strikes and cyberattacks aimed at critical infrastructure, as seen in Azerbaijan's integration of UAVs into battlefield during the 2020 Second Karabakh War. Annihilation strategies have embraced multi-domain integration, combining air superiority, precision artillery, special operations, and electronic warfare to dismantle enemy forces with speed and precision. Exhaustion, traditionally achieved through prolonged attritional warfare, has shifted toward non-kinetic tools such as economic sanctions, cyber sabotage, and disinformation campaigns designed to degrade a nation's resilience and public morale over time. The Russia-Ukraine conflict exemplifies this modern approach to exhaustion, incorporating conventional warfare alongside cyber and economic pressure. Intimidation has similarly evolved, now operating prominently in digital spaces through psychological operations and disinformation amplified by social media and cyberattacks. These tactics seek to undermine trust in institutions, sow confusion, and reduce an adversary's will to resist. Subversion, perhaps the most insidious of the five strategies, has become central to hybrid warfare. Through cyber espionage, election interference, and proxy warfare, states can destabilize adversaries from within while maintaining plausible deniability. Contemporary examples such as Russian election meddling and Iranian support for regional militias underscore how subversion challenges legal and normative frameworks of conflict.

Key words: strategy, extermination, annihilation, exhaustion, intimidation, subversion

1. INTRODUCTION

Over the centuries, military strategy – the art and science of deploying and using armed forces to accomplish political and strategic goals [1] has changed significantly in reaction to developments in technology, changes in geopolitics, and modifications in the nature of combat itself. The fundamental strategies of military doctrine – extermination, exhaustion, annihilation, intimidation, and subversion – remain essential to both conventional and unconventional conflict in spite of these developments. Despite having their roots in traditional military theory, these strategies have undergone substantial redefining and recontextualization in the context of 21st-century conflict, which increasingly involves various domains like as cyber, information, and space. These enduring strategic paradigms, while grounded in classical military thought, have been profoundly transformed by advances in technology and the evolving character of warfare. The proliferation of unmanned systems, cyber capabilities, precision-guided munitions, and real-time intelligence has expanded the operational environment beyond traditional physical battlefields to include digital, informational, and even cognitive domains. Consequently, modern military strategy necessitates an integrated, multidomain approach that synthesizes kinetic and non-

kinetic means to achieve strategic objectives.

Historically, military theorists such as Carl von Clausewitz and Sun Tzu recognized that strategy extends beyond mere battlefield tactics. Clausewitz's seminal work, *On War*, emphasizes war as a continuation of politics by other means, stressing the importance of strategic objectives over mere operational success [2]. Likewise, Sun Tzu's *The Art of War* outlines the psychological and subversive elements of strategy, such as deception and manipulation, which are echoed in today's information warfare and influence operations [3]. These classical frameworks provide a foundation for analyzing how ancient strategies endure, albeit in new and complex forms.

In the modern world, the implementation of these basic military strategies is profoundly shaped by the emergence of hybrid warfare, network-centric operations, and multi-domain integration. For instance, the strategy of annihilation, traditionally characterized by decisive and rapid defeat of enemy forces, now incorporates real-time data fusion, precision strikes, and cyber-enabled disruption [4]. Similarly, exhaustion strategies have shifted from attritional battlefield engagements to long-term economic sanctions, cyberattacks, and disinformation campaigns aimed at undermining national resilience and morale [5].

The rise of asymmetric and proxy warfare further underscores the relevance of subversion, where states and non-state actors exploit internal divisions within adversaries to destabilize societies from within. Meanwhile, strategies of intimidation are increasingly manifest in military posturing, nuclear signaling, and cyber demonstrations of force that aim to deter adversaries and reassure allies without engaging in direct conflict [6, s. 344].

This article explores each of the five fundamental military strategies – extermination, exhaustion, annihilation, intimidation, and subversion – and their application in modern warfare. It examines how traditional strategic concepts have been reinterpreted in light of technological innovation, strategic culture, and the evolving character of conflict. Drawing on contemporary examples, it highlights the adaptive nature of strategy in achieving political and military objectives across kinetic and non-kinetic domains.

Understanding these strategies in a modern context is essential for both military practitioners and policy analysts, as it offers critical insights into the conduct of contemporary warfare and the strategic behavior of states. As the global security landscape becomes increasingly dynamic and contested, the ability to recognize and respond to these foundational strategies – whether through deterrence, defense, or

diplomacy – remains a cornerstone of national and international security.

2. THE MAIN MILITARY STRATEGIES: OVERVIEW

Military strategy is not just a plan that outlines the utilization of military resources through specific employment concepts to accomplish military goals. Because this perception belies the inherent dynamism of strategic planning, which must constantly adapt to evolving operational environments, shifting political objectives, and the fluctuating availability of resources.

Unlike static planning models, military strategy is inherently contingent. Goals may change mid-conflict whether due to political shifts, public opinion, or changes in international alliances requiring a corresponding adjustment in military objectives and tactics. For instance, the strategic goals of the U.S. in Iraq evolved significantly between 2003 and 2011, transitioning from regime change to counterinsurgency, stabilization, and finally withdrawal, each phase demanding a different allocation and employment of military assets [7, s. 148-163].

Similarly, military resources, troops, technology, logistics, and intelligence are neither infinite nor fixed. Their availability can fluctuate based on economic capacity, industrial output, or attritional loss. In response, strategy must recalibrate. For example, during World War II,

Britain initially employed a strategy of direct confrontation but later pivoted toward strategic bombing and indirect engagements, such as supporting resistance movements, in response to resource constraints and the need to maintain public morale [8].

The information age has further complicated strategic planning, introducing cyber capabilities, unmanned systems, and real-time intelligence, all of which can both enhance and complicate the strategic picture. Contemporary hybrid conflicts such as the war in Ukraine demonstrate the need for strategies that integrate conventional and irregular forces, information warfare, and flexible operational objectives [9].

The fundamental ideas of strategy are still based on undermining the enemy's power or determination, even though the areas of war have moved from land, sea, and air to space and cyberspace. Throughout the ages, strategists have formulated different methods or "mini-theories" to elucidate how victories in wars can be achieved. Military strategy encompasses a broad spectrum of approaches aimed at achieving victory by undermining the adversary's ability to continue effective resistance. Over time, theorists and commanders have sought to categorize these approaches into conceptual frameworks that clarify the underlying objectives and mechanisms of warfare. Such

frameworks help distinguish between strategies that target physical destruction and those that seek to erode the enemy's psychological resilience or political cohesion. By breaking down complex campaigns into smaller, more focused theories, military thinkers can better analyze and apply specific methods tailored to particular contexts and goals. These mini-theories offer insight into the diverse ways in which conflict can be conducted beyond the battlefield, encompassing both direct and indirect means of compelling an opponent's surrender and highlight various strategic objectives, tactics, and psychological factors in combat. The most notable mini-theories, or classical approach of military strategies: extermination, exhaustion, annihilation, intimidation, and subversion represent distinct methods to weaken or destroy the enemy's capacity or will to fight.

Extermination centers on the total dismantling or removal of the adversary's troops [10]. It is the most harsh and straightforward tactic, aiming to physically destroy the enemy's military strength so they cannot fight any longer. This approach often entails direct and sustained combat operations designed to inflict maximum casualties, leaving little opportunity for the opponent to regroup or recover. Historically, extermination has been associated with campaigns marked by intense brutality and high human cost, reflecting a strategic

calculus that prioritizes absolute defeat over negotiated settlements or limited objectives. While effective in neutralizing military forces, the tactic carries profound ethical and political implications, as it frequently results in widespread destruction and civilian suffering. Moreover, reliance on extermination as a primary strategy can provoke international condemnation and may galvanize enemy resistance rather than diminishing it, thereby complicating long-term conflict resolution efforts.

Exhaustion focuses on destroying the adversary's resources and will over time, making prolonged conflict unsustainable [11]. This strategy aims to wear down the enemy gradually instead of fighting major confrontations. It depends on continuous pressure to deplete the adversary's resources, spirit, and determination to combat. Unlike extermination, which seeks immediate and absolute destruction, exhaustion requires patience, resilience, and the ability to sustain operations over an extended period. This approach often involves cutting supply lines, conducting harassment operations, and leveraging economic or diplomatic means to undermine the enemy's capacity to sustain warfare. While potentially less costly in terms of immediate casualties, exhaustion can impose significant strains on both the attacker and defender, as protracted engagements test logistical endurance and domestic support. Consequently, exhaustion strategies demand careful calibration

to avoid diminishing one's own fighting capability or political will. Ultimately, this method aims to compel surrender through attrition, capitalizing on the cumulative erosion of the opponent's strength rather than outright battlefield annihilation. The Roman general Fabius Maximus is often credited with pioneering a classical form of the strategy of exhaustion, particularly during the Second Punic War (218–201 BCE) against Hannibal Barca of Carthage. In response to Hannibal's unexpected and devastating victories – most notably at Cannae (216 BCE) – Fabius developed a defensive and attritional approach that came to be known as the Fabian strategy [12]. Rather than confronting Hannibal directly in large-scale battles, where Roman forces had suffered catastrophic losses, Fabius sought to undermine the Carthaginian campaign by avoiding decisive engagements, harassing supply lines, and exhausting enemy resources over time. This approach reflected the essential logic of the strategy of exhaustion: depriving the enemy of the opportunity for a swift and decisive victory while gradually weakening their operational capacity and political will. Fabius understood that Rome's strength lay in its capacity to endure and regenerate, while Hannibal, operating deep within hostile territory without consistent reinforcement or supply, was vulnerable to a long war of attrition.

Annihilation focuses on delivering rapid, decisive blows to incapacitate enemy forces, often through concentrated and overwhelming attacks [13]. It closely resembles extermination but emphasizes the decisive defeat of the enemy's main forces in a single or series of battles, rendering them incapable of further resistance. Annihilation strategies typically rely on superior maneuverability, intelligence, and coordination to exploit weaknesses in the enemy's formation or command structure. The objective is not merely to inflict casualties but to break the enemy's operational cohesion and morale, thereby accelerating the end of hostilities. Historically, such strategies have been employed by commanders seeking to avoid prolonged conflict by forcing a swift and conclusive outcome. However, the reliance on rapid victory also carries significant risks, as failure to achieve decisive results can lead to prolonged attrition or strategic overextension.

Intimidation involves psychological warfare and demonstrations of power designed to erode the enemy's will without necessarily engaging in full-scale conflict [10]. The approach utilizes psychological warfare tactics to break the enemy's will before or during the conflict, aiming to avoid prolonged fighting by creating fear or uncertainty. This strategy often employs displays of overwhelming

force, propaganda, and strategic misinformation to undermine the adversary's confidence and cohesion. In order to force surrender or concessions without having to pay the price of direct conflict, intimidation aims to create uncertainty and fear among both civilian populations and enemy ranks. Furthermore, the perceived resolve of the intimidating force and the veracity of threats determine how effective intimidation is, therefore perception management and communication are essential elements. By discouraging violence or encouraging voluntary withdrawal, intimidation can, when used effectively, result in a speedy resolution of conflicts; however, its effectiveness may be lessened if the enemy views such tactics as mere showmanship or if the enemy's morale is strong.

Subversion targets the enemy from within – through espionage, propaganda, sabotage, infiltration, or cyber disruption or support to dissident group, – to undermine their cohesion and legitimacy [10]. Each of these activities may be employed alone or in combination, depending on the nature of the conflict, the capabilities of the belligerents, and the strategic goals at stake.

By exploiting internal divisions, subversion seeks to weaken the adversary's political stability and erode public confidence in leadership, thereby reducing their capacity to effectively prosecute war. This method often operates

below the threshold of conventional warfare, blurring the lines between military and civilian domains and complicating the adversary's ability to respond decisively. Furthermore, subversion can have a prolonged and cumulative effect, gradually destabilizing institutions and creating conditions favorable to the subverting power's objectives. However, it also carries inherent risks, including the potential to provoke harsh reprisals or unintended escalation, and requires sophisticated intelligence capabilities and an acute understanding of the target society's vulnerabilities. Ultimately, subversion exemplifies a form of warfare that prioritizes psychological and political disruption over direct military confrontation, reflecting the increasingly multifaceted nature of modern conflict. The concept of subversion finds early articulation in the writings of Sun Tzu, the ancient Chinese military strategist whose treatise *The Art of War* remains foundational in strategic thought. Sun Tzu famously asserted that "*the supreme art of war is to subdue the enemy without fighting*," [14] a principle that aligns closely with the goals of subversion. Rather than relying on direct confrontation, Sun Tzu advocated for the use of deception, manipulation, and psychological influence to destabilize the adversary from within. Techniques such as sowing discord among enemy ranks, undermining alliances, and exploiting internal weaknesses reflect

a strategic preference for indirect methods – core tenets of subversive warfare. In this sense, subversion is not only consistent with Sun Tzu's philosophy but can be seen as a practical application of his broader emphasis on intelligence, deception, and strategic subtlety in achieving victory with minimal cost.

The five mini-theories of warfare – annihilation, extermination, exhaustion, intimidation, and subversion – represent distinct strategic approaches, each targeting different dimensions of the enemy's capacity or will to resist. Every strategy represents distinct objectives, moral considerations, and practical methods. From total devastation to psychological warfare, these tactics show many methods for accomplishing military goals. These strategies may function independently or in combination, offering military planners a flexible framework to adapt to the political, technological, and cultural contexts of a given conflict. Collectively, they illustrate the multifaceted nature of warfare and the complex considerations involved in achieving strategic success.

2.1. The modern implementation of classic strategic approaches

The basic principles of classic strategic approaches, mentioned above still shape contemporary warfare, although they have been adopted to fit modern technological contexts. These adaptations highlight

how classical strategies are not obsolete but are instead continually reinterpreted in light of new technologies, geopolitical dynamics, and hybrid modes of warfare. The enduring relevance of these strategic foundations underscores their adaptability and their continued importance in both conventional and unconventional military planning. The principles of annihilation, exhaustion, intimidation, subversion, and extermination continue to inform strategic planning, but they are now executed through increasingly sophisticated and multidimensional means. For instance, the principle of subversion, once reliant on covert human intelligence and propaganda, now finds expression in cyber warfare, disinformation campaigns, and digital espionage aimed at undermining political stability and public trust without deploying conventional forces. Similarly, the concept of exhaustion has expanded beyond battlefield attrition to encompass economic sanctions, long-term cyber disruption, and the strategic manipulation of energy supplies.

Furthermore, modern strategic environments often involve non-state actors, proxy wars, and asymmetric threats, requiring greater flexibility in the application of classical principles. These actors frequently leverage hybrid tactics – blending conventional, irregular, and information operations – to exploit vulnerabilities in technologically

advanced but strategically rigid adversaries. As such, contemporary military doctrine increasingly emphasizes adaptability, multi-domain integration, and resilience – attributes deeply rooted in the lessons of classical strategy but reformulated for modern complexity.

Ultimately, the continued relevance of classical strategic approaches lies in their conceptual clarity and operational versatility. Their application in modern contexts not only affirms their foundational value but also demonstrates the necessity of continually updating strategic thinking to reflect the evolving character of conflict. As technology, geopolitics, and social dynamics continue to reshape the battlefield, the reconsideration of these enduring principles remains essential to effective military strategy and national security policy.

Historically associated with total war and genocidal campaigns, modern extermination strategies have evolved with advanced technology, precision strikes, and AI-driven warfare. In contemporary warfare, extermination is less about wholesale slaughter largely due to international laws and norms and more about precision targeting. The modern extermination strategies rely on precision strikes enabled by drones, smart munitions, and satellite intelligence to eliminate critical enemy assets with minimal collateral damage. The focus shifts from total annihilation of personnel

to neutralizing command centers, missile sites, and logistical hubs. This approach reduces mass casualties but still seeks to cripple enemy capabilities decisively. Contemporary extermination methods depend on targeted strikes facilitated by drones, advanced munitions, and satellite reconnaissance to take out essential enemy infrastructure while minimizing collateral damage. The emphasis transitions from the complete destruction of personnel to incapacitating command centers, missile launch sites, and supply hubs. This strategy lessens large-scale casualties but continues to aim for a decisive blow to enemy capabilities. Modern extermination strategies can involve:

- *Decapitation Strikes* Targeted drone strikes against terrorist leaders, command centers, and critical infrastructure. The Second Karabakh War between Armenia and Azerbaijan in 2020 offers a contemporary example of the use of decapitation strikes a targeted strategy aimed at eliminating key enemy leadership, command infrastructure, or critical capabilities to disrupt coordination and morale. During the conflict, Azerbaijan employed Bayraktar TB2 drones, loitering munitions (such as Harop drones), and precision-guided artillery to systematically target Armenian command posts, radar systems, air defense units, and high-ranking officers [15, s. 52, 90]. These decapitation strikes were not limited to physical leadership elimination but

extended to disabling C2 (command and control) infrastructure, effectively paralyzing Armenian military responsiveness and degrading battlefield awareness. The rapid destruction of Armenian air defense systems and communication nodes in the early days of the war showcased Azerbaijan's effort to decapitate not just individuals but the operational coherence of the adversary. This strategic focus on leadership and critical systems was instrumental in Azerbaijan's swift territorial gains and highlighted how modern technologies particularly UAVs and ISR (intelligence, surveillance, reconnaissance) platforms have revitalized classical extermination strategies in the context of hybrid, high-tech warfare.

- *Cyber operations*

Cyber operations that destroy critical infrastructure represent a contemporary adaptation of classical military strategy of extermination, extending the battlefield into the digital realm to achieve strategic objectives with minimal kinetic force. It aims to incapacitate essential services such as power grids, communication networks, and transportation systems, thereby disrupting the adversary's ability to sustain military and civilian functions. The contemporary example of cyber operations reflecting an extermination strategy is the NotPetya cyberattack in 2017, widely attributed to Russian state-sponsored actors. Initially targeting Ukrainian institutions,

the malware rapidly spread to critical infrastructure, government ministries, energy companies, banks, and even international corporations operating within Ukraine. NotPetya functioned as a wiper, masquerading as ransomware but designed primarily to destroy data and disable systems beyond recovery. Its impact on Ukraine was severe: transportation networks, financial systems, and even parts of the power grid were disrupted, effectively paralyzing sectors critical to national resilience [16]. In spite of extensive manual labor and significant effort to locate a functioning backup, the estimated damage ranges from \$250 million to \$300 million [17]. This deliberate and systematic disabling of core operational infrastructure mirrors the logic of extermination, not in terms of physical troop destruction, but in terms of permanently degrading the adversary's capacity to operate and respond. The attack's scale and destructiveness demonstrated how cyber tools could serve strategic ends traditionally pursued through kinetic means, reinforcing the idea that modern extermination strategies may be digital rather than physical targeting the operational core of a state rather than its armed forces alone.

Annihilation seeks a decisive and rapid defeat of enemy forces, rendering them incapable of continued resistance. Contemporary warfare embraces this goal through network-centric operations combining air

superiority, precision artillery, special forces, electronic warfare, and cyber disruption. These elements synergize to create a multi-domain operational environment that overwhelms the adversary's ability to coordinate, communicate, and effectively respond, thereby accelerating the collapse of hostile military capabilities.

At the core of modern annihilation strategies is the principle of achieving information dominance. Network-centric warfare (NCW) enables real-time sharing of battlefield intelligence, facilitating rapid decision-making and precision engagement. This paradigm shift from platform-centric to network-centric operations allows friendly forces to synchronize actions across air, land, sea, space, and cyberspace domains, exploiting vulnerabilities with unmatched speed and accuracy. The integration of advanced sensors, unmanned systems, and artificial intelligence further enhances situational awareness, providing commanders with a comprehensive operational picture that drives swift and effective targeting.

Air superiority remains a foundational element in achieving annihilation. Control of the skies restricts enemy movement, protects friendly forces, and enables freedom of action for precision strikes. Air platforms equipped with stealth capabilities and long-range precision munitions can neutralize critical enemy nodes

such as command centers, logistics hubs, and air defenses before ground operations commence. The rapid destruction of these nodes disrupts the enemy's command and control (C2) architecture, creating cascading effects that degrade morale, coordination, and operational tempo.

Precision artillery complements air operations by delivering timely and accurate fire support to ground forces. Modern artillery systems, integrated with real-time targeting data, can engage enemy concentrations, fortifications, and logistical lines with minimal collateral damage. The use of guided munitions ensures that each round contributes maximally to the operational objective, shortening the engagement cycle and reducing the enemy's ability to regroup or counterattack.

Special forces play a critical role in exploiting the confusion sown by superior firepower and electronic disruption. Operating behind enemy lines, these elite units conduct reconnaissance, sabotage, and direct-action missions that further dismantle enemy cohesion. Their ability to seize or destroy key terrain, capture high-value targets, and gather human intelligence (HUMINT) creates operational dilemmas that compound the effects of conventional strikes, accelerating the overall campaign towards annihilation. A notable example of this was observed during the Second Karabakh War, where Azerbaijani special forces were instrumental in capitalizing

on battlefield disarray caused by overwhelming artillery and drone strikes [15, s. 58]. Utilizing their advanced training and mobility, these units penetrated Armenian defensive lines to seize key terrain, disrupt supply routes, and capture strategic positions such as high ground and critical infrastructure. Their operations were closely integrated with electronic warfare efforts that jammed enemy communications and drone control, amplifying the chaos and undermining Armenian command and control capabilities. This combination of precision strikes and special forces maneuvers accelerated the collapse of Armenian defenses, demonstrating the effectiveness of multi-domain operations in achieving rapid and decisive results.

Electronic warfare (EW) and cyber disruption act as force multipliers in the annihilation framework. By targeting enemy communications, radar, and weapon systems, EW operations degrade the adversary's ability to sense and respond to battlefield developments. Simultaneously, cyber operations can infiltrate and manipulate command networks, disable critical infrastructure, and spread disinformation. The convergence of electronic and cyber warfare creates a complex environment where enemy situational awareness and decision cycles are paralyzed, preventing effective resistance or countermeasures.

In summary, the pursuit of annihilation in contemporary conflict is realized through the seamless integration of technological advances and doctrinal innovation. The fusion of air dominance, precision firepower, special operations, and multi-domain electronic disruption forms a coherent strategy aimed at the rapid and comprehensive neutralization of enemy capabilities. As warfare continues to evolve, future developments in artificial intelligence, autonomous systems, and space-based assets are expected to further refine the principles of annihilation, emphasizing speed, precision, and the relentless degradation of adversary will and capacity to resist.

The strategy of exhaustion through prolonged conflict remains relevant but has expanded beyond physical battlefield engagements. Modern wars often incorporate economic sanctions, cyberattacks, and information blockades designed to sap an adversary's resources and morale over time without necessarily deploying large armies. These non-kinetic methods serve to systematically degrade an opponent's economic stability, social cohesion, and technological infrastructure, thereby imposing costs that can be as debilitating as conventional military defeat. Economic sanctions, for instance, target critical industries, financial networks, and trade relationships, aiming to constrain a nation's ability to sustain prolonged

military efforts or maintain civilian support for conflict. Such sanctions, when coordinated internationally, can isolate states diplomatically and economically, amplifying internal pressures that erode governmental legitimacy.

Cyber operations further complement this approach by disrupting essential services, communications, and industrial control systems. Unlike traditional attacks, cyberattacks can be conducted with plausible deniability and tailored precision, targeting specific vulnerabilities to cause cascading failures within critical infrastructure. These disruptions undermine public confidence and create uncertainty within decision-making circles, thus extending the battlefield into the virtual domain. Information blockades and propaganda campaigns, meanwhile, seek to influence both domestic and international audiences by controlling narratives, spreading disinformation, and undermining adversary morale. The strategic use of media and information warfare exploits societal divisions and challenges the cohesion necessary for sustained resistance.

Collectively, these tools reflect a broader understanding of conflict as a multidimensional contest where military, economic, informational, and cyber domains intersect. The extended application of exhaustion strategies in this holistic manner complicates traditional notions of victory and

defeat, as the damage inflicted often transcends physical destruction and manifests in the gradual erosion of an adversary's capacity and will to fight. Consequently, contemporary conflict management increasingly requires integrated approaches that address both kinetic and non-kinetic dimensions, highlighting the evolving character of warfare in the twenty-first century.

A pertinent modern example of the strategy of exhaustion through non-kinetic means is the ongoing conflict involving Russia and Ukraine, particularly since 2014 and intensifying after 2022. Russia's approach has combined prolonged military engagements in eastern Ukraine with extensive use of cyber warfare and information operations aimed at weakening Ukraine's resilience and international standing. Western nations, in turn, have imposed comprehensive economic sanctions on Russia targeting key sectors such as energy, finance, and technology [18]. Intimidation now extends far beyond displays of physical force. With the rise of social media and digital communication, psychological operations, disinformation, and cyberattacks are crucial to undermining enemy morale and sowing confusion. These non-kinetic tactics leverage the rapid dissemination and viral nature of information online to shape perceptions, manipulate public opinion, and destabilize societal trust. Psychological operations (PSYOP)

aim to exploit existing societal divisions, fears, and uncertainties, weakening the adversary's will to resist by fostering doubt and mistrust within their ranks and among the civilian population [19]. The strategic use of disinformation campaigns often amplified through bot networks and fake accounts can create echo chambers that reinforce false narratives, complicate fact-finding, and hinder effective decision-making at both government and grassroots levels.

Cyberattacks complement these efforts by directly targeting information systems, critical infrastructure, and communication channels. Disruption of networks through malware, ransomware, or denial-of-service attacks not only impairs operational capabilities but also projects an image of vulnerability, further eroding confidence in the state's ability to provide security and stability [20]. Moreover, the anonymity and ambiguity inherent in cyber operations complicate attribution, allowing actors to conduct intimidation campaigns without clear accountability, thus amplifying psychological pressure on both military and civilian targets [21].

The integration of these digital tools into intimidation strategies reflects a broader transformation in warfare where the boundaries between physical and cognitive domains blur. Modern conflict increasingly involves battles for hearts and minds fought not only

on traditional battlefields but also in cyberspace and the information environment. Understanding and countering these methods is essential for maintaining resilience and cohesion in the face of evolving hybrid threats.

In the contemporary strategic environment, subversion has become a core pillar of hybrid warfare, wherein state and non-state actors blend conventional military means with cyber, informational, and proxy methods to achieve political objectives without overt conflict. Subversion seeks to destabilize adversaries from within, eroding institutional trust, polarizing societies, and undermining state legitimacy all while maintaining a level of plausible deniability that complicates international response.

A prominent example of modern subversion is the alleged Russian interference in the 2016 U.S. presidential election, where cyber espionage, strategic leaks, and social media manipulation were employed to exacerbate political divisions and question democratic legitimacy [22]. By leveraging bots and troll farms such as the Internet Research Agency Russian operatives disseminated disinformation across platforms, targeting American voters with polarizing content designed to fuel mistrust and discord [23]. These tactics reflect a shift from direct confrontation to cognitive and sociopolitical disruption attacks

not on physical infrastructure, but on public opinion and democratic processes.

Subversion also manifests in proxy warfare, where external actors covertly support insurgent or separatist groups. For instance, Iran's support for militias in Iraq, Syria, and Yemen allows it to project power and destabilize adversaries without direct military engagement [24]. Similarly, in Eastern Ukraine, Russia's covert backing of separatist forces since 2014 has combined arms supplies, unmarked military personnel, and cyber operations to challenge Ukrainian sovereignty under a façade of internal rebellion [25].

This covert, multidomain approach to conflict complicates international norms and legal frameworks, making deterrence and retaliation challenging. As digital and information spaces become increasingly weaponized, subversion remains a potent tool for achieving strategic objectives below the threshold of open warfare.

Based on modern strategic studies and military theories, the application of the five core military strategies Extermination, Exhaustion, Annihilation, Intimidation, and Subversion can be systematically analyzed within the context of contemporary warfare by developing an integrated operational-strategic framework that encompasses their goals, means, ways and other factors.

Table 1 Military strategies

Factors	Extermination	Annihilation	Exhaustion	Intimidation	Subversion
Goals	Rapid and decisive neutralization of the enemy's center of gravity of an armed force.	Total and rapid destruction of enemy combat power	Degrade enemy resources, morale and political will over time Maximize time as a strategic asset	Avoid war while gaining strategic advantage Deter adversary action	Weaken or destabilize the opponent's political and military structure from within Disrupt the opponent's military effectiveness and decision-making
Object (Target)	Command centers Terrorist leaders Missile launch sites Logistical hubs Communication and control systems (C2 infrastructure) Critical infrastructure such as power grids, transportation, and communication networks	Command and Control (C2) systems Combat forces (troops, armored units, air defenses) Logistics and supply networks Communication and intelligence infrastructure Key terrain and operational nodes critical for enemy coordination	Economic stability (critical industries, financial networks, trade relationships) Social cohesion and public morale Technological and infrastructure systems (communications, industrial control, essential services) Governmental legitimacy and diplomatic standing	Enemy political leadership Military forces of the adversary Civilian population (indirect object) National infrastructure and strategic assets	Institutional trust and governance legitimacy Social cohesion and political unity Public opinion and democratic processes Internal security

Factors	Extermination	Annihilation	Exhaustion	Intimidation	Subversion
Force Typology (Means Employed)	<p>Precision Kinetic Strikes</p> <p>Cyber Operations</p> <p>Intelligence, Surveillance, and Reconnaissance (ISR) Platforms/</p>	<p>Air Power & Air Superiority</p> <p>Precision Artillery & Fire Support Systems</p> <p>Special Forces & Elite Ground Units</p> <p>Network-Centric Warfare</p> <p>Electronic Warfare</p> <p>Cyber Operations</p>	<p>Economic Instruments</p> <p>Cyber Operations</p> <p>Information Warfare & Propaganda</p> <p>Prolonged Kinetic Pressure</p> <p>Psychological Operations</p>	<p>Psychological Operations</p> <p>Disinformation & Propaganda Campaigns</p> <p>Cyberattacks on Information and Communication Infrastructure</p> <p>Information Environment Manipulation</p>	<p>Cyber Espionage & Information Leaks</p> <p>Social Media Manipulation & Disinformation Campaigns</p> <p>Proxy Warfare & Covert Support to Non-State Actors</p> <p>Hybrid Influence Operations</p>
Operational Mechanism (Ways)	<p>Targeted precise strikes</p> <p>Cyberattacks</p> <p>Disruption of civilian and military operational capabilities</p> <p>Satellite intelligence</p> <p>Real-time battlefield intelligence</p>	<p>Suppression of enemy air defenses</p> <p>Pre-emptive strikes on command centers and logistics nodes</p> <p>Reconnaissance and direct-action operations behind enemy lines</p> <p>Seizure of critical terrain and disruption of supply routes</p> <p>Disruption of radar, sensors, and targeting systems</p>	<p>Economic sanctions (targeting energy, finance, and technology sectors)</p> <p>Trade embargoes and financial restrictions</p> <p>Disruption of critical industries and markets</p> <p>Sustained low-intensity military engagements</p> <p>Attritional battles that draw out conflict duration</p> <p>Use of hybrid forces, including irregulars and paramilitaries</p> <p>Information blockades</p>	<p>Strategic signaling</p> <p>Show of force & posturing</p> <p>Strategic ambiguity</p> <p>Psychological and information operations</p> <p>Economic & hybrid pressure</p>	<p>Ideological and psychological infiltration</p> <p>Disinformation and propaganda warfare</p> <p>Infiltration of political and civil institutions</p> <p>Economic and infrastructure manipulation</p> <p>Support to internal opposition and proxy actors</p> <p>Legal and diplomatic sabotage</p> <p>Cyber subversion and digital espionage</p> <p>Slow escalation to instability</p>

Factors	Extermination	Annihilation	Exhaustion	Intimidation	Subversion
Temporal Scale	Rapid or medium-term shock effect	Short-duration, high-intensity operations	Long-term degradation over months or years	Episodic but strategically timed	Long-duration, clandestine or indirect
Visibility / Attribution	High (often overt and visible)	High (military visibility)	Medium-high	Medium (strategic signaling)	Low (covert, deniable)

3. CONCLUSION

The military strategy provides a framework for achieving military ends, its success lies in its flexibility. The most effective strategies are those that anticipate and respond to change whether in goals, resources, or the broader strategic environment. As history has shown, rigid adherence to initial plans often results in failure, while adaptive strategies that integrate shifting conditions offer the greatest chance of long-term success.

The five military strategies explored *extermination*, *exhaustion*, *annihilation*, *intimidation*, and *subversion* represent some of the most decisive and aggressive approaches in the history of conflict. Though often associated with historical total war and ideological struggles of the 20th century, these strategies remain highly relevant in the 21st century, albeit adapted to the evolving legal, ethical, and technological frameworks of modern warfare. Their continued implementation underscores the enduring reality that while the tools of war may change, the objectives of

dominance, deterrence, and control remain central to military strategy.

Modern extermination strategies are no longer defined by large-scale physical annihilation, but by surgical precision enabled by drones, smart munitions, and satellite intelligence. These tools allow for the targeted elimination of critical enemy assets such as command centers, air defense systems, missile platforms, and communication hubs while minimizing civilian casualties and physical destruction. The focus has shifted from mass killings to decisive incapacitation of an adversary's operational infrastructure. Strategic modernization of extermination focused not on eradicating life, but on systematically disabling the adversary's ability to respond, maneuver, or recover. In the *digital domain*, extermination has taken on a new form through *cyber operations*. These attacks target critical national infrastructure, aiming to inflict systemic failure with minimal or no kinetic action.

Modern annihilation strategy hinges on the integration of air

superiority, precision firepower, special forces, and multi-domain electronic and cyber warfare to rapidly incapacitate enemy forces. Network-centric operations enable real-time intelligence sharing and synchronized attacks across all domains, overwhelming adversaries' command, control, and communication systems. The success of this approach, exemplified in conflicts like the Second Karabakh War, demonstrates how combining technological innovation with tactical coordination accelerates the collapse of enemy resistance. As emerging technologies like AI and autonomous systems advance, annihilation strategies will continue evolving to prioritize speed, precision, and decisive operational dominance.

The strategy of exhaustion in modern conflict extends beyond the battlefield, integrating economic sanctions, cyberattacks, and information warfare to systematically weaken an adversary's resources and resolve. These non-kinetic tools disrupt critical infrastructure, undermine social cohesion, and erode political legitimacy, complicating traditional concepts of victory. The Russia-Ukraine conflict exemplifies this multidimensional exhaustion approach, with prolonged combat combined with cyber operations and coordinated international sanctions. As warfare evolves, exhaustion strategies increasingly emphasize

sustained pressure across military, economic, and informational domains, highlighting the need for comprehensive responses to both kinetic and non-kinetic threats.

Subversion in modern warfare has emerged as a strategic tool for achieving political objectives through covert, multidomain means. By exploiting cyber capabilities, disinformation, and proxy actors, states can destabilize adversaries without engaging in direct conflict. The examples of Russian election interference and Iran's proxy operations underscore how subversion erodes institutional trust and undermines national cohesion. Its plausibly deniable nature and impact on democratic systems make it a uniquely challenging threat. As digital and informational domains continue to expand, subversion will remain a central element of hybrid warfare, requiring adaptive and comprehensive responses from targeted states and the international community.

Contemporary warfare reshapes the classical mini-theories of military strategy by introducing new technologies, ethical considerations, and complex operational domains. While extermination and annihilation now emphasize precision and speed, exhaustion and subversion have expanded into economic and cyber realms. Intimidation thrives in the digital space through information

warfare, making psychological operations more pervasive than ever. Military leaders must thus modify these enduring strategic models to fit the dynamics of contemporary warfare—developing versatile, multi-domain strategies that utilize technology while managing political, legal, and social limitations. Grasping this evolution is essential for understanding how wars will be conducted and concluded in the 21st century.

REFERENCES

- [1] Jakobsen, Peter. V. Introduction: Military Strategy: What is the Use of It? [Electronic resource] / *Scandinavian Journal of Military Studies*, 5(1), p. 143–148. – September 9, 2022. URL: <https://sjms.nu/articles/10.31374/sjms.141>;
- [2] Miyata, F. The grand strategy of Carl Von Clausewitz: [Electronic resource] / *War Room* – March 26, 2021. URL: <https://warroom.armywarcollege.edu/articles/grand-strategy-clausewitz/>;
- [3] Карпов И. А. Психологическая война и дезинформация: классические подходы и современные практики // Научно-аналитический журнал «Геополитика и безопасность». — 2020. — Т. 12, № 2. — С. 21–30;
- [4] Lambert M. Precision Warfare and the Evolution of the Annihilation Strategy in the Digital Era, *Defence & Security Analysis*. — 2020. — Vol. 36, No. 4. — P. 372–386;
- [5] Mazarr M. J. The Psychological and Strategic Elements of Modern Conflict. *Parameters*, 2015, Vol. 45, No. 3, pp. 23–35;
- [6] Freedman L. Strategy: A History, L. Freedman. — Oxford: Oxford University Press, 2017. — 768 p;
- [7] Ricks T. E. Fiasco: The American Military Adventure in Iraq, T. E. Ricks. — New York: Penguin Press, 2006. — 482 p;
- [8] Griffin S. Iraq, Afghanistan and the future of British military doctrine: from counterinsurgency to stabilization, S. Griffin. — *International Affairs*, Vol. 87, Issue 2, March 2011. — Pp. 317–333;
- [9] Schnauffer, T. Redefining Hybrid Warfare: Russia's Non-linear War against the West: [Electronic resource], *Journal of Strategic Security* 10(1):17-31. – January 2016. URL: https://www.researchgate.net/publication/316637417_Redefining_Hybrid_Warfare_Russia's_Non-linear_War_against_the_West;
- [10] Randall, G. B. Military Strategy: Theory and Concepts: [Electronic resource], *A Dissertation*, Lincoln, Nebraska. – June 2013. URL: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?params=/context/poliscitheses/article/1026/&path_info=Military_Strategy_Dissertation_Final.pdf;
- [11] Nathan, K. F. On Strategy: A Primer: [Electronic resource] / *Combat Studies Institute Press Fort Leavenworth, Kansas*. – 2020. URL: <https://www.armyupress.army.mil/>

- Portals/7/combat-studies-institute/csi-books/on-strategy-a-primer.pdf;
- [12] Holmes, J. Fabian Strategies, Then and Now: [Electronic resource], *War On The Rocks* – September 17, 2015. URL: <https://warontherocks.com/2015/09/fabian-strategies-then-and-now/>;
- [13] Dubik, J. M. Strategy of Annihilation Not Yet Apparent: [Electronic resource], *The association of the United States army* – October 18, 2017. URL: <https://www.ansa.org/articles/strategy-annihilation-not-yet-apparent>;
- [14] Cunningham, J. China's Sun Tzu Strategy: The Supreme Art of Cyber: [Electronic resource], *Medium, Human stories & ideas* – September 7, 2016. URL: <https://cunningham-jeff.medium.com/the-art-of-cyber-war-35dc30a6f4c0>;
- [15] Piriye, H.K. İkinci Qarabağ müharibəsi. Hərbi-siyasi təhlil. / H.K.Piriye, R.K.Tahirov, X.İ.İsgəndərov – Bakı: Hərbi Nəşriyyat, – 2022. – 168 s;
- [16] McQuade, M. The Untold Story of NotPetya, the Most Devastating Cyberattack in History: [Electronic resource], *Wired* – August 22, 2018. URL: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>;
- [17] König S., Rass S., Schauer S. Cyber-attack impact estimation for a port, Digital Transformation in Maritime and City Logistics: Smart Solutions for Logistics. *Proceedings of the Hamburg International Conference of Logistics (HICL)*, Vol. 28. – Berlin: epubli GmbH, 2019. – C. 164-183;
- [18] Sadik, G. The effects of the Russia-Ukraine war on countering terrorism: [Electronic resource], *Centre of Excellence Defence Against Terrorism (COE-DAT)*, Ankara – TÜRKİYE. – 2025. URL: https://www.tmmm.tsk.tr/publication/researches/20-UKR_RUSwarEffectsCT.pdf;
- [19] Sidorova, Elena. "Book Review: Baines, Paul, O'Shaughnessy, Nicholas, and Nancy Snow, eds. *The SAGE Handbook of Propaganda*. London: SAGE, 2020." (2021);
- [20] Rid T., Buchanan B. Attributing cyber attacks, *Journal of strategic studies* – 2015. – T. 38. – №. 1-2. – C. 4-37;
- [21] Maness R. C., What Do We Know About Cyber War? Brandon Valeriano, *Bren Chair of Military Innovation: дис.* – American University;
- [22] Mueller R. S. et al. The Mueller Report: Complete Report on The Investigation Into Russian Interference in the 2016 Presidential Election. – *e-artnow*, 2019;
- [23] Rid T. Active measures: The secret history of disinformation and political warfare. – Profile Books, 2020;
- [24] Berti B., Guzansky Y. Saudi Arabia's Foreign Policy on Iran and the Proxy War in Syria: Toward a New Chapter?, *Israel Journal of Foreign Affairs* – 2014. – T. 8. – №. 3. – C. 25-34;
- [25] Galeotti M. Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?, *Small wars & insurgencies* – 2016 – T. 27. – №. 2. – C. 282-301.

CHARACTERIZING THE MILITARY CAREER OF ARTILLERY OFFICERS AND SERGEANTS IN THE PORTUGUESE ARMY: DETERMINANTS, CHALLENGES AND OPPORTUNITIES

Maria DÂMASO*, David Pascoal ROSADO, PhD*/**

*Academia Militar, Lisbon, Portugal

**Universidade Europeia, Lisbon, Portugal

This study explores the main contingencies, challenges, and opportunities associated with the military careers of Artillery Officers and Sergeants in the Portuguese Army. Using a mixed-methods approach, it triangulates qualitative and quantitative data to enhance analytical depth. The findings reveal significant associations between years of service, unit of origin, and perceptions of organizational culture, motivation, and career retention. Participants emphasized the importance of close leadership, international missions, ongoing training, and institutional recognition as key motivators. Conversely, a lack of personnel, excessive workloads, and outdated infrastructure emerged as substantial barriers to motivation and retention. The study highlights the critical role of organizational reforms, continuous investment in training and well-being, and fostering a culture of trust and recognition to enhance career sustainability and operational excellence in the Artillery branch.

Key words: Artillery, Military Career, Motivation, Organizational Culture, Retention.

1. INTRODUCTION

Military careers within the Artillery branch of the Portuguese Army are shaped by a complex interplay of sociocultural and organizational factors. These dimensions influence motivation, performance, job satisfaction, and retention. As Rijo et al. (2018) emphasize, unexpected personnel departures not only represent a loss

of specialized human capital but also disrupt the accumulation of critical knowledge and operational experience. Conversely, positive leadership practices, international deployments, ongoing training opportunities, and institutional recognition serve as key facilitators of professional development and operational effectiveness. Research plays a vital role in understanding

such social phenomena, offering a systematic and objective method that encourages critical reflection, practical debate, and innovation (Coutinho, 2015).

To explore these dynamics, the present study adopts a mixed-methods approach, as recommended by Yin (2005) and Flick (2004), which allows for a more comprehensive understanding of multifactorial phenomena. Combining qualitative interviews and quantitative survey data, the study investigates how specific sociocultural and organizational determinants shape the professional trajectories of Artillery Officers and Sergeants, with particular emphasis on motivation, well-being, and career sustainability in operational contexts.

The findings aim to inform military leadership and defense policymakers by offering evidence-based insights to enhance personnel retention, improve career development strategies, and optimize human resource management within the Armed Forces.

A well-formulated research question guides the entire investigative process by clarifying the researcher's focus (Campenhoudt, Marquet, & Quivy, 2019). In line with Fortin (1999), the general objective of this study is to explore, identify, and assess the main contingencies, challenges, and opportunities that affect the career paths of Artillery

Officers and Sergeants. The central research question is: “What are the main contingencies, challenges, and opportunities related to the military careers of Artillery Officers and Sergeants?”.

To address this question, the study is structured around three specific objectives (SO) and corresponding derived questions (DQ), which provide a logical and integrated framework for data collection and analysis:

- SO1 / DQ1: Identify the sociocultural and organizational determinants associated with military careers in the Artillery branch;
- SO2 / DQ2: Analyze how these determinants influence career trajectories and professional development;
- SO3 / DQ3: Propose strategic recommendations to mitigate the negative effects of these determinants and enhance retention and commitment.

2. LITERATURE REVIEW

2.1. Sociocultural Determinants

Sociocultural factors shape how military institutions anticipate and adapt to shifting social expectations (Redko et al., 2020). Organizational culture, though widely debated, remains difficult to define because it simultaneously guides behavior and resists change (Whelan, 2016).

In the Portuguese Army, these cultural foundations are deeply rooted in historical and institutional evolution, reflected in shared values that express what is considered important and how strongly such convictions are held (Rosado et al., 2017; Robbins, 2005).

Military culture remains distinct from civilian culture, prioritizing hierarchy, self-sacrifice, and operational readiness over individual freedom and flexibility (Grilo, 2004). Despite increased integration of women and minorities, military environments still exhibit masculine and heteronormative traits, often lacking structured inclusion strategies (Alves, 1999; Azevedo & Pereira, 2025). Although progress has been made - particularly in gender representation and shared parenting policies (Gonçalves, 2013) - confusion between gender integration and gender equality persists, hindering policy implementation (Morais, 2016).

2.2. Organizational Determinants

Organizational determinants refer to internal structures and practices that shape military performance. Organizational culture operates at multiple levels and influences how knowledge is shared and applied, affecting adaptability and institutional effectiveness (Adams, 1993; Belkhouja et al., 2007). In modern warfare, the rapid

pace of technological innovation - highlighted by recent conflicts such as in Ukraine - requires military structures to evolve and anticipate change, particularly in areas like electromagnetic operations and the integration of disruptive technologies (Costa, 2024).

Between 2006 and 2013, Europe saw a sharp decline in defense investment (fundings fell by over 27%), raising concerns about a growing capability gap and the risk of deindustrialization in the sector (Correia, 2017). In this context, military education institutions are critical hubs for cultivating strategic thinking and preparing personnel to operate in technologically complex environments (Vicente, 2007).

2.3. Quality of Work Life

The quality of work life significantly influences well-being and organizational performance (De Greef & Van den Broek, 2004). Walton (1973) highlights core dimensions such as remuneration, safety, work-life balance, and meaning at work. As noted by De Greef and Van den Broek (2004), aligning human resources with innovation and health promotion improves workplace effectiveness. Job satisfaction, defined as one's general attitude toward work (Robbins, 2005), is shaped by these factors. Although military and civilian contexts differ, both face similar human resource

challenges, including recruitment, retention, and training (Romão et al., 2020).

Dissatisfaction with remuneration remains a central issue, with pay levels often lagging civilian equivalents, compromising the attractiveness of military careers and fueling personnel shortages (Ferrão, 2024; Mandeiro, 2024). Although recent legislation has introduced financial incentives and updates to allowances (Repartição de Abonos, 2025), the wage gap continues to erode institutional loyalty.

Safety and occupational health are growing concerns in military settings due to their impact on well-being (Pereira & Eusébio, 2021). Burnout - marked by exhaustion, detachment, and reduced efficacy (Ahola et al., 2005; Enzmann et al., 1998; Honkonen et al., 2006) - is often linked to poor leadership and work-life imbalance (Brooks & Greenberg, 2018).

Skill development is vital for operational adaptability. While training enhances both technical and theoretical competencies (Billett, 2011), shortcomings in program design still limit effective knowledge transfer (Loureiro, 2023). The rise of advanced technologies and Artificial Intelligence intensifies the need for continuous upskilling within the Armed Forces (Frey & Osborne, 2013; Ferrão, 2024).

Staff shortages remain a critical constraint, limiting the ambition levels that units can realistically pursue, as highlighted by Ferrão (2024). This limitation compounds the difficulty in ensuring professional growth and career stability, often jeopardized by outdated promotion systems and stagnant career paths. Many military professionals seek early retirement or transition to the civilian sector in search of better pay and recognition (Rosado et al., 2017).

Furthermore, the balance between professional and personal roles is often compromised when the demands of one interfere with the performance of the other (Greenhaus & Beutell, 1985). In military settings, excessive demands divert time and energy from personal life, heightening emotional fatigue and health risks (Croon et al., 2005; Pereira & Eusébio, 2021). Ferrão (2024) also notes the decline of institutional support in areas like housing and welfare, which further undermines work-life integration.

Finally, organizational commitment continues to serve as a buffer against dissatisfaction. Military personnel often remain loyal due to a deep sense of purpose and institutional identity (Robbins, 2005). Nevertheless, when organizational support and recognition falter, this commitment weakens, leading to attrition. The Portuguese military's

international reputation and the sense of contributing to national defense help sustain motivation, but long-term engagement requires more than symbolic value - it depends on tangible improvements in quality of life and career conditions (Rosado et al., 2017; Ferrão, 2024).

3. METHODOLOGY

3.1. Study Design and Methodological Approach

This research follows a non-experimental, mixed-methods design, integrating qualitative and quantitative strategies - specifically interviews, questionnaires, and observation. This triangulated approach enhances data complementarity and strengthens the validity of findings (Flick, 2004; Paranhos et al., 2016; Yin, 2005). The epistemological approach supports the application of empirical tools from the natural sciences to the social sciences (Santos & Lima, 2019), and the inductive reasoning adopted allows for theoretical generalizations based on data analysis (Rosado, 2017).

3.2. Data Collection Techniques and Analysis

A structured questionnaire was used to collect quantitative data on perceptions of career determinants, challenges, and opportunities. The responses were analyzed using IBM

SPSS Statistics, applying descriptive statistics and inferential techniques to explore associations between variables such as rank, years of service, and unit (Campenhoudt, Marquet & Quivy, 2019).

To deepen the analysis, semi-structured interviews were conducted with five-unit commanders, allowing open-ended responses about organizational culture, personnel management, and policy challenges. Interview material was transcribed and coded using NVivo software.

3.3. Sample

The sample comprised officers and sergeants from four representative Artillery units: Anti-Aircraft Artillery Regiment No. 1 (RAAA1); Artillery Regiment No. 4 (RA4); Artillery Regiment No. 5 (RA5); and units stationed at the Military Field of Santa Margarida (CMSM). The units were selected for their relevance and diversity. Participation was voluntary and based on prior informed consent.

4. RESULTS AND DISCUSSION

4.1. Interviews

Organizational Culture

While a shared base culture rooted in hierarchy and esprit de corps is recognized, the unique identity of the Artillery has weakened, primarily due to resource constraints, personnel turnover, and the diversion of focus to non-operational tasks. Commanders

emphasized the need for continuity, updated equipment, and leadership proximity to revitalize institutional identity.

Gender and Inclusion

All interviewees denied any discriminatory practices, affirming that gender and minority integration are normalized. However, proactive strategies are scarce. Only one unit reported awareness-raising activities, indicating that inclusion is often assumed rather than structured through policies.

Career Challenges and Opportunities

Retention difficulties, competitive civilian job markets, and technological demands were recurrent concerns. Nevertheless, commanders highlighted training, leadership development, international missions, and modernization as key opportunities. Clearer career paths and specialized training were considered essential.

Motivation and Retention

Motivation was viewed as dependent not only on salary but also on fair workload distribution, career development, recognition, and well-being. Structural reforms, such as improved housing and flexible schedules, were seen as more effective than operational incentives alone.

Work-Life Balance

All units acknowledged the impact of service frequency and

limited staffing. Commanders reported initiatives such as scheduled rest, cultural activities, flexible time arrangements, and the promotion of open dialogue. These practices aim to reduce stress and enhance emotional stability.

Well-being

Physical training, periodic medical evaluations, and psychological support were common. Nutrition improvements and sports activities were also mentioned. Despite existing initiatives, most commanders recognized the need to strengthen support mechanisms for mental health and stress prevention.

Organizational Policies

There was consensus on the need for strategic reform: modernizing infrastructure, updating employment doctrines, and integrating emerging technologies. Structural issues such as unclear progression systems and insufficient social support were seen as barriers to development and retention.

4.2. Questionnaire Results

A total of 97 Artillery personnel responded to the survey. The majority were sergeants (71.1%), followed by captains/junior officers (17.5%) and senior officers (12.4%). Most respondents had between 1 and 10 years of service (53.6%). The main units represented were RAAA1 (37.1%) and RA4 (27.8%).

Table 1 Key Dimensions by Unit

Organizational Culture	It was most positively rated in RA4 (88,4%), especially among those with 21-30 years of service. In contrast, CMSM and RA5 revealed more polarized perceptions, including negative and very negative assessments.
Inclusion Strategies and Well-being	Were acknowledged by the majority in CMSM (64.7%) and RA5 (70.6%), but significantly less so in RA4 (40%), where criticism of work-life balance was also more prevalent.
Technology Adaptation	Received favorable ratings from senior officers across units. However, critical views were more common among younger personnel and sergeants, particularly in RAAA1, where 50% rated the response as poor or very poor.
Career Challenges and Opportunities	Such as stagnated promotion, workload pressure, and outdated equipment were more frequently identified in RA5. Participation in international missions was the most valued opportunity across all units.
Retention Policies	Were broadly considered ineffective. RA5 recorded the most positive ratings (47% effective or moderately effective), while RA4 had the lowest (only 7.7% considered them effective).
Feedback Mechanisms	Were more appreciated in RA5 and CMSM, while RA4 stood out for its lower responsiveness, with 57.7% stating that feedback is rarely or never considered.
Organizational Reforms	Prioritized by respondents included improvements in infrastructure and personnel management. These needs were most prominently expressed in RA5 (82.4%) and CMSM (70.6%).

4.3. Integrated Analysis

The cross-analysis between experience, unit affiliation, and personal perceptions revealed consistent patterns. Personnel with more than 11 years of service tended to evaluate organizational culture, leadership practices, and retention policies more positively, suggesting that institutional commitment and job satisfaction increase with time. Conversely, military members with

less than 10 years of service were more critical, particularly regarding inclusion strategies, leadership effectiveness, and work-life balance, indicating a potential gap in early-career engagement and support.

Notable differences emerged between units. Respondents from RA5 and CMSM provided more favorable assessments of infrastructure conditions, emotional well-being support, and the responsiveness of leadership to

feedback. In contrast, those from RA4 reported lower levels of satisfaction across multiple dimensions, pointing to a more challenging organizational climate. These discrepancies suggest that unit-specific practices and environments play a decisive role in shaping motivation, commitment, and retention.

Data convergence across methods revealed that, while financial compensation is a critical factor, it is not sufficient on its own to ensure sustained motivation and institutional commitment. Both interviewees and survey respondents emphasized the importance of clear and achievable career pathways, access to specialized training, institutional recognition, fair workload distribution, and effective leadership. These elements emerged as central to preserving morale and encouraging long-term career investment. The evidence also highlights a general lack of structured and proactive inclusion policies, limited responsiveness to personnel feedback, and inconsistent implementation of well-being strategies. Nonetheless, the commanders interviewed identified realistic and actionable improvements, including infrastructure upgrades, modernization of operational equipment, and the adoption of more human-centered leadership models that value proximity, fairness, and adaptability.

In summary, the sustainability of military careers within Artillery depends on a delicate balance between institutional demands and individual needs. Units that foster an environment of trust, cohesion, and development - supported by inclusive policies, responsive leadership, and strategic modernization - demonstrate stronger levels of retention and motivation. Conversely, structural rigidity, operational overload, and insufficient recognition continue to pose significant risks to workforce stability and mission readiness.

5. CONCLUSION

This study examined the career trajectories of Artillery officers and sergeants in the Portuguese Army, revealing a complex interplay between sociocultural and organizational factors. Statistically significant associations were found between variables such as length of service, unit of assignment, and perceptions of organizational culture, equality, motivation, and performance. Military personnel placed high value on close leadership, international missions, training opportunities, and institutional recognition. In contrast, personnel shortages, work overload, and inadequate working conditions emerged as key challenges to motivation and retention. The quantitative findings added depth and context to the qualitative insights,

reinforcing the multidimensional nature of the career experience.

In addressing Research Question 1 - *What determinants shape the military careers of Artillery officers and sergeants?* - the findings point to a dual framework: organizational and sociocultural. On the organizational side, career development is influenced by factors such as institutional culture, retention strategies, leadership quality, work environment, and the structuring of tasks. Sociocultural influences include a sense of mission, equality of opportunity, perceived fairness, and work-life balance. These factors interact dynamically to shape commitment, job satisfaction, and the decision to remain in service.

Concerning Research Question 2 - *To what extent do these factors shape career trajectories?* - the evidence confirms a structural impact across the career span. Organizational culture plays a central role in early career stages, functioning as a key driver of integration and initial motivation. As service time increases, perceptions of recognition, career development opportunities, leadership quality, and working conditions become more decisive. Career trajectories are thus guided by a perceived equilibrium between expectations, demands, and rewards - a balance that varies according to rank, experience, and organizational setting. Units with

more supportive environments tend to foster stronger professional commitment, while those marked by overload and lack of recognition tend to undermine retention.

In response to Research Question 3 - *What measures can mitigate the effects of these determinants?* - the study proposes a set of structural and organizational interventions. At the structural level, investments in modernizing infrastructure, renewing equipment, and updating organizational frameworks are essential. Organizationally, recommendations include implementing flexible work arrangements, strengthening participative and fair leadership, clarifying career pathways, and ensuring sustained investment in training and specialization. Furthermore, policy reform must address salary structures and expand social support programs such as access to housing and family support. Finally, formal mechanisms of recognition are essential to reinforce morale and institutional commitment.

These findings directly address the Primary Research Question - *What are the main contingencies, challenges, and opportunities associated with the military careers of Artillery officers and sergeants?* The main contingencies include persistent personnel and equipment shortages, rigid structures, and the

accumulation of non-operational tasks. Key challenges involve the retention of qualified personnel, difficulty maintaining work-life balance, and increasing demands for technological adaptation. On the other hand, valued opportunities include access to advanced training, participation in international missions, proximity-based leadership, and a cohesive professional identity grounded in institutional pride and esprit de corps. These factors emerge as strategic priorities for ensuring the sustainability and attractiveness of military careers in Artillery.

The study acknowledges several limitations. First, the relatively small number of survey participants may limit the representativeness of the findings. While the data yielded statistically significant trends, the limited sample size may not capture the full spectrum of perceptions within the Artillery branch. Additionally, some ranks or demographic groups may have been underrepresented, potentially influencing internal trend interpretations. The exclusive focus on Artillery prevents generalization to other military branches. Finally, time and resource constraints restricted both the scope of data collection and the depth of some analyses.

Despite these limitations, this research provides a comprehensive and evidence-based contribution

to understanding the conditions shaping Artillery careers. The mixed-methods approach - and the inclusion of participant voices - adds depth and relevance, offering actionable insights for improving human resource policies and reinforcing the operational readiness of the Portuguese Armed Forces.

5.1. Directions for Future Research

Future studies could replicate this methodology across other countries, branches and services, enabling comparative analyses beyond the Artillery context. Repetition of the current study may also be valuable in the coming years, especially as the integration of enlisted personnel into the Permanent Staff becomes more structured in the Portuguese Army. Longitudinal studies would further enhance understanding of how perceptions evolve over time, particularly during periods of institutional reform. Additionally, focused evaluations on the impact of recently implemented policies - such as the new military compensation regime - would offer valuable insight into their effectiveness and long-term implications.

Funding Information

The authors received no financial

support for the research, authorship, or publication of this article.

Conflict of Interest Statement

The authors declare no conflict of interest.

REFERENCES

- [1] Adams, G. B. 1993. Organizational metapatterns: Tacit relationships in organizational culture. *Administration and Society*, 25(2), 139-159.
- [2] Ahola, K., Honkonen, T., Isometsä, E., Kalimo, R., Nykyri, E., Aromaa, A., & Lönnqvist, J. (2005). The relationship between job-related burnout and depressive disorders - results from the Finnish Health 2000 Study. *Journal of Affective Disorders*, 88(1), 55-62.
- [3] Alves, J. H. E. (1999). A mulher e as Forças Armadas Portuguesas [Women and the Portuguese Armed Forces]. *Nação e Defesa*, (88), 71-80.
- [4] Azevedo, J., & Pereira, H. (2025). Gender and sexual minorities in the armed and police forces: Perceptions and mental health implications of Portuguese militaries - A qualitative study. *Armed Forces & Society*, 51(3), 313-336.
- [5] Belkhodja, O., Amara, N., Landry, R., & Ouimet, M. (2007). The extent and organizational determinants of research utilization in Canadian health services organizations. *Science Communication*, 28(3), 377-417.
- [6] Billett, S. (2011). *Vocational Education: Purposes, Traditions and Prospects*. Springer.
- [7] Brooks, S. K., & Greenberg, N. (2018). Non-deployment factors affecting psychological wellbeing in military personnel: literature review. *Journal of Mental Health*, 27(1), 80-90.
- [8] Campenhoudt, L. V., Marquet, J., & Quivy, R. (2019). *Manual de investigação em ciências sociais* [Handbook of research in social sciences] (5th ed.). Gradiva.
- [9] Coutinho, C.P. (2015). *Metodologia de investigação em ciências sociais e humanas: Teoria e prática* [Research methodology in social and human sciences: Theory and practice] (2nd ed.). Almedina.
- [10] Correia, A. de M. (2017). Que futuro para a indústria europeia de defesa? [What future for the European defense industry?]. *Revista Militar*, (2587/2588), 681-706.
- [11] Costa, P. S. (2024). Desafios das Forças Armadas na sequência da invasão Russa à Ucrânia [Challenges of the Armed Forces following the Russian invasion of Ukraine]. *Revista Militar*, (2669/2670), 585-592.
- [12] Croon, E., Sluiter, J., Kuijter, P., & Frings-Dresen, M. (2005).

- The effect of office concepts on worker health and performance: A systematic review of the literature. *Ergonomics*, 48(2), 119-34.
- [13] De Greef, M., & Van den Broek, K. (2004). *Quality of the working environment and productivity: Research findings and case studies*. European Agency for Safety and Health at Work.
- [14] Enzmann, D., Schaufeli, W. B., Jansen, P., & Rozenman, A. (1998). Dimensionality and validity of the Burnout Measure. *Journal of Occupational and Organizational Psychology*, 71(3), 331-351.
- [15] Ferrão, M. (2024). A situação mais preocupante para as FFAA são as tabelas remuneratórias dos militares [The most concerning issue for the Armed Forces is the military pay scale]. *Nascer do SOL*. <https://sol.sapo.pt/2024/04/13/general-mendes-ferrao-a-situacao-mais-preocupante-para-as-ffaa-sao-as-tabelas-remuneratorias-dos-militares/>
- [16] Flick, U. (2004). *Uma introdução à pesquisa qualitativa* [An introduction to qualitative research] (2nd ed.). Bookman.
- [17] Fortin, M. F. (1999). *O processo de investigação: Da concepção à realização* [The research process: From conception to implementation]. Luso Ciência.
- [18] Frey, C. B., & Osborne, M. A. (2013). *The Future of Employment: How susceptible are jobs to computerisation?* Oxford Martin Programme.
- [19] Gonçalves, F. M. (2013). Militares do sexo feminino no exército português - os últimos 20 anos [Female soldiers in the Portuguese Army - the last 20 years]. *Revista Militar*, (2536), 393-413.
- [20] Greenhaus, J. H., & Beutell, J. N. (1985). Sources of Conflict Between Work and Family Roles. *Academy of Management Review*, 10(1), 76-88.
- [21] Grilo, A. J. R. (2004). *Deontologia Militar Percepção de elementos caracterizadores da cultura e ambiente militar para o Século XXI* [Long-duration individual paper, Instituto de Altos Estudos Militares]. Repositório Institucional do Instituto de Altos Estudos Militares
- [22] Honkonen, T., Ahola, K., Pertovaara, M., Isometsä, E., Kalimo, R., Nykyri, E., Aromaa, A., & Lönnqvist, J. (2006). The association between burnout and physical illness in the general population - results from the Finnish Health 2000 Study. *Journal of Psychosomatic Research*, 61(1), 59-66.
- [23] Loureiro, N. A. R. S. (2023). *Influência da formação militar de carreira no desenvolvimento de competências dos militares das forças armadas portuguesas*

- [Influence of career military training on the development of skills among Portuguese Armed Forces personnel]. Instituto Universitário Militar.
- [24] Mandeiro, N. (2024). Quanto ganha um militar? De 821,83€ a 6.558,53€ [How much does a soldier earn? From €821.83 to €6,558.53]. *CNN Portugal*. <https://cnnportugal.iol.pt/recrutamentoobrigatorio/soldados/quanto-ganha-um-militar-de-821-83-a-6-558-53/20240405/660e7757d34e0498921f5e36>
- [25] Morais, D., 2016. A Integração da Perspetiva do Género nas Operações Militares. Vantagens e Desafios a Ultrapassar [The integration of the gender perspective in military operations: Advantages and challenges to overcome]. *Revista de Ciências Militares, IV* (2), 359-395.
- [26] Paranhos, R., Figueiredo Filho, D. B., Rocha, E. C. da, Silva Júnior, J. A. da, & Freitas, D. (2016). Uma introdução aos métodos mistos [An introduction to mixed methods]. *Sociologias, 18*(42), 384-411.
- [27] Pereira, R., & Eusébio, R. (2021). Riscos psicossociais. Uma ameaça no meio militar: O papel da autoeficácia, qualidade da liderança geral e conflito trabalho-família no burnout [Psychosocial risks. A threat in the military: The role of self-efficacy, general leadership quality and work-family conflict in burnout]. *Sociologia On Line, (27)*, 79-98.
- [28] Redko, L. L., Kuleshin, M. G., Goncharov, V. N., Kovalskaia, O. Yu., & Ivashova, V. A. (2020). Sustainable Development of Educational Organizations in a Rural Region: Socio-Cultural Determinants. *Advances in Economics, Business and Management Research, 147*, 145-148. Proceedings of the International Conference on Policies and Economics Measures for Agricultural Development (AgroDevEco 2020).
- [29] Repartição de Abonos/Direção de Serviços de Pessoal/Comando do Pessoal. (2025). *Atualizações remuneratórias com impacto nos abonos do pessoal do Exército* [Salary updates impacting Army personnel allowances]. Exército Português.
- [30] Rijo, F., Marreiros, J., Mairós, J., & Paquete, O. (2018). A retenção dos militares nas forças armadas [The retention of military personnel in the armed forces]. *Revista de Ciências Militares, 6*(1), 333-356.
- [31] Robbins, S.P. (2005). *Comportamento organizacional* [Organizational behavior] (11^a Edição). Pearson Prentice Hall.
- [32] Romão, A., Baltazar, S. M., Rosado, D. P., Fonseca, D., & Lopes, H. S. (2020). Reserva e reforma no Exército Português: Os números e as reconfigurações [Retirement and reform in the Portuguese Army:

- Figures and reconfigurations]. *Sociologia On Line*, (22), 138-163.
- [33] Rosado, D. P. (2017). *Elementos Essenciais de Sociologia Geral* [Essential elements of general sociology] (1ª Edição). Gradiva.
- [34] Rosado, D., Romão, A., Baltazar, M. S., & Fonseca, D. (2017). Forças Armadas, Cultura Organizacional e Valores Partilhados: Estratégia, Profissionalismo Militar e Desafios na Gestão de Recursos Humanos do Exército [Armed Forces, organizational culture and shared values: Strategy, military professionalism and challenges in Army human resources management]. *Proceedings of the II International Meeting of ISSOW*.
- [35] Santos, L. A., & Lima, J. V. (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* [Methodological guidelines for research projects] (Cadernos do IUM N.º 8, 2ª Edição). IUM.
- [36] Vicente, J. P. N. (2007). Inovação, Revolução e Transformação Militar em Curso: Contributos para um Enquadramento Conceptual [Innovation, revolution, and ongoing military transformation: Contributions to a conceptual framework]. *Revista Militar*, (2461/2462), 257-270.
- [37] Walton, R. E. (1973). Quality of working life: What is it? *Sloan Management Review*, 15(1), 11.
- [38] Whelan, C. (2016). Organisational culture and cultural change: A network perspective. *Australian & New Zealand Journal of Criminology*, 49(4), 503-519.
- [39] Yin, R. K. (2005). *Estudo de caso: Planejamento e métodos* [Case study: Design and methods] (2ª Edição). Bookman.

A NOVEL INSTRUCTIONAL DESIGN MODEL FOR MILITARY ACADEMIES: VALIDITY EVIDENCE FROM GENDARMERIE OFFICER CADETS

Steven HORNSTRA*, **Steven DURNING****,
Jaap HOOGENBOEZEM***, **Paul NEELISSEN******,
Walther VAN MOOK*****

*NATO Command and Control Centre of Excellence, Utrecht, The Netherlands; Royal Netherlands Army, Armed forces of the Netherlands, The Netherlands; School of Health professions Education, Maastricht University, Maastricht, The Netherlands; Academy for postgraduate medical education, Maastricht University Medical Centre+, Maastricht, The Netherlands, ** Department of medicine, Uniformed Services University of the Health Sciences, Bethesda, MD, USA; Center for health professions education, Uniformed Services University of the Health Sciences, Bethesda, MD, USA, *** Royal Netherlands Army, Armed forces of the Netherlands, The Netherlands; Department of political science, Maastricht University, Maastricht, The Netherlands, **** Royal Netherlands Army, Armed forces of the Netherlands, The Netherlands; Financial Audit Department, Netherlands Court of Audit, The Hague, The Netherlands, ***** School of Health professions Education, Maastricht University, Maastricht, The Netherlands; Academy for postgraduate medical education, Maastricht University Medical Centre+, Maastricht, The Netherlands; Department of intensive care medicine, Maastricht University Medical Centre+, Maastricht, The Netherlands

Integrating military training with academic education at military academies presents a significant challenge. Consequently, officer cadets often develop skills and academic abilities through separate learning tracks. This disjointed approach can hinder their capability to apply both domains cohesively in real-world contexts. To address this, an innovative integrated instructional design model was developed to align military training and academic education. A mixed methods study was conducted to gather validity evidence for this model, involving surveys and focus group sessions with officer cadets of the ROYAL NETHERLANDS MARECHAUSSEE

(i.e. a Gendarmerie Corps) at the NETHERLANDS DEFENCE ACADEMY. The findings of this study indicate that this integrated instructional design model successfully fulfills the requirements of both military training and academic education, and they provide insights for its potential implementation. Future research could explore the model's applicability in other professional domains, such as police education, where similar integration challenges exist.

Key words: *military academy; officer education; instructional design.*

1. INTRODUCTION

Military organizations are often among a nation's largest training organizations, in which the range in training programs varies widely, enabling professional development varying from cooks to tank drivers (Kerry: 2013). Training is crucial to ensure military personnel are fully prepared for the demands and unpredictability of military operations. For example, Laslie (2015) pointed out that after U.S. involvement in the Vietnam War, training programs put American pilots in a much better position against their adversaries than technological advancements did.

However, limited budgets and training facilities, among other things, continue confine military training activities (Kerry: 2013; McIntyre & Smith, 2013). Therefore, military organizations have to optimize their training efforts, and strive for effective and efficient learning environments. Vogel-Walcutt et al. (2013) stated that there is a need for appropriate instructional strategies to design such military

learning environments. Grant and Wesolkowski (2013), Stanney et al. (2013) and Walwanis et al. (2013) also emphasized the importance of suitable instructional strategies and design to advance the military learning processes. Moreover, Christensen and Tremblay (2013) and Vogel-Walcutt et al. (2013) advised to utilize evidence-based instructional design (ID) to enhance military training. Drawing on these perspectives, this paper elaborates upon a specific branch of military training: instruction of officer cadets to become officers.

Note, the concept of training is, as described above, often used to refer to activities that promote learning in general. However, regarding the professional development of officer cadets, Hornstra et al. (2023) have previously explicitly distinguished between (military) training and (academic) education. Both learning tracks are viewed as essential parts of an officer education program. Herein, (military) training aims at developing skills in order to perform a particular task. For instance, officer cadets are trained in skills required

to provide basic medical care in field conditions and to implement protective protocols in the event of chemical warfare incidents. On the other hand, (academic) education aims at developing strategic thinking, which represents higher-order cognitive abilities in military and related knowledge domains, in order to cope with situations that may have never been previously encountered. For instance, officer cadets receive education in geopolitical theory to anticipate evolving geopolitical dynamics during the conduct of military operations in their future roles. The strategic part of an officer's job cannot be learned by skills, drills and instruction cards, but is much more ambiguous and dependent on circumstances.

Naturally, certain subjects can be examined from both a military training and an academic education standpoint. To illustrate, the subject of leadership encompasses, among other things, the ability to communicate clear commands as well as the study of diverse leadership theories. During military operations, officers often need to use skills and strategic thinking simultaneously or even integrated. As an example, in territorial defense operations, Dutch Civil-Military Cooperation officers are required to effectively influence civilian stakeholders (demonstrating communication skills), and to assess the interests and manage the potential

impacts of these civilian stakeholders on the military operation within a given context (exhibiting strategic thinking) (Hornstra et al., 2024a). Nonetheless, at a military academy, military training and academic education are typically not optimally linked (Hornstra et al., 2023).

Officer cadets must focus on military training, academic education and character development (Van Schilt: 2011; Lepinoy et al., 2021). In his study of character building during the professional development of Dutch officer cadets, Van Schilt (2011) concluded that military training and academic education are explicitly and formally embedded in the institution's curriculum, whereas character building is considered a process of socialization by peers.

In the military, a widely endorsed training philosophy is "train as you fight" (Rietjens et al., 2013), in which training is meant in the general sense (i.e. both military training and academic education). To honor this well-known adage, it is imperative to foster a meaningful connection between military training and academic education throughout the professional development of officer cadets. Thus, Hornstra et al. (2024b) designed an integrated instructional design model, the so-called TrEd (Training-Education, pronounced as "tred") ID model, based on both the Nine events of instruction model (Gagné et al., 1992)

as an ID model for military training and STAR Legacy (Schwartz et al., 1999a, 1999b) as an ID model for academic education (see Appendix 1). Supported by the definition of ID of Burton et al. (1996), an ID model can be defined as a model structuring

a systematic process that uses tenets of learning theories to plan and present instruction or instructional sequences... to promote learning.

(p.115). In other words, an ID model arranges the ID process, such an ID process produces a purposeful learning environment, and such a learning environment stimulates and facilitates the actual learning of the students (e.g. officer cadets). Herein designers and teachers (e.g. military trainers and academic educators) focus on promoting student learning.

Könings et al. (2014, p.1) emphasized that the collaboration of different stakeholders

can improve the quality of the instructional design process and the resulting learning environments.

Or as Martens et al. (2019, p.1205) put it, a collaboration of designers, teachers and students in the ID process

improves active student engagement, student experience and effectiveness of the learning environment.

While Hornstra et al. (2025) have explored the perspectives of

teachers, it is equally important to consider the viewpoints of other stakeholders, notably those of the students. Students, such as officer cadets, are the users of designed instruction as they undergo the learning process. Even if students are often unaware of the underlying design and its intentions (Deslauriers et al., 2019), they are experienced users of designed instruction and should bring their expertise into the ID process (Könings & McKenney, 2017; Könings et al., 2017; Martens et al., 2019). The viewpoint of the students should therefore be considered to help improve the ID and the resulting instruction.

In the military context, students should also be involved in the designing process (Culkin: 2017). Fawley and Kyrsak (2013) highlighted that instruction to officer cadets should be tailored to their specific characteristics and needs. Moreover, this recommendation fits well with the general shift in the military from a teacher-centered to a student-centered approach (Sagendorf et al., 2009), as is simultaneously observed in, for example, health sciences education (Alizadeh et al., 2024). The purpose of the present study was to gather validity evidence for the TrEd ID model at a military academy from officer cadets' perspectives in order to refine and optimize the ID's framework and to explore

the requirements of its potential implementation at a military academy.

2. METHODS

We conducted a sequential mixed methods study, consisting of a survey and focus group sessions, to gather further validity evidence for the TrEd ID model at a military academy. The purpose of the survey was (a) to ascertain officer cadets' awareness of ID frameworks and (b) to gain primary insights on what officer cadets consider important regarding an ID framework. These primary insights served as areas of emphasis for the focus group sessions. The purpose of the focus group sessions was (c) to obtain a deeper understanding of the officer cadets' perspective on the TrEd ID model and the requirements of its potential implementation at a military academy. Thus, from the survey we mainly derived *what* elements of an ID model are important or less important to officer cadets, whereas during the focus group sessions we explored *why* these elements are valued as such, and how these elements can be related to the TrEd ID model and can potentially contribute to the TrEd ID model's implementation.

2.1. Survey

The survey contained 14 items to be rated on a 5-point Likert scale,

being (1) not important at all, (2) not important, (3) neutral, (4) important and (5) very important. The items reflected the various elements (i.e. prescribed activities) of the TrEd ID model (e.g. item 4 which reflected element 2.a). The survey ended with 3 open-ended questions about officer education. In formulating the items and open-ended questions, we used layman's language (e.g. item 4: *When I learn something, the teacher must build on my existing skills and knowledge instead of It is important to activate prior skills and knowledge before starting the learning process*). As input for the focus group sessions, the items rated as (very) important ($M > 4.00$, 1-5 scale) and the items rated as less than neutral ($M < 3.00$), reflecting positive and negative opinions respectively, in addition to the items that generated strong differences of opinion ($SD > 1.00$), were considered particularly relevant. In addition, for each of the three open-ended survey questions, if over 25% of the respondents provided the same answer, reflecting a certain degree of consensus, this response was identified as an area of particular interest throughout the focus group sessions. See Appendix 2 for an overview of the items and open questions of the survey.

2.2. Focus group sessions

We subsequently conducted face-to-face focus group sessions.

Focus groups enable participants during a social interactive process to complement and refine each other's views on a topic. Focus groups are thus particularly useful to gain and enhance in-depth insights on a topic from the perspective of the participants (Hennink: 2014; Carey et al., 2016; Davis: 2016). We followed the guidelines of the Association for Medical Education in Europe (AMEE) Guide No. 91 on the usage of focus groups in medical education research (Stalmeijer et al., 2014). In addition, we applied Krueger and Casey's (2009) questioning route, as applied in the aforementioned AMEE Guide. See Appendix 3 for an overview of the questioning route as utilized during the focus group sessions.

Each focus group session lasted a maximum of 90 minutes. The sessions were directed by a semi-structured interview guide. See Appendix 4 for the semi-structured interview guide. The development of this guide was based on the teaching and learning activities suggested by the TrEd ID model. To prevent participants from merely reacting to the different elements of the TrEd ID model instead of engaging in active discussion, we did not provide this ID framework to the focus group participants.

2.3. Participants

As typical officer cadets at a modern military academy, the officer cadets of the

ROYAL NETHERLANDS MARECHAUSSEE (i.e. a Royal Gendarmerie Corps) at the ROYAL MILITARY ACADEMY of the NETHERLANDS DEFENCE ACADEMY (NLDA) have to concentrate on military training, academic education and character development (De Waard et al., 2021). These Dutch officer cadets are thus familiar with military learning processes related to military training and academic education. Moreover, a robust foundational officer education (i.e. military training and academic education) is essential for the continued individual professional growth and the overall effectiveness of the ROYAL NETHERLANDS MARECHAUSSEE (De Waard et al., 2021). Indeed, the deployment of gendarmerie forces is increasingly regarded as vital for the success of NATO peace and stability operations (Ciampini & Dziedzic, 2022). That is why our purposive sampling strategy consisted of officer cadets of the ROYAL NETHERLANDS MARECHAUSSEE at the ROYAL MILITARY ACADEMY of the NLDA.

As De Waard et al. (2021) described, in the Netherlands, all officer cadets of the ROYAL NETHERLANDS MARECHAUSSEE are educated at the NLDA. Officer cadets with a prior bachelor's or master's degree follow a shortened officer education program,

the so-called short model. Depending on their future positions, this category of officer cadets may need to follow additional technical courses at the EDUCATION, TRAINING AND KNOWLEDGE CENTER of the ROYAL NETHERLANDS MARECHAUSSEE. In the long model, officer cadets with high school qualifications need to complete a military science bachelor's degree, which is offered by the FACULTY OF MILITARY SCIENCES of the NLDA. Focusing on the requirements of their future positions, this category of officer cadets must follow additional courses at the same EDUCATION, TRAINING AND KNOWLEDGE CENTER. Furthermore, De Waard et al. (2021) mentioned that selected non-commissioned officers (NCOs) follow a specific officer education program, whereas specialists and reserve officers follow a shortened specialist education program.

To guarantee that the scope of this study was limited to military training and academic education in the military context, we only selected long model officer cadets. Moreover, to ensure that the scope was confined to academic education as we above defined it (i.e. provided by the FACULTY OF MILITARY SCIENCES of the NLDA), we only selected long model officer cadets at the ROYAL MILITARY ACADEMY before they attend

the EDUCATION, TRAINING AND KNOWLEDGE CENTER of the ROYAL NETHERLANDS MARECHAUSSEE. On top of that, we only selected senior officer cadets (e.g. at the end of the first, second or third year) who had the opportunity to reflect on their learning processes. After all, junior officer cadets (e.g. at the beginning of their first year) made the transition from civilian to military life recently and may be less able to reflect on the learning process that they just started.

2.4. Theoretical framework and methodology

The study was set within the constructivism paradigm. This paradigm underscores the importance of qualitative research methods that allow active co-construction of data and analyses by participants and researchers (Peters et al., 2013; Chandra et al., 2017). Therefore, we selected as our research method the combination of focus groups and thematic analysis, in which a preceding survey provided additional input to the focus group sessions. Furthermore, our study was based on a phenomenological approach. As a philosophical viewpoint, phenomenology claims that human experiences are the origin of all knowledge. As a research methodology, phenomenology intends to capture the meaning of a phenomenon, in terms of both what

and how humans experienced such a phenomenon (Teherani et al., 2015). Phenomenological research enables us to understand complex phenomena, including phenomena related to learning (Neubauer et al., 2019). Here, we meant to understand the TrEd ID model in the context of a military academy, through the experiences of officer cadets.

2.5. Setting and procedure

We performed our study at the ROYAL MILITARY ACADEMY of the NLDA in Breda, the Netherlands. The ROYAL MILITARY ACADEMY offers officer education to officer cadets of the ROYAL NETHERLANDS ARMY, the ROYAL NETHERLANDS AIR FORCE and the ROYAL NETHERLANDS MARECHAUSSEE (Van Schilt: 2011). During the morning roll call, the commander of the officer cadet battalion of the ROYAL NETHERLANDS MARECHAUSSEE at the ROYAL MILITARY ACADEMY invited the officer cadets to participate in the study. The dates and location of the survey and the focus group sessions were determined by this commander based on the participants' availability. As Carey et al. (2016) have recommended, to avoid a difference in interpretations of concepts, all participants of the focus group sessions have previously participated in the survey.

The survey was administered on paper in class by the company commander of the officer cadets to optimize the response rate (March 31, 2023; Breda, the Netherlands). The focus group sessions were introduced (e.g. purpose and protocol) and conducted by two researchers; one as the moderator and one as the observer (SH and PN respectively) (June 6, 14 and 15, 2023; Breda, the Netherlands). All focus group sessions were audio recorded and transcribed verbatim.

To avoid being seen as outsiders, the researchers, who were themselves military officers, opted to wear their uniforms during the focus group sessions. Furthermore, at their introduction, the researchers requested the officer cadets to be addressed by their first names instead of ranks. Moreover, the researchers explicitly encouraged the officer cadets to share their opinions during the focus group sessions, whereas the researchers did not express theirs. In this way, we hoped that the officer cadets were not inhibited in expressing their opinions, despite being outranked by the researchers. The researchers further stimulated the participants to share their ideas and experiences freely by guaranteeing at the start of each focus group session that all data would be processed and reported anonymously.

2.6. Data analysis

We continued conducting focus group sessions until data saturation was reached, i.e. until the time when new ideas no longer arose (Stalmeijer et al., 2014). The research team determined, by consensus, the time of achievement of saturation, based on the thematic analysis in progress.

In the thematic analysis, we followed the six-step procedure of the deductive approach, as prescribed by Kiger et al. (2020) in AMEE Guide No. 131 on thematic analysis of qualitative data: (1) familiarizing with the data, (2) generating initial codes, (3) searching for themes, (4) reviewing themes, (5) defining and naming themes, and (6) writing the report. Two members of the research team (SH and PN) conducted the thematic analysis, in which inconsistencies on codes and themes were settled by consensus. If consensus was not reached, these differences were found a solution to by discussion within the whole research team (SH, JH, SD, PN, WvM). We utilized SPSS (version 28.0.0.0) and ATLAS.ti (version 24) for analyzing the quantitative data of the survey and organizing the thematic analysis respectively.

Member checking in general provides the participants the opportunity to check whether they have been interpreted correctly by the researchers. We applied the more comprehensive approach of

Olmos-Vega et al. (2022), enabling the participants to elaborate upon their earlier views and the researchers' interpretations of these views as well. In this way, member checking is an even more valuable extension of the process of co-construction of knowledge. In order to contribute to scientific rigor, we performed member checking during and at the conclusion of the focus group sessions, as part of the ongoing interaction, by frequently summarizing and verifying our interpretations of the discussions. After the sessions, we performed additional member checking by presenting the research findings to the participants by email allowing them to further reflect.

2.7. Reflexivity

We followed the guidelines of AMEE Guide No. 149 on reflexivity in qualitative research (Olmos-Vega et al., 2022). So we considered reflexivity as a continuous process during this study, in which we rather benefit from than try to explain and neutralize the researchers' background. Additionally, we used Walsh's (2003) typology of reflexive dimensions, as applied in AMEE Guide No. 149: (1) personal (the influence of the researchers' subjectivity on the research), (2) interpersonal (the influence of relationships between the persons involved on the research),

(3) methodological (the influence of the methodological decision-making process and decisions on the research), and (4) contextual reflexivity (the influence of the context on the people involved and the research).

We performed a collaborative method of reflexivity: every about six weeks the research team had a meeting, in which we examined and managed the meaning of our decisions. These considerations were structured by Walsh's (2003) typology, and included throughout the different sections of this manuscript.

Because of the strong influence on this study, three comments about personal reflexivity deserve their own place in this text. Firstly, four researchers (SH, SD, JH, PN) are experienced as (former) military officers. Secondly, two researchers (SD, WvM) are experienced as medical specialists. Thirdly, four researchers (SH, SD, JH, WvM) have professional credentials in education.

3. RESULTS

In this section, we first present the quantitative and qualitative findings from the survey, followed by the qualitative findings from the focus group sessions.

3.1. Survey - quantitative

24 out of 24 respondents completed the survey. Table 1 displays

the demographic characteristics of the survey participants.

Table 1 Demographic characteristics of participants

Age (years)	20.88 (Mean) 1.51 (SD)
Academic year	1 (N=6) 2 (N=9) 3 (N=9)
Highest previous education	High school diploma (N=24)

Note N=24.

Table 2 shows an overview of the quantitative survey results. Participants had a more positive opinion about item 11 (*I want to get feedback when I am practicing and trying out solutions*) (M=4.21, SD=0.71), whereas they had a more negative opinion about item 5 (*Before learning something, the other officer cadets and I want to share among ourselves our existing skills and knowledge*) (M=2.22, SD=0.78), item 9 (*The teacher must guide me when I am learning*)

(M=2.63, SD=1.15) and item 13 (*When learning, I need an assessment of my performance*) (M=2.88, SD=0.73). Further, there is little consensus about item 1 (*When a class starts, the teacher must get my attention first*) (M=3.58, SD=1.08) and again item 9.

Table 2 Summary of the quantitative survey data

Item	Mean (SD)
1. When a class starts, the teacher must get my attention first	3.58 (1.08)
2. At the beginning of a class, the teacher must tell me specifically what I must learn	3.50 (0.96)
3. At the beginning of a class, the teacher must show a real-life problem that I must learn to solve	3.09 (0.78)
4. When I learn something, the teacher must build on my existing skills and knowledge	3.65 (0.76)
5. Before learning something, the other officer cadets and I want to share among ourselves our existing skills and knowledge	2.22 (0.78)
6. The teacher must demonstrate or present to me what I must learn	3.83 (0.76)
7. I want to compare what I must learn on the one hand with my existing skills and knowledge on the other	3.13 (0.90)
8. I want to improve my skills and knowledge by experimenting and studying	3.91 (0.58)
9. The teacher must guide me when I am learning	2.63 (1.15)
10. I want to practice and try out solutions	3.88 (0.53)
11. I want to get feedback when I am practicing and trying out solutions	4.21 (0.71)
12. When learning, I want to apply my new skills and knowledge in a real-life environment	3.79 (0.87)
13. When learning, I need an assessment of my performance	2.88 (0.73)
14. At the end of a class, I want to reflect on the way I learned, and compare what I learned to what I should have learned	3.46 (0.71)

Note 1=very unimportant 2=unimportant 3=neutral 4=important 5=very important

3.2. Survey - qualitative

Table 3 presents an overview of the qualitative survey results. Participants indicated that the most important aspects of their officer education program are the linkage with the professional domain (i.e. connection with their prospective professional responsibilities) (54%) and active learning strategies (i.e. instructional design) (29%). Further, the most noteworthy facets are the teacher's quality (50%) and again the linkage with the professional domain (29%). Lastly, the areas identified for improvement are lengthy non-interactive lectures (i.e. instructional design) (29%) and yet again the linkage with the professional domain (29%).

3.3. Focus group sessions - qualitative

Across the three focus group sessions (N=6, N=6, N=5), we identified five themes that described participants' perceptions of the quality of their officer education program, that is to say, military training and academic education at a military academy: (1) Demarcation of learning process, (2) Support of learning process, (3) Authentic learning environment, (4) Active learning, and (5) Overall long-term objective of learning process. Table 4 shows the five identified themes, along with their respective definitions and illustrative quotes.

Table 3 Summary of the qualitative survey data

Open-ended question	Answers with a certain degree of consensus (>25%)
What two aspects are most important to you in your officer education?	Linkage with professional domain (54%) Instructional design (29%)
What two aspects do you appreciate most in your officer education?	Teacher's quality (50%) Linkage with professional domain (29%)
What two aspects would you like to improve in your officer education?	Instructional design (29%) Linkage with professional domain (29%)

Table 4 Definitions of themes

Theme	Description	Example quote
Demarcation of learning process	Qualities of an adequate beginning and end of a learning process	“...what have we learned, how can we look back on it”
Support of learning process	Assistance provided to officer cadets throughout a learning process	“When I get feedback, I prefer something concrete that you can work with”
Authentic learning environment	Connection of classroom learning with real-world issues	“If you learn something in a classroom and you can, like, do it in the woods half an hour later, I think that’s really useful”
Active learning	Officer cadet engagement and participation in the learning process	“...encouraged to think about the content and thus form your own opinion...”
Overall long-term objective of learning process	Focus on the overarching goal of the learning process	“Producing a high-quality outcome, namely a competent military leader”

3.4. Theme 1 – demarcation of learning process

The theme “Demarcation of learning process” describes the qualities of both an adequate beginning and end of a learning process. Concerning that beginning, participants underscored the significance of a teacher capturing the attention of officer cadets at the commencement of a class to initiate the learning process. For instance,

if a teacher plays a video at the beginning,

...everyone starts looking at it and then it seems as if the class starts a bit smoothly.

(Participant 4, Session 1). However, they had a high opinion of a teacher who

can keep the class under control... and not necessarily whether he has the tricks or ideas [for gaining attention].

(Participant 4, Session 2). Additionally, they pointed out that paying attention from the outset is primarily a matter of

...discipline [of officer cadets]... [and] respect [of officer cadets towards the teacher]...

(Participant 4, Session 1), and it is thus not solely the responsibility of the teacher to ensure this.

Participants valued a well-defined conclusion of the learning process, which was facilitated through reflective activities, especially via questions posed at the end of the class. These questions were seen as instrumental in promoting reflection on both the learning process and its outcomes, thereby aligning with the learning objectives and effectively concluding the learning experience. For instance, participants appreciated closing questions such as “...*what have we learned, how can we look back on it*” (Participant 5, Session 1). The advantages of such reflective practices might not be confined to the cognitive domain but also encompass emotional benefits, as participants articulated,

I think it can help some people to build in some certainty if you experience stress from it [i.e. the learning process]...

(Participant 6, Session 2).

3.5. Theme 2 – support of learning process

The theme “Support of learning process” put forward the

assistance provided to officer cadets throughout a learning process, focusing on learning objectives and prior knowledge/skills in the early stages of the learning process, and explicit directions and feedback in the subsequent stages. Participants emphasized the critical role of learning objectives in aiding their focus and structuring their learning process. They noted that

The learning objectives often also appear in the exams, so you have a clear guideline throughout the lectures: Okay, this is really the most important part of the lecture and I really have to pay attention to this.

(Participant 3, Session 2). Additionally, participants stressed the importance of having concise and limited learning objectives, which allow for better pre-lecture processing:

...there could be six of them [i.e. learning objectives], really long sentences, that you just can't process right away. In the meantime, the teacher just keeps talking, because he just keeps going on with his presentation...

(Participant 2, Session 1). Furthermore, participants recognized the relevance of building new knowledge and skills upon existing ones. They reported that prior knowledge facilitated the understanding of new concepts, as stated in the commentary

I really noticed that: Oh yes, I learned this before [i.e.

prior knowledge] and that I could understand it [i.e. the new knowledge] more easily, I think, than if I had not had that prior knowledge.

(Participant 6, Session 1).

Moreover, the significance of explicit directions in the learning process was also underlined. Participants appreciated clear cues, such as

...this is important, so read this section of the literature...

(Participant 4, Session 1). They also valued other forms of guidance, including following the teacher's thought process and learning structured problem-solving methodologies, as voiced by participants respectively:

It was very nice to follow the teacher's train of thought.

(Participant 3, Session 1) and

...you learn to look at problems in a certain way, a kind of structured approach to a final solution.

(Participant 5, Session 1). In addition, feedback was deemed highly beneficial by participants, particularly performance-oriented feedback that offered concrete, actionable suggestions:

When I get feedback, I prefer something concrete that you can work with.

(Participant 4, Session 3). Affirmative feedback was also highly valued, as evidenced by participants' cheerful reactions to teachers' constructive comments:

Interesting that you look at it that way and thanks for your input. Just very positive.

(Participant 2, Session 1).

3.6. Theme 3 – authentic learning environment

The theme "Authentic learning environment" represents the connection of classroom learning with real-world issues. Participants thought highly of linking theoretical insights with direct practical application:

If you learn something in a classroom and you can, like, do it in the woods half an hour later, I think that's really useful.

(Participant 2, Session 1). In addition to that, with a view to the longer term, participants accentuated the necessity for an educational setting that addresses the future professional domain explicitly, as participants appreciated

...more focus on [professional] practice and on the future execution of our tasks.

(Participant 2, Session 3) for their learning environment. This focus includes visits to relevant professional locations such as "...an operational border control post..." (Participant 1, Session 3) and "...[the international airport] Schiphol..." (Participant 6, Session 2). Participants even communicated downright demotivation when the connection to their prospective professional area was not apparent, reflected in the remark

But the ROYAL NETHERLANDS MARECHAUSSEE was never discussed. So we thought: Well, whatever.
(Participant 3, Session 3).

3.7. Theme 4 – active learning

The theme “Active learning” describes the officer cadet engagement and participation in the learning process. Participants indicated an aversion to passive information absorption over extended periods, often metaphorically referred to as “sponging” (Participant 6, Session 2), which they felt “...leads to a loss of concentration” (Participant 3, Session 2). Instead, in class, participants valued the “*alternation between practice and theory*” (Participant 1, Session 1). They favored being

...encouraged to think about the content and thus form your own opinion...

(Participant 2, Session 1), resulting in

...not only acquiring knowledge but also learning to think [critically].

(Participant 3, Session 1). Indeed, they appreciated active learning methods such as “...discussion...” (Participant 2, Session 1), creating “...a video to explain the subject matter to your class...” (Participant 2, Session 1), watching

...a video and you get some questions about it... that you get some practical examples and how are you going to apply that [i.e. new knowledge/

skills] to it [i.e. video/practical examples].

(Participant 3, Session 3), and designing and reflecting on strategies through a “war game” (Participant 4, Session 3). At curriculum level, participants thought highly of the typical diversity of activities at a military academy, that is a “...*variety of sports, study, military activities*” (Participant 6, Session 2). However, participants cautioned against a standardization in active learning methods, in particular the so-called “syndicate assignments”, which can be experienced as tedious, as noted in the remark about their typical composition,

Here's an assignment, here's a question, you have five minutes, work it out with a group and then you present it.

(Participant 3, Session 2).

Simultaneously, they expressed fascination

...when someone tells a really interesting story for an hour and a half, with passion.

(Participant 1, Session 2). For such lectures to be effective, they prioritized a clear focus on the most essential content, avoiding excessive detail that could lead to confusion, asserting that it is critical that

... [a teacher] leaves it at the really important things, and doesn't go into everything with the result that in the end you don't even know what you need to know for the test.

(Participant 3, Session 1). Nevertheless, it was perceived

crucial that this focus does not become overly rigid. To prevent monotony in classes, flexibly incorporating “...experiences [of the teacher]...” (Participant 3, Session 3) and fostering “...interaction [between teachers and officer cadets]...” (Participant 3, Session 2) are essential.

In active learning in class, participants emphasized the pivotal role of the teacher, that is to say the military trainer and academic educator, as illustrated by the comment

...the teacher is very important, how a teacher stands in front of a group, how he speaks and how he takes into account the interaction of the class.

(Participant 6, Session 2). Elaborating on the teacher’s qualities, participants felt that, above all, a teacher has to be an “...expert...” (Participant 4, Session 1). While acknowledging the criticality of subject matter expertise, they stressed the imperative for teachers to present their expertise in an engaging manner, as remarked by the commentary

...so not very tedious and just that you can convey it a little bit nicely, that you make a nice story out of it.

(Participant 1, Session 1). At curriculum’s level, participants appreciated the variety of teachers as well, as reflected in the observation,

One time there is a professor who is a civilian, and the next time there is a general

or major standing in front of you.

(Participant 3, Session 2).

3.8. Theme 5 – long-term objective of learning process

The theme “Long-term objective of learning process” represents the focus on the overarching goal of the learning process, which is to transform officer cadets into competent officers. Participants made a point of the lack of cohesion between military trainers and (civilian) academic educators in their joint commitment to the professional development of officer cadets. This sentiment was echoed by participants who remarked,

...I don’t really feel a sense of unity between the faculty [i.e. academic educators] and the military academy [i.e. military trainers]...

(Participant 3, Session 3). Additionally, concerns about that collaboration emerged, with statements such as

...the faculty and the military academy are somewhat different islands...

(Participant 4, Session 3). Across different sessions, participants independently used the metaphor of “...a child of divorced parents...” (Participant 6, Session 2; Participant 4; Session 3) to describe their situation, feeling caught between military training and academic education. As a result, participants expressed a sense of “...living in two worlds” (Participant 3, Session 3), necessitating

...constantly switching... It shouldn't be that way, but that's how it works.

(Participant 2, Session 3). Consequently, participants emphasized

...that they [i.e. military trainers and academic educators] need to coordinate much better with each other.

(Participant 3, Session 3). They believed that a meaningful link between military training and academic education would be advantageous to their professional development, embedded in their response

...that this [linkage] is a much more effective way to educate officer cadets...

(Participant 2, Session 3). For example, participants discussed the

...great opportunity to link the knowledge of all the professors and doctors to a [military] exercise that we are going to do... this could be more intertwined...

(Participant 1, Session 3). They communicated downright excitement

...where we had really a linkage [between military training and academic education] and that was also really cool.

(Participant 2, Session 3).

Participants reasoned along the same lines that the objective of the learning process should extend beyond the mere achievement of passing exams, positing instead that assessments ought to serve

as a mechanism for determining the readiness of officer cadets for their impending duties. As a result, participants reported that teachers should orient their assessment strategies towards

Producing a high-quality outcome, namely a competent military leader.

(Participant 3, Session 1) rather than officer cadets jumping through hoops.

4. DISCUSSION

The results of our study provided validity evidence supporting the teaching and learning activities of the TrEd ID model, an integrated ID model for both military training and academic education, as an effective learning strategy for officer cadets. Additionally, the results offered potential directions for implementation of this ID model. In the below sections, we elaborate on these two main points.

4.1. Validity evidence for the TrEd ID model

The majority of the survey and focus group data revealed that officer cadets appreciated the activities linked to the sequential phases of the TrEd ID model. Table 5 illustrates the ways in which the activities of this ID model potentially jointly support the principal themes recognized by officer cadets as critical to the quality of their officer education program. The officer cadets' perceptions of this quality thus aligned with the TrEd ID model's teaching and learning activities.

Table 5 Alignment of TrEd ID model activities with key themes

Description	Theme
Getting attention Reflecting on learning process and outcomes in relation to the learning objectives	Demarcation of learning process
Providing learning objectives Activating prior knowledge/skills/experiences Sharing initial skills/ideas Comparing content with initial skills/ideas Providing guidance Providing feedback	Support of learning process
Providing authentic problem to be solved Performing skills/solving problems in authentic environments	Authentic learning environment
Showing content Complementing skills/ideas by experimenting and studying Practicing skills/trying out solutions	Active learning
Assessing performance/problem solving	Overall long-term objective of learning process

They considered *Activating prior knowledge/skills/experiences*, *Sharing initial skills/ideas*, and *Comparing content with initial skills/ideas* as either a single joint, aggregated activity or three closely interwoven activities that collectively connect the learning process with prior knowledge and skills. Officer cadets seemed to view activities related to addressing realistic problems, including *Providing authentic problems to be*

solved, *Complementing skills/ideas through experimenting and studying*, *Practicing skills/trying out solutions*, and *Performing skills/solving problems in authentic environments*, likewise either as a single activity or as four closely interconnected activities that collectively support practice in an authentic learning environment. These officer cadets' experiences suggest that the activities within the TrEd ID model do not need to be as distinctly separated and

linearly sequential as the design (see Appendix 1) displays. Consistent with Barua and Lockee's (2024) call for more flexible course design through customizing content and instructional strategies, this implies that teachers could adopt a flexible approach to the design, clustering activities or altering their sequence as needed, provided that the purpose of the activities continues to receive adequate attention.

4.1.1. Discrepancy between survey and focus group data

Based on the quantitative survey data only, it initially appeared that officer cadets either disagreed with or did not fully appreciate certain activities of the TrEd ID model. The findings from the focus group sessions subsequently revealed a more nuanced perspective. These initially suggested differences between the data appear attributable to several explanatory factors.

First, quantitative survey data indicated that officer cadets did not perceive a need to share their existing skills and knowledge with each other before initiating mastering new content. Focus group data clearly suggested that officer cadets nevertheless recognized the importance of building new knowledge and skills upon their existing ones. As previously mentioned, it appeared that they did not consider *Sharing initial*

skills/ideas a distinct activity. Additionally, it is conceivable that they were previously unfamiliar or uncomfortable with this specific activity, or they believed that there was no opportunity to engage in it during class due to time constraints.

Second, quantitative survey data demonstrated little consensus and appreciation regarding support during the learning process. Nonetheless, focus group data unequivocally showed that officer cadets greatly appreciated support during the learning process, including explicit directions. A possible reason for this discrepancy is that, when asked about the need for support without contextual information in the survey, some officer cadets may have anticipated a reduction in their sense of autonomy, which could negatively impact their intrinsic motivation (Deci & Ryan, 2000).

Third, according to quantitative survey data, officer cadets did not highly value assessments. The reason for this may be that, as focus group data revealed, officer cadets often perceived current assessment methods as artificial and lacking meaningfulness. Consequently, these assessments may fail to foster a sense of competence, thereby again not enhancing intrinsic motivation (Deci & Ryan, 2000).

Fourth, quantitative survey data indicated a divergence of opinions regarding the necessity for teachers

to capture officer cadets' attention at the beginning of a class. However, focus group data clearly underscored the importance of establishing a definitive starting point for the learning process. Given that discipline and respect are esteemed virtues among officer cadets (Van Schilt: 2011), some officer cadets viewed active participation in the learning process mainly as a personal responsibility. This perspective may account for the observed lack of agreement in the quantitative survey data.

4.2. Potential directions for implementation of TrEd ID model

The findings of this study offer recommendations for the implementation of the TrED ID model at a military academy. These recommendations concern the teacher's involvement, real-world connection, and linkage between military training and academic education. In the following sections, we discuss these recommendations in detail.

4.2.1. Teacher's involvement

We consider the role of teachers in fostering an active learning environment pivotal, as emphasized by the officer cadets. The TrEd ID model is a possible instrument to substantiate the active learning style desired by the cadets. After all, active learning implies students' active

participation in class to engage them in their learning process (Park & Xu, 2024), which is exactly the intention of the TrED ID model's activities. Wang (2023) emphasized the critical role of teachers in ID in higher education, highlighting their contribution to creating effective learning experiences and the resultant positive learning outcomes. With regard to officer education programs, Kem and Bassett (2018) arrived at the same conclusion. Consequently, proficient teachers, by which the officer cadets meant military trainers and academic educators who possess substantive knowledge and pedagogical expertise, should play an active role in introducing and applying models such as the TrEd ID model.

4.2.2. Real-world connection

In this section, we address the officer cadets' emphasis on the importance of an authentic learning environment and the integrations of the TrEd ID model with practical applications to bridge the gap between theory and real-world practice. The officer cadets persistently expressed the relevance of an authentic learning environment. It is therefore recommended that the TrEd ID model not be implemented in isolation from practice, but rather be used as a bridge to the real world. Various activities of the model explicitly aim to create an authentic learning environment, for

example, *Performing skills/solving problems in authentic environments*. However, the remaining activities of the TrEd ID model, such as *Showing content* and *Providing learning objectives*, can also be aligned with realistic situations. For instance, the teacher could illustrate the content with examples from professional practice or current events. As another example, the teacher could link the learning objectives to tasks within the cadets' future duties.

4.2.3. Linkage between military training and academic education

This section delves into the disparity that officer cadets experience during their professional development between military training and academic education. The officer cadets expressed that they generally perceived military training and academic education as separate and distinct domains within the military academy. For officer cadets, this historically evolved organizational division evidently introduces unnecessary obstacles in the planning and coordination of learning activities within a military academy as a whole. This disconnection also seemed to affect negatively their experience of the ultimate learning goal: becoming a competent military leader.

On such disconnections in general, Vygotsky (1978) offered a socio-cultural viewpoint. He

claimed that cognitive processes, such as learning processes, cannot be understood in isolation from their environment. Vygotsky (1978) posited that cognitive processes are shaped through language and tools in interaction with a socio-cultural context. In practice, this means that learning processes are developed through language use, terminology, methods, customs and practices. Consequently, during their officer education, cadets must navigate and adapt alternately to the distinct socio-cultural contexts of both military training and academic education. This necessitates proficiency in two separate sets of language and tools. According to Vygotsky (1978), this introduces unnecessary complexity into the cadets' learning process.

The validity evidence collected in this study for the TrEd ID model, as an integrated ID model addressing both military training and academic education, suggests that its terminology and procedure could help establish a unified language and set of tools for both military trainers and academic educators. This common ground could potentially strengthen the linkage between military training and academic education at a military academy, thereby enhancing the cadets' learning experience. By leveraging this common ground, military trainers and academic educators could eventually collaborate to

optimize the learning process of officer cadets. They could achieve this by cooperatively designing and offering real-life tasks within authentic learning environments. This approach would foster a unified socio-cultural context, wherein cadets would need to integrate both skills and strategic thinking.

4.3. Strengths and limitations

This study has a number of strengths. We conducted the research at the end of the academic year when all participants had already experienced both military training and academic education. Additionally, all participants, including first-year officer cadets, had ample opportunity to reflect on their learning process. This combination optimized the likelihood of obtaining well-considered and substantiated opinions from the cadets regarding their officer education experience. Furthermore, we limited this study to “long-term model students” only. This means that all participants began their officer education program directly after high school. Consequently, their opinions were not influenced by experiences at other higher education institutions but solely pertain to their experience at the military academy.

However, there are also some limitations. The Dutch officer education program of the ROYAL NETHERLANDS

MARECHAUSSEE was only added to the ROYAL MILITARY ACADEMY of the NLDA since the beginning of this century. This means that for nearly two centuries, the officer education programs there were merely focused on the needs of cadets of the army, and later also air force. Additionally, the group of officer cadets from the ROYAL NETHERLANDS MARECHAUSSEE continues to be small compared to the officer cadets from the other branches (a few dozens versus hundreds each academic year). As a result, the officer education program is naturally often primarily still oriented towards the army and air force, as repeatedly confirmed by the focus group participants. This orientation can negatively affect the ROYAL NETHERLANDS MARECHAUSSEE officer cadets' perception of their officer education program, and consequently, the findings of this study. Furthermore, the reliance on single-site sampling potentially limits the transferability of the study's findings to other military academy contexts. Moreover, the survey design may not have provided participants with sufficient contextual information to optimally interpret and consequently answer the survey questions. Lastly, the member checking procedure was not appropriate to contribute to our interpretation of the differences between the quantitative and qualitative data.

4.4. Future research

Future research should further explore the differences in the quantitative and qualitative data during follow-up focus group sessions with the participants in order to gain deeper insights into officer cadets' perceptions of the quality of an officer education program in general and the TrEd ID model in particular. In addition, adding perspectives from other groups of stakeholders of the officer cadets' learning process at a military academy, including future commanders of the officer cadets, contributing to further validity evidence for the TrEd ID model is necessary to acquire a full understanding of the TrEd ID model, and its practical implications for the military in general. Non-military fields are likewise challenged to bridge the gap between military training and academic education in their professional development programs, including police education (Voigt & Zinner, 2023) and medical education (Firstenberg & Stawicki, 2022). So future research could also aim to collect validity evidence for the TrEd ID model in additional fields.

5. CONCLUSIONS & ACKNOWLEDGMENT

This study provides validity evidence for the TrEd ID model as an integrated ID model that effectively meets the requirements of

both military training and academic education for officer cadets. The TrEd ID model's activities thus align with the key themes identified by officer cadets as crucial to the quality of their officer education program. However, the findings of this study indicate that military trainers and academic educators could employ a flexible approach to the ID model. They can group the TrEd ID model's activities or modify their sequence as necessary, as long as the objectives of the activities remain adequately addressed. Regarding the implementation of the TrEd ID model, providing authentic meaningful content and context by competent military trainers and academic educators in collaboration was perceived paramount from the officer cadets' perspective.

5.1. Acknowledgment

We thank the following officers of the ROYAL NETHERLANDS MARECHAUSSEE for their support and organization: LCOL Mark Helgers, MAJ Dewi Kunstt, CPT Daan Langenberg and CPT Vincent Engelen.

REFERENCES

- [1] Alizadeh, M., Parmelee, D., Nordquist, J., The power of metaphor: Learning space and faculty development. In: *Medical Science Educator*, Vol. 34, No. 1, 2024. DOI: 10.1007/s40670-024-02024-w
- [2] Barua, L., Lockee, B.B., A review of

- strategies to incorporate flexibility in higher education course designs. In: *Discover Education*, Vol. 3, No. 1, Article number 127, 2024. DOI: 10.1007/s44217-024-00213-8
- [3] Burton, J., Moore, D., Magliaro, S., (1996). Behaviorism and instructional technology. In D. Jonassen (Ed.), *Handbook of Research for Educational Communications and Technology*. Prentice Hall.
- [4] Carey, M.A., Asbury, J.-E., (2016). *Focus Group Research (digital edition)*. Routledge. DOI:10.4324/9781315428376
- [5] Chandra, Y., Shang, L., An RQDA-based constructivist methodology for qualitative research. In: *Qualitative Market Research*, Vol. 20, No 1, 2017. DOI:10.1108/QMR-02-2016-0014
- [6] Christensen, B., Tremblay, R., (2013). Generational learning differences: Myth or reality. In G. Galanis, R. Sottolare, C. Best (Eds.), *Fundamental issues in defense training and simulation*. CRC Press.
- [7] Ciampini, D., Dziedzic, M., Assessing the results of gendarmerie type forces in peace and stability operations. In: *Militaire Spectator*, Vol. 191, No. 3, 2022. https://militairespectator.nl/sites/default/files/teksten/bestanden/militaire_spectator_3_2022_dziedzic_ciampini_GTF.pdf
- [8] Culkin, D.T., Military design insights for online education program evaluation: A revised theoretical construct. In: *American Journal of Distance Education*, Vol. 31, No. 4, 2017. DOI:10.1080/08923647.2017.1359138
- [9] Davis, C., (2016). *Focus groups: Applying communication theory through design, facilitation, and analysis (1st ed.)*. Routledge. DOI:10.4324/9781315298511
- [10] De Waard, E.J., Den Boer, M., Helgers, M., ‘Een leven lang leren’ binnen de Koninklijke Marechaussee. Ondersteunt het huidige officiersonderwijs het streven naar ‘een leven lang leren’? (‘Lifelong learning’ within the Royal Netherlands Marechaussee. Does the current officer education support the pursuit to ‘lifelong learning’?). In: *Militaire Spectator*, Vol. 190, No. 6, 2021. https://www.militairespectator.nl/sites/default/files/teksten/bestanden/militaire_spectator_6_2021_dewaard.pdf
- [11] Deslauriers, L., McCarty, L.S., Miller, K., Callaghan, K., Kestin, G., Measuring actual learning versus feeling of learning in response to being actively engaged in the classroom. In: *Proceedings of the National Academy of Sciences*, Vol. 116, No. 39, 2019.
- [12] Fawley, N.E., Kyrzak, N., (2013). Serving those who serve: Outreach and instruction for student cadets and veterans. In D.M. Mueller (Ed.), *Imagine, innovate, inspire: The proceedings of the Association of College and Research Libraries 2013 Conference*. Association of College and Research Libraries.
- [13] Firstenberg, M.S., Stawicki, S.P., (2022). *Medical education for the 21st century*. IntechOpen.
- [14] Gagné, R.M., Briggs, L.J., Wager, W.W., (1992). *Principles of instructional design (4th ed.)*. Harcourt Brace Jovanovich College Publishers.
- [15] Grant, S., Wesolkowski, S., (2013). The allocation of training to live and virtual environments. In G.

- Galanis, R. Sottolare, C. Best (Eds.), *Fundamental issues in defense training and simulation*. CRC Press.
- [16] Hennink, M.M., (2014). *Focus group discussions*. Oxford University Press.
- [17] Hornstra, S.P.A., Hoogenboezem, J.A., Durning, S.J., Van Mook, W.N.K.A., Instructional design linking military training and academic education for officer cadets: A scoping review. In: *Journal of Military and Strategic Studies*, Vol. 22, No. 4, 2023. <https://jmss.org/article/view/76275/57091>
- [18] Hornstra, S.P.A., Hoogenboezem, J.A., Durning, S.J., Van Mook, W.N.K.A., Military design thinking: Shaping a new training program for Dutch Civil-Military Cooperation officers. In: *NATO C2COE Annals of Command and Control*, Vol. 1, No. 1, 2024a.
- [19] Hornstra, S.P.A., Durning, S.J., Hoogenboezem, J.A., Van Mook, W.N.K.A., Closing the gap between skills training and academic education at a military academy: An integrated instructional design model. In: *Ukrainian Journal of Educational Studies and Information Technology*, Vol. 12, No. 1, 2024b. <https://uesit.org.ua/index.php/itse/article/view/445>
- [20] Hornstra, S.P.A., Hoogenboezem, J.A., Durning, S.J., Van Mook, W.N.K.A., The best of two worlds? Gathering validity evidence for an integrated instructional design model for skills training and academic education at a military academy. In: *Journal of Defense Resources Management*, Vol. 16, No. 1, 2025. <https://jodrm.eu/wp-content/uploads/2025/05/JODRM-APRIL-2025.pdf>
- [21] Kem, J.D., Bassett, W.E., The right education and training at the right time: Deciding what to teach and ensuring it happens. In: *Journal of Military Learning*, Vol. 2, No. 1, 2018. <https://www.armyupress.army.mil/Journals/Journal-of-Military-Learning/Journal-of-Military-Learning-Archives/April-2018-Edition/The-Right-Education-and-Training-at-the-Right-Time>
- [22] Kerry, J., (2013). Competency in the military. In G. Galanis, R. Sottolare, C. Best (Eds.), *Fundamental issues in defense training and simulation*. CRC Press.
- [23] Kiger, M.E., Varpio, L., Thematic analysis of qualitative data: AMEE Guide No. 131. In: *Medical Teacher*, Vol. 42, No. 8, 2020. DOI:10.1080/0142159X.2020.1755030
- [24] Könings, K.D., Bovill, C., Woolner, P., Towards an interdisciplinary model of practice for participatory building design in education. In: *European Journal of Education*, Vol. 52, No. 4, 2017. DOI: 10.1111/ejed.12230
- [25] Könings, K.D., McKenney, S., Participatory design of (built) learning environments. In: *European Journal of Education*, Vol. 52, No. 3, 2017. DOI:10.1111/ejed.12232
- [26] Könings, K.D., Seidel, T., Van Merriënboer, J.J.G., Participatory design of learning environments: Integrating perspectives of students, teachers, and designers. In: *Instructional Science*, Vol. 42, No 1, 2014. DOI:10.1007/s11251-013-9305-2
- [27] Laslie, B.D., (2015). *The Air Force way of war: U.S. tactics and training after Vietnam*. The

- University Press of Kentucky.
- [28] Lepinoy, A., Lo Bue, S., Vanderlinde, R., Basic needs satisfaction in a military learning environment: An exploratory study. In: *Military Psychology*, Vol. 34, No. 1, 2021. DOI:10.1080/08995605.2021.1973793
- [29] Martens, S.E., Meeuwissen, S.N.E., Dolmans, D.H.J.M., Bovill, C., Könings, K.D., Student participation in the design of learning and teaching: Disentangling the terminology and approaches. In: *Medical Teacher*, Vol. 41, No. 10, 2019. DOI:10.1080/0142159X.2019.1615610
- [30] McIntyre, H.M., Smith, E., (2013). Key tenets of collective training. In G. Galanis, R. Sottolare, C. Best (Eds.), *Fundamental issues in defense training and simulation*. CRC Press.
- [31] Neubauer, B.E., Witkop, C.T., Varpio, L., How phenomenology can help us learn from the experiences of others. In: *Perspectives on Medical Education*, Vol. 8, 2019. DOI:10.1007/s40037-019-0509-2
- [32] Olmos-Vega, F.M., Stalmeijer, R.E., Varpio, L., Kahlke, R., A practical guide to reflexivity in qualitative research: AMEE Guide No. 149. In: *Medical Teacher*, 2022. Advance online publication. DOI:10.1080/0142159X.2022.2057287
- [33] Park, E.S., Xu, D., The effect of active learning professional development training on college students' academic outcomes. In: *Journal of Research on Educational Effectiveness*, Vol. 17, No. 1, 2024. DOI:10.1080/19345747.2022.2151954
- [34] Peters, L.D., Pressey, A.D., Vanharanta, M., Johnston, W.J., Constructivism and critical realism as alternative approaches to the study of business networks: Convergences and divergences in theory and in research practice. In: *Industrial Marketing Management*, Vol. 42, No. 3, 2013. DOI:10.1016/j.indmarman.2013.02.003
- [35] Rietjens, S., Van Fenema, P.C., Essens, P., "Train as you fight" revisited: Preparing for a comprehensive approach. In: *PRISM*, Vol. 4, No. 2, 2013.
- [36] Ryan, R.M., Deci, E.L., Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. In: *American Psychologist*, Vol. 55, No. 1, 2000. DOI: 10.1037/0003-066X.55.1.68
- [37] Sagendorf, K., Noyd, R.K., Morris, D.B., The learning-focused transformation of biology and physics core courses at the U.S. Air Force Academy. In: *Journal of College Science Teaching*, Vol. 38, No. 3, 2009.
- [38] Schwartz, D.L., Brophy, S., Lin, X., Bransford, J.D., Software for managing complex learning: Examples from an educational psychology course. In: *Educational Technology Research and Development*, Vol. 47, No. 2, 1999a. DOI:10.1007/bf02299464
- [39] Schwartz, D.L., Lin, X., Brophy, S., Bransford, J.D., (1999b). Toward the development of flexibly adaptive instructional designs. In C.M. Reigeluth (Ed.), *Instructional-design theories and models: New paradigms of instructional theory, Volume 2*. Lawrence Erlbaum Associates.
- [40] Stalmeijer, R.E., McNaughton, N., Van Mook, W.N.K.A., Using

- focus groups in medical education research: AMEE Guide No. 91. In: *Medical Teacher*, Vol. 36, No. 11, 2014, DOI:10.3109/0142159X.2014.917165
- [41] Stanney, K., Carroll, M., Champney, R., DeVore, L., Hale, K., (2013). Virtual environment training design: Pros, cons, and tailored solutions. In G. Galanis, R. Sottolare, C. Best (Eds.), *Fundamental issues in defense training and simulation*. CRC Press.
- [42] Teherani, A., Martimianakis, T., Stenfors-Hayes, T., Wadhwa, A., Varpio, L., Choosing a qualitative research approach. In: *Journal of Graduate Medical Education*, Vol. 7, No. 4, 2015. DOI: 10.4300/JGME-D-15-00414.1
- [43] Van Schilt, J.T., (2011). *Herfsttij van het militaire elitegevoel. Het elitair zelfbeeld van aspirant-officieren op de Koninklijke Militaire Academie in de periode 1948 tot 2008 (Autumn tide of the military elite feeling. The elitist self-image of officer cadets at the Royal Military Academy in the period from 1948 to 2008)*. [Doctoral dissertation]. Tilburg University.
- [44] Vogel-Walcutt, J.J., Fiorella, L., Malone, N., Instructional strategies framework for military training systems. In: *Computers in Human Behavior*; Vol. 29, No. 4, 2013. DOI:10.1016/j.chb.2013.01.038
- [45] Voigt, L., Zinner, C., How to improve decision making and acting under stress: The effect of training with and without stress on self-defense skills in police officers. In: *Journal of Police and Criminal Psychology: The Official Journal of the Society for Police and Criminal Psychology*, Vol. 38, No. 4, 2023. DOI: 10.1007/s11896-023-09607-0
- [46] Vygotsky, L.S., (1978). *Mind in society: The development of higher psychological processes*. Cambridge, MA: Harvard University Press.
- [47] Wang, Y., Teachers' design thinking of instructional design in higher education. In: *The Educational Review, USA*, Vol. 7, No. 12, 2023. DOI: 10.26855/er.2023.12.013
- [48] Walsh, R., The methods of reflexivity. In: *The Humanistic Psychologist*, Vol. 31, No. 4, 2003. DOI:10.1080/08873267.2003.9986934
- [49] Walwanis, M.M., Swanson, B.L., Wheeler Atkinson, B.F., (2013). The role of instructor operator stations in training. In G. Galanis, R. Sottolare, C. Best (Eds.), *Fundamental issues in defense training and simulation*. CRC Press.

Appendix 1 –TrEd ID Model (Hornstra et al., 2024b)

Phase	Activity
1) Focusing	a) Trainer/Educator getting attention b) Trainer/Educator providing learning objectives c) Trainer/Educator providing authentic problem to be solved
2) Getting ready	a) Trainer/Educator activating prior knowledge/skills/experiences b) Learners sharing initial skills/ideas a) Trainer/Educator showing content (e.g. demonstration, presentation)
3) Presenting	b) Learners comparing content with initial skills/ideas c) Learners complementing skills/ideas by experimenting and studying a) Trainer/Educator providing guidance (e.g. discussion, tools, checklists, job aids)
4) Practicing	b) Learners practicing skills/trying out solutions c) Trainer/Educator/Learners providing feedback a) Learners performing skills/solving problems in authentic environments
5) Getting real	b) Trainer/Educator/Learners assessing performance/problem solving c) Trainer/Educator/Learners reflecting on learning process and outcomes in relation to the learning objectives

Appendix 2 – Survey Officer cadets about their officer education

The survey contains 14 statements and 3 open-ended questions about your officer education. Please rate each of the following statements on a scale from 1 to 5, with (1) being not important at all and (5) being very important. Please answer each open-ended question. This survey takes a maximum of 15 minutes.

1. When a class starts, the teacher must get my attention first.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

2. At the beginning of a class, the teacher must tell me specifically what I must learn.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

3. At the beginning of a class, the teacher must show a real-life problem that I must learn to solve.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

4. When I learn something, the teacher must build on my existing skills and knowledge.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

5. Before learning something, the other officer cadets and I want to share among ourselves our existing skills and knowledge.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

6. The teacher must demonstrate or present to me what I must learn.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

7. I want to compare what I must learn on the one hand with my existing skills and knowledge on the other.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

8. I want to improve my skills and knowledge by experimenting and studying.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

9. The teacher must guide me when I am learning.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

10. I want to practice and try out solutions.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

11. I want to get feedback when I am practicing and trying out solutions.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

12. When learning, I want to apply my new skills and knowledge in a real-life environment.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

13. When learning, I need an assessment of my performance.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

14. At the end of a class, I want to reflect on the way I learned, and compare what I learned to what I should have learned.

(1) not important at all (2) not important (3) neutral (4) important (5) very important

15. What two aspects are most important to you in your officer education??

16. What two aspects do you appreciate most in your officer education??

17. What two aspects would you like to improve in your officer education??

Appendix 3 – Krueger and Casey’s (2009) Questioning route for focus group sessions, as applied in AMEE Guide No. 91 (Stalmeijer et al., 2014)

1) *Opening questions*

Facilitate early engagement in the discussion.

2) *Introductory questions*

Introduce the discussion topic and encourage participants to reflect on their personal connection to it.

3) *Transition questions*

Transfer the discussion towards the central questions that drive the study, thereby setting the stage for productive key questions.

4) *Key questions*

Discuss the key questions driving the study.

5) *Ending questions*

Conclude the discussion effectively.

Appendix 4 - Semi-structured interview guide

Opening questions (10 minutes)

- 1) Which subjects do you like?
- 2) Which subjects do you find difficult?

Introductory questions (15 minutes)

- 3) How do you feel about officer education in general?
- 4) How do you feel about educational methods in general?

Transition questions (15 minutes)

- 5) How would you describe your experiences with your officer education?
- 6) How would you describe your experiences with the educational methods of your officer education?

Key questions (45 minutes)

- 7) How do you experience the way you become focused at the beginning of a class?

Prompts: - Attention.

- Learning objectives.
- Authentic problems.

Points of attention from the survey

* *Opinions vary widely: When a class starts, the teacher has to get my attention first.*

- 8) How do you experience the way you are prepared to learn?

Prompts: - Prior knowledge/skills/experiences.

- Initial skills/ideas.

Points of attention from the survey

* *Not important: Before I learn anything, the other cadets and I should discuss what we already know and what we are already able to.*

- 9) How do you experience the way the content is presented to you?

Prompts: - Showing content.

- Comparing content with initial skills/ideas.
- Complementing skills/ideas by experimenting and studying.

- 10) How do you experience practicing the newly learned skills and knowledge?

Prompts: - Guidance.

- Practice of skills/trying out solutions.
- Feedback.

Points of attention from the survey

* *Not important / Opinions vary widely: The teacher should guide me when I learn.*

* *Important: I want to get feedback when I practice and try out solutions.*

11) How do you experience the transfer of the newly learned skills and knowledge from the educational setting to the real world?

Prompts: - Performance of skills/solving problems in authentic environments.

- Assessment of performance/problem solving.

- Reflection on learning process and outcomes in relation to the learning objectives.

Points of attention from the survey

* Not important: *Something I have learned needs to be assessed.*

* *In the top two of important things / In the top two of most valued things / In the top two of areas for improvement: The clear relationship between officer education and professional practice (Theory applied to practice, realistic / authentic education, preparation for professional practice, current affairs, field trips, emphasis on missions, relevance).*

12) How do you feel about the educational methods of your officer education?

Points of attention from the survey

* *In the top two of important things / In the top two of areas for improvement: Educational methods (Variation, diversity, effectiveness, efficiency, interaction, active learning, guidance, not too often and not too long lectures).*

13) How do you feel about the teachers (i.e. military trainers and academic educators) of your officer education?

Points of attention from the survey

* *In the top two of most valued things: Teachers (Good, accessible, passionate, committed, open attitude, interaction, military, experienced, close contact).*

Ending questions (5 minutes)

14) Is this summary of the discussion complete and correct?

15) Is there anything we should have talked about, but didn't?

THE MILITARY LEADER'S CHALLENGE: ACHIEVING THE BALANCE BETWEEN SUBORDINATES' PERSONAL VALUES AND ORGANIZATIONAL VALUES

Cristian DRAGOMIR

”Henri Coandă” Air Force Academy, Braşov, Romania

This article analyzes the fragility of the balance between the personal values of the members of the military organization and the institutional values promoted by the aforementioned organization. Starting from the premise that the operational efficiency and the cohesion of the unit depend largely on the harmony between these two value systems, the paper explores, starting from the clarification of the concepts of personal and organizational values, the risks that may be associated with the conflict between these two categories of values, as well as some strategies through which military leaders can prevent and manage the discrepancies that arise. The issue of the challenges faced by military leaders in managing conflicts between the two sets of values, as well as their impact on organizational performance, is also addressed. The paper is based on studies and sources published after 2015, relevant, one could say, for the current realities associated with military leadership.

Key words: *personal values, organizational values, leadership, conflict, balance of values.*

1. INTRODUCTION

The essence of any large organization, regardless of the field of activity to which it belongs, has its origins of functionality in a set of values, clearly defined that support the basic components of the organizational climate.

Referring to this aspect, from the point of view of human resources and in the spirit induced by this

material, the members of these organizations are not abstract entities, but individuals with their own set of values and personal beliefs. The key to achieving efficiency at the organizational level thus lies in achieving the balance between these two dimensions.

In the military environment, elements such as discipline, cohesion, efficiency and the ability

to react in critical situations oblige military leaders, but not only, to become key actors, capable of facilitating the harmonization of personal values with institutional ones, without compromising any of the aforementioned dimensions.

Contemporary military leadership is a complex and essential area within the national defense system. In a constantly changing environment, military leaders not only have to make rapid and effective strategic decisions, but they also have to manage a subtle but critical aspect: the balance between personal values and organizational values.

This binomial is often the source of moral and decision-making dilemmas, which equally influence cohesion, operational efficiency, and organizational climate. Thus, understanding how military leaders can intervene and align their own ethical beliefs and those of their subordinates within the value structure of the institution becomes a priority objective for effective leadership.

In this regard, to achieve this goal, ways will be explored in which military leaders can fulfill their role as vectors of institutional values without compromising their personal integrity and without endangering the unity and morale of the troops.

2. ELEMENTS RELATED TO PERSONAL VALUES AND ORGANIZATIONAL VALUES IN THE MILITARY ENVIRONMENT

2.1. Personal values

Personal values are part of human identity, conscious or unconscious, just like personality, will, motivation, attitudes (Pop, 2024). There are many types of personal values that reflect the fundamental principles of each individual and that profoundly shape their behaviors, choices and relationships. Among the most important are integrity, which involves honesty, respect for moral principles and coherence between what a person says and does, even when there is no audience or external constraint. Another essential value is empathy, the ability to understand and feel the emotions of others, which plays a crucial role in building harmonious relationships and a community based on mutual understanding and support. Freedom is also a central principle for those who value independence of thought and action, giving them the opportunity to build their lives according to their own choices. Authenticity, on the other hand, reflects a person's devotion to their

own identity and values, without succumbing to social pressures or conformity.

Each of these values contributes to creating a solid internal framework, providing a clear direction for decision-making and for managing personal and professional relationships. In essence, personal values represent the foundation of a life lived with meaning, integrity and satisfaction, being the pillars that define our identity and help us navigate the complexity of existence. The taxonomy of values is an extremely vast one and encompasses various approaches or relationships, with consonances in various domains: ethical, social, emotional, financial, spiritual, etc.

Moral values are those that guide an individual's perception of right and wrong, providing an ethical framework for making decisions and interacting with others. This is even though our moral compass does not always help us discern whether certain actions or people are right or wrong (Davidson and Thomas, 2020). However, they include principles such as fairness, justice, loyalty, and respect for truth. For example, a person who values fairness will avoid making decisions that may benefit themselves at the expense of others, and loyalty to

friends, family, or colleagues will lead to supportive and protective behavior toward them. These values are fundamental to building a life of integrity and earning the trust of others.

Social values play a central role in how people interact with each other and in building group relationships. They include tolerance, solidarity, respect for diversity, and the desire to contribute to the common good. For example, tolerance of the opinions and beliefs of others creates a climate of respect and understanding, while solidarity involves mutual support, especially in times of crisis or difficulty. These values are essential for the formation of harmonious, equitable communities capable of collaborating to achieve common goals.

Emotional values reflect aspects that influence emotional well-being and interpersonal relationships. Love, compassion, empathy, and gratitude are just a few of these. They help people develop deep relationships, based on trust and mutual respect. For example, empathy allows individuals to understand and connect with the emotions of those around them, which reduces conflict and promotes harmony. At the same time, gratitude contributes to a more positive

outlook on life, increasing the level of personal satisfaction.

Personal values related to individual development are those that support personal growth and fulfillment. Courage, self-discipline, perseverance, continuous learning, and creativity play an important role in achieving goals and overcoming challenges. For example, self-discipline allows a person to maintain focus on goals, even in the face of temptations or obstacles, and continuous learning contributes to the enrichment of knowledge and skills, allowing better adaptation to changes in society. These values encourage self-reflection and constant progress, helping the individual to reach his or her full potential.

Material-financial values are associated with the need for stability and security in everyday life. For some people, financial security and material success are important values, providing comfort, independence, and opportunities to fulfill their aspirations. For example, someone who values financial stability will be more careful in managing their resources and will make responsible decisions regarding savings and investments. While these values may seem more practical, they play a significant role in ensuring a balanced and financially stress-free life.

Spiritual values reflect an individual's connection to deeper dimensions of existence, whether through religion, spirituality, or the pursuit of a higher purpose. They include inner peace, wisdom, universal harmony, and transcendence of everyday problems. For those who value them, these values provide a deeper meaning to life and a guide in times of uncertainty or difficulty. For example, inner peace can help a person face life's challenges with calm and poise, and wisdom can provide a broader perspective on important decisions.

Last but not least, personal values are fundamental to a person's identity, contributing to a sense of authenticity and inner coherence. When individuals live in accordance with their values, they feel more secure and fulfilled. Values reflect who we are, what we want, and what we consider right or wrong, giving us purpose and direction in life. For example, a person who values personal growth will always seek to develop, learn, and improve their skills, thus contributing to an identity based on progress and self-fulfillment. Therefore, personal values are key to building a stable and satisfying identity that helps us navigate life's challenges and opportunities.

2.2. Organizational values

Organizational values are a central element of the identity of any institution. They reflect the fundamental principles and standards that guide the collective behavior of the members of that entity. These values, formalized and promoted by leadership, provide a common framework for decision-making and priority setting. In the military environment, for example, institutional values such as honor, discipline, and loyalty are essential for organizational cohesion and effectiveness.

The definition of institutional values varies depending on the context (Gehman et al., 2013), but in general they are described as sets of principles and standards that define acceptable and expected behaviors in an organization. “*Our company is driven by values*” is the statement made by the CEO of a large organization in a context that reinforces the general belief that any company is driven by values based on external natural laws (Covey, 2017).

In understanding these concepts, we could consider three main elements or aspects: their status, character and scope. First, institutional values are formal. They are usually documented in the

organization’s mission and vision or in codes of ethics. In military institutions, for example, values such as “*integrity first, service before self and excellence in all we do*” are explicitly formulated and communicated to the organization’s members (AFDP 1, 2021).

Second, institutional values are imposed by leadership. They are promoted through organizational policies, procedures, and practices. When organizational values are imposed from the top, it is important that they are about development and, especially, about encouraging people to take responsibility for themselves and for those around them (Owen et al., 2006).

In modern armies, these values are transmitted through rigorous training and the personal example of leaders. To support this idea, I will refer to Sinek, who, through neurochemistry, explains the role of hormones, such as oxytocin and serotonin, in strengthening social bonds and trust between team members. These chemicals contribute to creating a sense of belonging and loyalty, essential for the effective functioning of teams, especially in high-risk environments, such as the military (Sinek, 2022).

Third, institutional values are collective, meaning they guide

the behavior of the group, not just individuals. This is crucial in environments where cooperation and coordination are essential, such as in military theaters. Shared values ensure team cohesion and reduce internal conflict.

Establishing institutional values is a strategic process that involves analyzing organizational objectives and consulting with stakeholders, by appealing to the organizational mission and vision, which serve, in this context, as pillars of the institution's identity. In other words, the process of phasing involves, first of all, the identification by the organization's management of the values that are essential for achieving strategic objectives. Then, these values are communicated to the organization's members through various means, such as courses, internal regulations or events on this topic. In the military environment, for example, the process of integrating values begins from the first days of training, when new recruits, in military institutions of higher education or continuing education, are educated in the spirit of institutional discipline and principles.

A clear example of defining values is that of the United States Army, where the fundamental values include loyalty, duty, altruism,

respect, honor, and personal service (ADP 6-22, 2019). These have a formal character, given by official documents, and are promoted through training programs and leadership initiatives (America's Air Force: A profession of arms, The little blue book, 2015).

3. CONFLICT SITUATIONS THAT ENDANGER THE BALANCE OF VALUES AND THEIR HARMONIZATION

3.1. Conflict of values

The conflict between personal and institutional values is a complex issue that often occurs in organizational settings. Personal values are the fundamental beliefs of an individual that guide their behavior and choices. Institutional values, on the other hand, are the principles promoted by an organization to achieve its goals. When these values conflict, tensions arise that can affect both the individual and the organization.

The conflict situation, as we imagined and represented in Fig. 1, can be analyzed and explained through four situations. The first of these is when the individual does not find himself at all in the sphere of influence of the organizational culture, which translates into a total lack of congruence between the

organization's values and personal values.

The second situation is that of the intersection of the two spheres of influence, in which case, from the point of view of leadership efficiency, we are moving towards a possible communion.

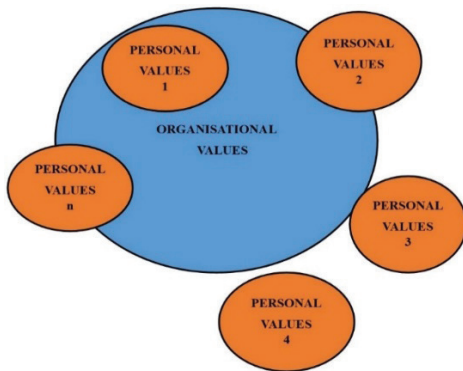


Fig. 1 Personal values vs organizational values
Source: Author's interpretation

Last, but not least, is the case where personal values are found entirely within the organizational ones, a situation that, from a conflict point of view, is not justified to analyze. A challenge is represented by the tangential situation of the two sets of values, a situation that can be considered a buffer, rather preferable, to the first situation.

Situations where employees' personal values conflict with institutional values are common in various fields, but are particularly

salient in military institutions. A common example is the case of an officer who prioritizes time spent with his family, but who is asked to participate in extended and demanding missions. This situation creates an internal conflict in which personal values, such as family responsibility, conflict with institutional requirements, which impose absolute loyalty to the mission (Sinek, 2022). Long periods of time away from family can lead to feelings of guilt and chronic stress.

Another example occurs when a soldier refuses to follow orders that he or she considers unethical, such as using tactics that go against humanitarian principles. These situations highlight the tensions between personal ethics and organizational politics (Covey, 2016). For example, in modern armed conflicts, soldiers may be forced to make difficult decisions, such as choosing between following orders and protecting civilians, aspect which are strictly regulated by the rules of engagement.

The causes of conflict between personal and institutional values are varied and determined by several factors. First, differences in priorities between the individual and the institution are a frequent source of tension. Military institutions, for example, are oriented towards

achieving strategic objectives, such as national security and mission execution, without always taking into account the personal needs of soldiers. This discrepancy becomes especially evident in times of war or crisis, when operational requirements are particularly stringent.

From the perspective of the effects produced by the conflict situation, it can be stated that the consequences can be felt on two levels: at the personal level and at the organizational level. At the individual level, such conflicts can lead to severe stress, anxiety and other mental health problems. A relevant example is the case of soldiers who face burnout syndrome or post-traumatic stress disorder as a result of a prolonged conflict of values (Mărineanu et al., 2022).

The feeling of helplessness and the lack of alignment between personal values and the requirements of the institution can lead to an unhappy ending characterized by demotivation and, why not, in extreme situations, even the desire to leave the organization.

At the institutional level, the consequences can be just as serious. A decrease in productivity and an increased rate of resignations are common problems in organizations that do not take into account the

personal values of employees. In the military environment, this can have a direct impact on operational efficiency. For example, a military unit with demotivated soldiers or who do not feel their values are respected may have difficulty maintaining cohesion and morale. In the long term, a lack of empathy and understanding on the part of leaders can lead to wider consequences, such as the erosion of trust in the institution, affecting its stability.

An important aspect is moral and professional education. In modern armies, the introduction of ethics and leadership courses can help soldiers better understand institutional values and find ways to integrate them, along with their own beliefs. Leadership communication, in particular, plays a crucial role in shaping organizational culture and values, impacting employees' commitment to organizational goals (Kimani, 2023).

Conflict between personal and institutional values is inevitable in some contexts, but it can be effectively managed by creating an organizational environment based on mutual respect. To do this, authentic leaders “*create a work environment in which people are respected for their contributions....*” (George et al., 2019). In the military environment,

this approach to authenticity is essential for maintaining morale and operational efficiency. By aligning personal and institutional values, stronger working relationships can be built, characterized by loyalty and performance.

3.2. Harmonization of values

Aligning personal and institutional values is a major challenge in contemporary organizations and one of the key solutions is to embrace open communication and compromise. Open communication allows employees to freely express their values, concerns, and priorities. Through active dialogue, leaders can identify commonalities between organizational and individual values. At first glance, this may seem contradictory to what was stated earlier, when we referred to the nature of the process of establishing organizational values. However, the self-regulating function of organizational management, which leads to an update and possible alignment of the two categories of values, should not be overlooked.

As mentioned above, compromise plays a key role in reconciling values. For example, employers can adjust policies and procedures to accommodate

employees' personal values without compromising organizational goals. This process requires flexibility on the part of both parties, as well as a willingness to work together to achieve a sustainable balance.

Another important element in such reconciliation is the adoption of flexible institutional policies that support diversity and inclusion. Flexible working hours, for example, offer employees the opportunity to organize their time according to their personal needs, which leads to increased satisfaction and productivity. A recent study shows that flexible working hours lead to a feeling of appreciation from employees, which will ultimately result in increased loyalty to the organization (Wheatley, 2017). Inclusion policies, in turn, promote an environment in which each individual feels respected and valued, regardless of cultural, ethnic or religious affiliation.

Leaders play a crucial role in promoting harmony between personal and institutional values. They can inspire respect for organizational values through personal example and by cultivating a work environment based on respect and collaboration. An authentic leader is one who understands the needs of employees and provides

them with support to integrate personal values into the professional context. The leader must be a moral model for subordinates and in this way the values of the organization will be transferred through consistent behaviors (SMG 46, 2006). In other words, employees are more likely to adopt organizational values if they see that their leaders live and respect them.

Another way leaders can support value alignment is by adopting a transformational leadership style that emphasizes employee personal development and a sense of shared purpose. This approach not only improves employee-organization relationships, but also contributes to increased performance and job satisfaction (Northouse, 2019). In this regard, leaders can use creative methods to generate ideas to identify shared solutions to organizational problems, actively involving employees in decision-making. Also, by recognizing and rewarding personal values that align with those of the organization, leaders can foster a sense of belonging and increased motivation.

A healthy organizational culture is essential for reconciling personal and institutional values. It is based on principles such as mutual respect, transparency, and mutual support. Organizations that promote work-

life balance provide a concrete example of how employees' personal values can be integrated into organizational values.

4. CONCLUSIONS

In the military environment, personal and institutional values are particularly important, and their harmonization is essential for maintaining a climate of discipline, efficiency and cohesion among the armed forces. The personal values of the military are fundamental to their behaviors and decisions in the face of daily challenges.

In parallel, institutional values, such as strict discipline, integrity, responsibility and duty to the country, define the structure and functioning of the army. When these values are in harmony, trust between the military and the institution is strengthened, and the military organization can act effectively, in accordance with a deep sense of mission accomplished and institutional belonging.

Harmonizing personal values with institutional values therefore represents a serious challenge for all military leaders, regardless of their echelon, representing an action whose success contributes to the formation of a united military body, capable of successfully responding to the nation's security and defense

requirements, while ensuring respect for the rights and dignity of each individual within the military system.

The issue of leaders harmonizing personal and organizational values is a very vast one and exceeds the scope of this article. In this sense, however, I could state that many other research directions can be opened on the balance of the presented binomial, with much broader connotations and implications for military leadership.

REFERENCES

- [1] Pop, D., “*Valorile personale modele validate*”, Baia Mare, 2024, Available at https://www.researchgate.net/publication/384109065_Valorile_personale_modele_validate (Accessed: 02 June 2025);
- [2] Davidson, F., Hughes, T., “*Moral Dimensions of Leadership*”, Oxford Research Encyclopedia of Education, February 28, 2020, Available at <https://www.researchgate.net/publication/> (Accessed: 02 June 2025);
- [3] Covey, S., “*Cele 12 pârghii ale succesului*”, Ed. ALLFA, București, 2017;
- [4] Gehman, J., Treviño, L. K., Garud, R., “*The Value of Values for Institutional Analysis*”, Academy of Management Annals, 7(1), 2013, pp. 283–317, Available at <https://journals.aom.org/doi/epub/10.5465/annals.2018.0074> (Accessed: 02 June 2025);
- [5] Owen, H., Hodgson, V., Gazzard, N., “*Manual de leadership – Ghid practic pentru un leadership eficient*”, Ed. CODECS, București, 2006;
- [6] Air Force Doctrine Publication 1, *The Air Force*, March 2021, Available at https://www.doctrine.af.mil/Portals/61/documents/AFDP_1/AFDP-1.pdf (Accessed: 02 June 2025);
- [7] Sinek, S., “*Liderii mănâncă ultimii: De ce unele echipe lucrează bine împreună, iar altele nu*”, Ed. Publica, 2022;
- [8] ADP 6-22, “*Army leadership and the profession*”, Headquarters, Department of the Army, July 2019, Available at https://talent.army.mil/wp-content/uploads/2020/11/ARN20039_AD6-22-C1-FINAL-WEB.pdf (Accessed: 02 June 2025);
- [9] America’s Air Force: A profession of arms, “*The little blue book*”, July 2015, Available at https://www.airman.af.mil/Portals/17/001%20Home%20Page/005_The_Little_Blue_Book/Profession%20of%20Arms_Final_For%20Screen.pdf?ver=2015-08-21-135633-620 (Accessed: 02 June 2025);
- [10] Covey, S., “*Cele 7 deprinderi ale persoanelor eficiente*”, Ed. ALLFA,

- București, 2016;
- [11] Mărineanu, V., “*Ghid de pregătire psihologică a liderilor militari*”, editura Centrului Tehnic Editorial al Armatei, București, 2022;
- [12] Kimani, B., “*Internal Communication Strategies and Employee Engagement*”, Journal of Public Relations, Vol.2, Issue No.1, pp.13 – 24, 2023, Available at <https://www.researchgate.net/publication/> (Accessed: 02 June 2025);
- [13] George, B., Ibarra, H., Goffee, R., Jones, G., “*Authentic Leadership*” (HBR Emotional Intelligence Series), Harvard Business Review, București, Ed. Libra, 2019;
- [14] Wheatley, D., “*Employee satisfaction and use of flexible working arrangements*”, Work, employment and society, Vol. 31(4), pp. 567–585, 2017, Available at <https://www.researchgate.net/publication/> (Accessed: 02 June 2025);
- [15] SMG 46, “*Codul de conduită etică a militarului român*”, 2006;
- [16] Northouse, P. G., “*Leadership: Theory and Practice*” (8th Edition), Thousand Oaks, CA: Sage Publications, 2019.

MOTIVATION, COMPETENCE, AND ADAPTABILITY: LEVERAGING CIVILIAN-MILITARY TALENT SYNERGY AS UKRAINE'S STRATEGIC HUMAN RESOURCE ADVANTAGE

Arsen BIEKIROV

Ministry of Defense of Ukraine

Ukraine's experience in defense human resource management during times of crisis underscores the strategic importance of aligning talent with tasks rather than focusing solely on numbers. The effective mobilization of educated, experienced civilians into leadership roles within the armed forces has significantly enhanced Ukraine's resilience and operational effectiveness. While civilian specialists have not wholly replaced military leaders, their integration has acted as essential lubrication for the complex machinery of the defense system, increasing efficiency and reducing obstacles. Institutionalizing this hybrid model, supported by targeted training, inclusive leadership doctrines, and clear policies recognizing civilian contributions, offers a paradigm for contemporary and future security challenges. As warfare becomes more hybrid and multidimensional, Ukraine's model illustrates that adaptability, diverse skillsets, and intelligent human resource management can be decisive factors in military success. The combined motivation, advanced leadership, and entrepreneurial spirit of civilian specialists, when strategically integrated, have become core elements of Ukraine's defense resilience and a source of international admiration. This study contributes a key lesson for nations navigating modern defense personnel challenges in volatile security environments.

Key words: *Civilian-military integration, defense human resource management, hybrid warfare, talent management, crisis mobilization, strategic leadership, adaptability, Ukraine defense forces, military resilience, security workforce development.*

1. INTRODUCTION

In the field of Human Resources Management, especially within the realm of Defense Resource Management, the principle of assigning the right people to the right positions at the right time remains a cornerstone of organizational efficiency and national security. This becomes increasingly relevant during periods of heightened threat or conflict, when effective human resource deployment may determine not only operational success but the survival of the state.

In February 2022, Ukraine was subjected to an unprovoked, full-scale military invasion by the Russian Federation, whose armed forces significantly outnumbered Ukraine's Defense Forces in both manpower and equipment. This numerical superiority played a crucial role in the initial success of the invasion, which advanced from seven different directions. As a result,

Ukraine suffered the rapid loss of extensive territories in the early days of the conflict. In an effort to support the embattled Ukrainian military, ordinary civilians - professionals from various sectors - rushed to assist. The world watched in awe as footage circulated globally, showing Ukrainian authorities handing out Kalashnikov rifles to anyone willing to defend their country. What emerged was a hybrid defense force - composed of traditional military personnel and highly educated civilians - whose synergy proved vital to Ukraine's resilience.

2. THE CHALLENGE OF WAR: THE CASE OF UKRAINE

With the start of Russia's full-scale invasion of Ukraine in February 2022, the Ukrainian Armed Forces (UAF) experienced an unprecedented demand for manpower. The mobilization of hundreds of thousands of individuals



Fig. 1 Growth of AFU personnel (2021-2025). The figures given based on the President Zelensky's claim, including several open sources data. [1]

became necessary to counter the aggression. As the numbers of servicemen and women grew, so too did the size and complexity of the military's structural units and command apparatus. However, the rapid scaling of the armed forces exposed a significant shortfall: a shortage of qualified officers and administrative personnel capable of effectively managing the growing military infrastructure.

Unlike enlisted personnel, senior officers cannot be trained or promoted in a matter of weeks or even months. Years of education, experience, and leadership development are typically required to produce competent military commanders. This created a critical gap in the operational capabilities of the entire Defense Forces of Ukraine.

3. UKRAINE'S HYBRID SOLUTION

To mitigate the shortage, Ukraine turned to an unconventional yet effective solution: integrating highly educated civilian professionals into military roles. These included top managers, project managers, IT specialists, logistics professionals, and administrative experts - individuals with strong leadership backgrounds and social influence but no prior military experience. These professionals, whom we may refer to as "hybrids," brought to the Armed Forces a fresh perspective, modern management skills, and agile problem-solving capabilities.

It would be counterproductive to employ a corporate executive or a highly qualified specialist as an enlisted soldier, especially during a strategic shortage of command personnel. Instead, these individuals were given a chance to be positioned within newly created Departments and Directorates for logistics, procurement, analytics, communication and technological support units, as well as cyber security, where their experience could yield the highest benefit.

4. THE LEGAL AND STRATEGIC FRAMEWORK

Recognizing this, President Volodymyr Zelensky signed Decree No. 893/2024 [2], which allows mobilized individuals with a master's degree and at least 2 years of management experience in civilian life to be appointed to various positions, including the rank of colonel. With the simultaneous assignment of the officer rank.

"Our goal is to attract individuals with management experience to officer positions in the Armed Forces," emphasized Defense Minister Rustem Umerov. "The key factor for appointment to leadership positions should be practical management skills, not merely years of service or ranks." [3]

"Many strong professionals have joined the army through mobilization. Previously, without military education, they could only hold enlisted positions. We must replenish the Army with professional

cadres and give talented managers all opportunities for development. The Army must be technological and modern", - added Deputy Minister of Defense for Digitalization Kateryna Chernohorenko. [4]

This highlights a critical imbalance that had existed before: the military, having finally gained access to highly qualified civilian professionals - previously out of reach in peacetime - was unable to fully capitalize on their potential. These individuals, often far exceeding the capabilities and experience of junior officers, were confined to enlisted roles. This not only stifled operational effectiveness but also created tension and conflict within the ranks. The army, having finally gained the resource it had long desired - highly skilled specialists - could not use them effectively due to regulatory barriers that placed them in subordinate positions. These talented professionals were expected to follow orders from

officers who, though trained, lacked the same level of practical leadership experience. This mismatch created friction that could no longer be ignored. Addressing this imbalance through legal reform was essential to maintaining morale, cohesion, and efficient command structures.

The decree provided a structured and lawful pathway for integrating civilian expertise into the military's command and administrative frameworks without undermining military discipline. Through this legal mechanism, the UAF significantly enhanced its capacity to address planning, operational, and logistical challenges.

5. COMPARATIVE ADVANTAGES AND NEW OPPORTUNITIES

To further explore the impact of this approach, we examine the qualitative distinctions between professional officers and hybrid officers in the table below.

Table 2 Human quality comparison between Career Officer and Hybrid Officer (based on the author's personal observations)

Criteria	Career Officer	Civilian
Military Experience	Extensive	Limited or none
Administrative Skills	Developed within military	Advanced in civilian sector
Adaptability	Moderate	High (due to cross-sector skills)
Flexibility	Limited due to discipline and subordination	More freedom in decision making

Criteria	Career Officer	Civilian
Initiative and Creativity	Constrained due to military regulations	Rewarded financially for both
Strategic Thinking	Military-focused	Multidimensional
Leadership Style	Command-centric	Team-oriented inclusive and innovative

As a result of hybrid approach Ukrainian Army received new human qualities, that has led to notable improvements in operational and strategic effectiveness across key areas:

1. *Military Technology and Systems* – Civilian experts have been instrumental in advancing Ukraine’s use of modern technologies such as Unmanned Systems and software tools for situational awareness on the battlefield like “Delta”, application for the artillerymen “Kropyva”, and SAP-based logistical accounting systems.

2. *Defense Procurement and Logistics* – based on the market experience civilian professionals introduced efficient procurement mechanisms and supply chain management, crucial for sustained operations.

3. *International Cooperation* – Hybrid officers, often fluent in multiple languages and experienced in communication, significantly strengthened Ukraine’s defense dialogue with Western partners, improving aid coordination and support for Ukraine.

This fusion of military discipline with civilian innovation has resulted in a more agile, versatile, and forward-looking defense force, capable of responding effectively to modern security challenges.

6. HISTORICAL CONTEXT AND NOVELTY

Historically, the integration of civilians into military operations has occurred during periods of total war. For instance, during World War II, the United States and the United Kingdom mobilized industrial managers, scientists, and engineers to support the war effort, especially in logistics, intelligence, and weapons development. However, these individuals typically worked in the civilian sector or as advisors and were rarely integrated directly into military command structures.

In the United States, in 1940 - 42, such top managers as William S. Knudsen (former head of General Motors) and Charles E. Wilson (future Secretary of Defense, then president of General Electric) were invited to join the government. Knudsen received a commission as

a lieutenant general and was put in charge of military production, but remained largely a superstructure over the army organization rather than commanding actual troops. [5]

The creation of the War Production Board (WPB) in 1942 is a prime example of the integration of civilian experts into the management of military-industrial power: the WPB coordinated production, material distribution, and resources between the Army, Navy, and industry, but did not exercise direct military control at the front. [6]

Ukraine's model is distinct in that it not only utilizes civilian expertise but does so by officially incorporating these individuals into the military hierarchy through formal ranks and responsibilities. This level of integration - during an active war - is relatively unprecedented and reflects a novel approach to defense management under crisis.

The strategic success of Ukraine's hybrid model may thus serve as a blueprint for modern conflict adaptation, where conventional military structures are insufficient to address complex hybrid warfare challenges.

7. A NEW PERSPECTIVE ON INTEGRATION

It is widely accepted that military veterans transitioning to civilian life often begin their second careers not at entry-level positions, but in senior,

well-compensated roles, thanks to their leadership experience and strategic outlook. This integration is not only normalized but encouraged by both the public and private sectors.

Following the same logic, the reverse integration - of seasoned civilian professionals into the military - should not provoke skepticism among career officers. These "hybrids" bring complementary skills to the defense sector, bridging gaps that traditional military education may not cover. This bilateral flow of expertise strengthens both spheres and provides a powerful argument in favor of flexible personnel policies during national emergencies.

8. CROSS-SECTOR COMPARISONS AND INSIGHTS

Let us compare both categories from another angle - how they perform across civilian and military domains. Retired military officers often transition into senior roles in the corporate or public sectors: security directors, emergency response coordinators, consultants in strategic planning. They rarely begin at the bottom; their leadership acumen places them into influential roles.

Now consider the reverse. When civilian experts - entrepreneurs, lawyers and even MP's, program directors, communication companies top managers, engineers - are

integrated into military structures, they bring a wealth of creativity and modern approaches, as well as attract the others. Historical examples show that revolutionary and guerrilla movements often drew their leadership not from military academies, but from civilians. Che Guevara, a trained physician, became one of the most iconic guerrilla leaders. Similarly, T. E. Lawrence ("Lawrence of Arabia"), a British archaeologist, played a crucial military role in the Arab Revolt during World War I. These examples underline that the ability to lead and adapt in combat does not reside solely with career soldiers.

By incorporating civilian leadership into military frameworks, Ukraine is harnessing this dual potential - aligning wartime necessity with peacetime ingenuity.

9. COMPETITION FOR HUMAN RESOURCES

The Armed Forces are in constant competition with the civilian sector for human resources. In most cases, the civilian market prevails, offering higher salaries and more flexible conditions. This problem is well known to military recruiters across developed countries, as they confront it daily. However, during wartime and general mobilization, the military gains a unique opportunity to attract a wide range of civilian professionals who are otherwise inaccessible in peacetime.

The effective and rational use of this resource necessitates a revision of certain doctrines and policies. Leadership must be open to adapting traditional regulations to new realities, where highly qualified civilian experts can play a key role in strengthening national defense.

As Carl von Clausewitz wrote, "The necessary knowledge for a high position in military action ... [is] to be gained by experience of life as well as by study and reflection... These are things the knowledge of which cannot be forced out by an apparatus of scientific formula and machinery: they are only to be gained by the exercise of an accurate judgment in the observation of things and of men, aided by a special talent for the apprehension of both." [7]

As a practical manifestation of these ideas, some of the most effective combat units in the Ukrainian Armed Forces today are led by individuals without formal military education who joined the military after Russia's full-scale aggression. Several of them have been awarded the title of Hero of Ukraine for being most effective on the battlefield.

10. CONCLUSION AND FUTURE PROSPECTS

Ukraine's experience offers a valuable lesson in defense Human Resource Management: in times of crisis, it is not only numbers that matter, but the strategic alignment of

talent to tasks. The mobilization of educated, experienced civilians into leadership roles within the military has contributed substantially to Ukraine's resilience and operational effectiveness. Although civilian specialists did not fully replace military leaders, they became the vital oil that kept the gears of the Armed Forces running smoothly with fewer obstacles and more effectively.

The institutionalization of this hybrid integration model could serve as a paradigm for nations navigating complex security environments in the 21st century. For this to be successful, it must be accompanied by targeted training programs, inclusive leadership doctrines, and clear policies that recognize the added value of civilian input within military structures.

As global warfare becomes increasingly hybrid and multidimensional, the success of Ukraine's model illustrates a key maxim for the future: adaptability, diversity in skillsets, and intelligent HR management may outweigh sheer numbers or traditional hierarchies in determining victory.

The motivation, experience, talents, adaptability, entrepreneurial spirit, and advanced leadership qualities of mobilized civilian specialists - when wisely and strategically integrated into the

structure of Ukraine's Defense Forces - have become one of the decisive factors behind the country's resilience. This synergy has not only become a source of national pride for the Ukrainian people but also earned admiration from international allies, who recognize in Ukraine a model of modern, adaptive warfare that meets the demands of the 21st century.

REFERENCES

- [1] The Kyiv Independent, *Ukraine's military now totals 880,000 soldiers, facing 600,000 Russian troops, Zelensky says*, 15 January 2025.
- [2] Presidential Decree of Ukraine №893/2024, *On Amendments to the Regulations on Military Service by Citizens of Ukraine in the Armed Forces of Ukraine*, December 31, 2024.
- [3] Ministry of Defense of Ukraine, *Official Statement by Defense Minister Rustem Umerov*, Ministry Website, 2 January 2025.
- [4] Chernohorenko, Kateryna, *Comment on integration of civilian professionals*, Deputy minister's Chernohorenko Official FB account, 31 December 2024.
- [5] Wikipedia, William S. Knudsen / Charles E. Wilson
- [6] Wikipedia, War Production Board
- [7] Carl von Clausewitz, *On War*, Book II, Chapter 2 ("On the Theory of War"), 1832.

PRINCIPLES-BASED LEADERSHIP AND ITS IMPACT ON MILITARY ORGANIZATION EFFECTIVENESS

Cristian DRAGOMIR*, Lucia BOROTA**

**"Henri Coandă" Air Force Academy, Braşov, Romania

**Romanian Air Force, Bacau, Romania

This paper explores the significance of principles-based leadership in the military organization, emphasizing its strategic role and impact on organizational effectiveness. The study analyzes key components of military leadership, such as responsibility, influence, and vision, and underscores the importance of coherence between ethical values and operational decisions. Furthermore, the paper discusses the main factors that influence leadership efficiency and identifies major challenges that military leaders face in today's complex security environment. Additionally, the paper includes a practical guide for developing character and principled leadership, offering concrete strategies for military leaders. The findings highlight the relevance of a principled approach as a foundation for sustainable and effective leadership in the armed forces.

Key words: leadership, efficiency, decision-making, military, principles, discipline.

1. INTRODUCTION

Leadership in the military is more than a matter of hierarchy or formal authority, it is a complex process grounded in responsibility, ethical judgment, and strategic vision. In an environment characterized by unpredictability, discipline, and high operational demands, the presence of principled leadership becomes not just desirable, but essential. Leaders must operate under significant

pressure, make decisions with far-reaching consequences, and maintain the cohesion and morale of their teams, often in high-stakes situations.

This paper explores the role of principles in shaping effective military leadership, examining both the foundational elements and the challenges leaders face in contemporary military settings. By analyzing the impact of values such as integrity, responsibility, and professionalism, the study aims to

highlight how principled leadership enhances decision-making, fosters trust, and contributes to institutional resilience.

In addition to the theoretical analysis, the paper includes a practical guide to developing character and ethical conduct, focusing on actionable steps that leaders can take to enhance their influence, adaptability, and moral authority. By integrating both conceptual and applied perspectives, the study aims to offer a comprehensive view of how principle-based leadership can serve as a pillar of operational success and institutional trust.

2. SHORT HISTORY ON DEFINING LEADERSHIP IN THE SPECIALIZED LITERATURE

Because the term leadership is so commonly used or misunderstood, it is important to begin by defining what it means. Unfortunately, the use of the term leader has been popularly expanded to include almost anyone, whether in the upper management of an organization or in a politically occupied position [1].

There are many ways to complete the sentence: “Leadership is . . .”. In fact, as Ralph M. Stogdill, one of the leading theorists of this phenomenon, pointed out in a research journal dedicated to leadership, there are almost as many different definitions of leadership as there are researchers

who have tried to characterize it [2]. It can be likened to defining the words democracy, love, or peace. Although each of us intuitively knows what we mean by such words, they can have distinct meanings for different people.

The large number of definitions issued for this field suggests that, despite decades of research conducted in this regard, finding a common definition for the term “leadership” has proven to be very difficult. However, each of the definitions provides certain elements of what the term leadership means and tends to describe certain qualities of the leader. For the sake of illustration, we will reproduce below some of the representative definitions of leadership and we will try to reach a consensus on what leadership entails, based on the comparison of key constitutive elements.

Stogdill, in the same research journal above mentioned, defines leadership as “*an interaction between members of a group. Leaders are agents of change, people whose actions affect other people more than their actions affect them. Leadership occurs when a group member changes the motivation or skills of other members of the group*”.

Gibson, Ivancevich and Donnelly define leadership as the process by which an individual influences the behavior of others to achieve the proposed objectives

without exercising any form of coercive influence. According to them, leadership is “an attempt to use non-coercive influence in motivating individuals to achieve the same objective” [3].

A third definition that we present is that described in the Meriam-Webster Dictionary, in which leadership is defined as “the position or orientation of a leader or the ability to lead the members of a group” [4].

Another interesting definition of leaders and leadership can be found in a paper written by Jennifer M. George and Gareth R. Jones, where leadership is defined as “the influence exerted by one member of a group or organization on other members in order to achieve its common objective”[5].

Despite the multitude of ways in which leadership has been conceptualized, the following components can be identified as central elements of the phenomenon (Fig. 1.):

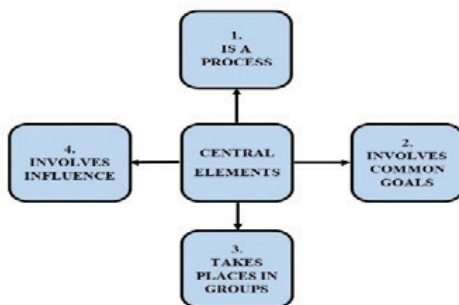


Fig. 1. Central elements of leadership

Based on the components illustrated in the figure above, the following definition of leadership could be formulated: “Leadership is a process by which a single individual influences a group of people to achieve a common goal” [6].

Defining leadership as a process means that it is not a trait or characteristic that resides in the leader, but rather can be seen as a transactional event that occurs between the leader and followers. The process implies that a leader's actions will affect others but that the leader, in turn, will be affected by followers.

Leadership involves focusing on shared goals. Leaders direct their energies toward individuals and, in doing so, try to accomplish something together. Shared means that leaders and followers have a mutual purpose.

Groups are the context in which leadership manifests itself. It involves influencing a group of individuals who have a common purpose, which can be expressed either through a small task group, a community group, or a large group that encompasses an entire organization.

According to Wright, leadership theories are important because they help to outline different points of view and delimit various ideas. Bergman is the one who states that the multitude of theories provides the foundation upon which specifications for leadership competencies can be

built. The main research studies refer to the characteristics of the leader, the situations in which leaders operate, the behaviors and skills that leaders use, the perceptions of followers and combinations of these, as well as other factors.

3. INCREASING EFFICIENCY AND MANAGING CHALLENGES AS STRATEGIC GOALS IN MILITARY LEADERSHIP

Leadership based on principles implies the conscious adoption of a set of values and moral standards that consistently guide a leader's decisions and actions [7]. In the military environment, these principles take on a special significance, as they lie at the intersection of personal ethics, institutional discipline, and strategic imperatives. Exercising leadership in such a context requires more than formal authority, it demands moral credibility, strategic clarity, and personal balance.

Leaders guided by strong principle are not only defined by their hierarchical position, but by their ability to positively influence behaviors, foster initiative, and cultivate a climate of trust. Their legitimacy is reinforced by the alignment between what they say and what they do, especially in situations marked by uncertainty or adversity. These leaders become true models of conduct, offering stability and

moral direction to those under their command.

Military leadership is structured around a set of traits and competencies aimed at influencing, taking responsibility, and directing the team towards institutional objectives. Influence is based on trust and consistency, responsibility reflects the leader's ability to manage resources effectively, and vision provides unity and purpose. In all these dimensions, moral and professional principles represent the core anchor of military leadership.

From a strategic perspective, principles are not abstract ideals, but practical tools for navigating complexity and pressure. They provide the leaders with a framework for consistent and ethically grounded decision-making, reinforcing institutional cohesion and enhancing organizational performance.

Leadership, as previously presented, is commonly defined as the process of influencing, motivating, and guiding personnel toward mission accomplishment in ways that enhance efficiency and minimize risk [8]. At tactical and operational levels, leaders must develop personal qualities and operational competencies that allow them to effectively command troops [9]. These leaders are expected to act in accordance with a core set of values such as honor, integrity, loyalty, and courage, serving as behavioral

benchmarks and directly impact group cohesion and operational effectiveness.

On the other hand, strategic level leadership assumes that individuals have already proven themselves through all previous stages of command and now possess the advanced capabilities required to manage military institutions. These leaders are responsible not only for strategic vision and institutional performance, but also for identifying and mentoring future officers with the potential to serve in higher command positions.

Modern military leadership is increasingly confronted with a complex and dynamic environment, demanding leaders to demonstrate not only strategic vision, but also operational efficiency. The ability to achieve results with limited resources, under pressure and in uncertain contexts, becomes a decisive factor for success. Therefore, analyzing the variables that influence leadership effectiveness, along with identifying and addressing the challenges encountered by military leaders, is essential for strengthening institutional performance and resilience.

Leadership efficiency in a military context is closely linked to both the professional competence of leaders and their capacity to build trust and motivate subordinates [10]. The application of principled

leadership, based on integrity, responsibility, and fairness, cultivates discipline and operational cohesion. In addition, efficiency is shaped by the leader's ability to adapt quickly, communicate clearly, and maintain a high level of decision-making quality under pressure.

Another important determinant is the alignment of personal leadership style with the organizational culture and the nature of the mission [11]. Leaders who can calibrate their actions in accordance with the situational demands, while remaining anchored in a solid value system, tend to perform better. Furthermore, emotional intelligence and interpersonal skills contribute significantly to team performance, particularly in stressful or conflictual scenarios.

Military leaders face multiple challenges, from the management of intercultural teams to the need to integrate new technologies and deal with hybrid threats. One major challenge is the growing complexity of military operations, often requiring joint action with other institutions or even multinational forces, which necessitates enhanced coordination skills and strategic diplomacy [12]. Moreover, generational differences and the changing expectations of young military personnel may cause friction within hierarchical structures, thus requiring a flexible and inclusive leadership approach. Leaders

must also navigate bureaucratic inertia, ethical dilemmas, and the psychological impact of long deployments, all while maintaining the operational effectiveness of their units [13].

4. DEVELOPING CHARACTER AND PRINCIPLES-BASED LEADERSHIP IN THE MILITARY ORGANIZATION: A PRACTICAL GUIDE

The path to principle-based leadership in the military is not accidental—it must be intentionally cultivated through sustained character development, education, and practical application.

Effective leadership begins with knowing oneself, therefore by embracing self-reflection and self-discipline, leaders are able to regularly reflect on their values, motivations, and behavior. Keeping a personal leadership journal or seeking honest feedback from peers and subordinates can enhance self-awareness. Practicing self-discipline in small, everyday decisions builds the foundation for ethical behavior in stressful environments.

Leading by example in a consistently way is much needed because principle-based leadership is credible only when leaders align their words with their actions. Every decision, gesture, and attitude sends a message. Maintaining consistency between stated values and operational

conduct reinforces trust and inspires others to uphold the same standards. Military leadership is not limited to issuing orders, it also requires the ability to influence behavior and motivate personnel.

A military leader's influence is built on three key factors: formal authority, professional competence, and personal charisma [14]. While authority stems from the hierarchical position held, competence and charisma are developed and, in some cases, earned over time. These are essential for maintaining effective relationships with subordinates. Although respect can be enforced through rank and institutional status, the ideal is for it to be earned. True respect arises when leaders inspire their teams through personal example and the manner in which they face and manage challenges both personal and organizational. By demonstrating calm, fairness, and resilience, leaders become role models, capable of motivating and guiding their units not through fear, but through authentic leadership.

In an age of growing immorality, promoting ethical decision-making becomes essential. Military leaders must be trained not only to make fast decisions, but also to make the right ones under pressure. Case-based discussions, moral dilemma simulations, and open dialogues about ethical challenges should be embedded in leadership development

programs. Encouraging the question "*What is the right thing to do?*" must become part of the organizational culture.

Responsibility and accountability are core pillars of principled leadership in the military. In environments where decisions carry serious consequences, the ability to take ownership of actions, outcomes, and even failures is what distinguishes a leader from a mere functionary.

At the individual level, leaders must set the tone by assuming full responsibility for their decisions and for the performance of their teams. This includes recognizing mistakes, correcting course without shifting blame, and treating failure as an opportunity for growth.

At the organizational level, a culture of accountability is built by ensuring that expectations are clearly defined and communicated, that feedback is ongoing and constructive, and that ethical breaches or incompetence are addressed transparently and consistently. A responsible culture avoids both micromanagement and authoritarianism, it empowers personnel to act autonomously within well described parameters, while also reinforcing the understanding that freedom of action comes with a duty to justify one's choices.

Institutionally, the military must support accountability

not only through disciplinary systems, but also by fostering psychological safety and ethical mentorship. Leaders should create an environment where subordinates feel safe to admit mistakes, ask questions, and take initiative without fear of disproportionate punishment or reputational harm. In such an environment, accountability is no longer synonymous with fear, but with professionalism and integrity.

I would also like to mention empathy and emotional intelligence which are often underestimated in military leadership, yet they are essential for building cohesion, trust, and resilience. In environments with a high level of pressure and stress, emotionally intelligent leaders are able to de-escalate tension, communicate effectively, and offer support without compromising discipline or standards. In order to developing emotional intelligence, it requires intentional effort through self-reflection, feedback, and training focused on interpersonal skills. Empathy does not mean weakness; it reflects the strength to listen actively, understand diverse perspectives, and make balanced decisions that consider both mission success and human impact. Leaders who demonstrate empathy foster loyalty and openness, making their teams more adaptable and committed. In modern military contexts, where complexity and human factors

are deeply intertwined, emotional intelligence is not optional, it is strategic.

Military leadership requires ongoing development grounded in three key pillars: formal education, practical training and experience, and self-directed learning (Fig. 2).

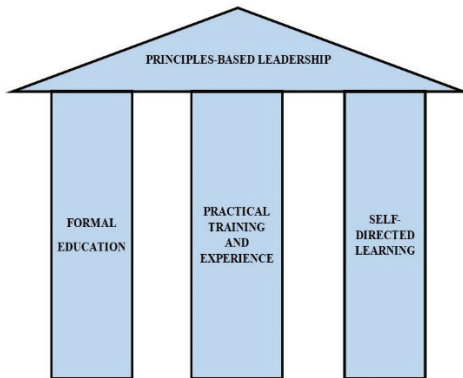


Fig. 2. The three pillars of principles-based leadership

These elements intertwine to create a leader who is not only tactically and strategically competent but also adaptable in fast-changing operational environments. In the Romanian Armed Forces, leadership development is structured through academic military education, foundational and advanced leadership courses. Beyond the classroom, participation in multinational exercises, NATO missions, and joint operations provides leaders with essential exposure to real-world challenges and collaborative decision-making.

Continuous learning enables leaders to think critically, respond

quickly, and act with precision in diverse scenarios [15]. It also prepares them to operate in international environments, where success depends on cross-cultural communication, language proficiency, negotiation skills, and an understanding of allied military cultures. Modern leaders must be multidisciplinary, innovative, and agile. In a world of hybrid threats and multinational coalitions, leadership excellence depends on a lifelong commitment to personal and professional growth.

CONCLUSIONS

Military leadership based on solid principles serves as a strategic advantage in a context marked by operational complexity and organizational pressures. Leaders who internalize and apply values consistently not only increase the effectiveness of their commands but also strengthen institutional trust and credibility.

The challenges faced by military leadership today require a balanced approach that combines discipline, adaptability, and emotional intelligence, all anchored in a clear values-based system.

The practical guide included in this study outlines the core elements necessary for building principles-based leadership, such as accountability, example-based influence, emotional intelligence, and

a commitment to lifelong learning. These recommendations are not abstract ideals but actionable paths toward more coherent, respected, and resilient leadership.

By cultivating character as intentionally as competence, modern military institutions can prepare leaders who are equipped not just to command, but to inspire, protect, and evolve alongside the ever-changing demands of defense and security.

REFERENCES

- [1] D. R., Kolzow, *Leading from within: building organizational leadership capacity*, Warner Books, 2014, Available at https://www.iedconline.org/clientuploads/downloads/edrp/leading_from_within.pdf, accessed on 25 Feb.2025;
- [2] R. M. Stogdill, *Handbook of leadership*, New York Free Press, 1974, Available at <https://archive.org/details/stogdillshandboo0000stog/page/n3/mode/2up>, accessed on 12 March.2025;
- [3] J. L. Gibson, J. M. Ivancevich, J. Jr. H. Donnelly, R. Konopaske, *Organizations: Behavior, Structure, Processes*, Irwin McGraw-Hill, 14th ed., Boston, 2011, Available at https://dl.motamem.org/organizations_behavior_structure.pdf, accessed on 12 March.2025;
- [4] <https://www.merriam-webster.com/dictionary/leadership>;
- [5] J. M. George, G. Jones, *Understanding and Managing Organizational Behavior*, Ediția 6, Upper Saddle River, NJ, Prentice Hall, 2012, Available at https://www.academia.edu/33133235/UNDERSTANDING_AND_MANAGING_ORGANIZATIONAL_BEHAVIOR_SHARED_BOOK_and_DOCUMENT_For_Educational_purposes_, accessed on 25 Feb.2025;
- [6] P. G. Northouse *Leadership: Theory and Practice*, 4th ed., Thousand Oaks, CA, Sage Publications, 2007, Available at https://www.academia.edu/30456341/Book_Leadership_Theory_and_Practice, accessed on 13 Feb.2025;
- [7] S.R. Covey, *Principle-Centered Leadership*, New York, RosettaBooks LLC, Electronic edition, 2009 Available at [https://ruduct.com/servant-1/Principle-Centered%20Leadership%20\(Stephen%20R.%20Covey,%20Stephen%20Covey\)2018.pdf](https://ruduct.com/servant-1/Principle-Centered%20Leadership%20(Stephen%20R.%20Covey,%20Stephen%20Covey)2018.pdf), accessed on 25 Feb. 2025;
- [8] C. Trocan, Scribd Inc., *Leadership-ul – preocupare constantă în armatele țărilor membre NATO și în Armata României*, 2015, Available at <https://www.scribd.com/>, accessed on 25 Feb. 2025;
- [9] C. Mostoflei, P. Dutu, *Liderul militar în România*, Ed. Universității Naționale de Apărare „Carol I”,

- București, 2007;
- [10] P. Dutu, *Leadership și management in armată*, Ed. Universității Naționale de Apărare „Carol I”, București, 2008;
- [11] R. Roberts, *Twelve Principles of Modern Military Leadership*, NCO Journal, Army University Press, May 2018, Available at <https://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2018/May/12-Principles-Part1/>, accessed on 10 March 2025;
- [12] C. Zisu, A. Mihalcea, *Leadershipul și liderii în era digitală*, Agenția Media a Armatei, 2019, Available at <https://presamil.ro/>, accessed on 12 March 2025;
- [13] Shivane, *Military Leadership Challenges: Navigating Complexities of 21st Century*, Centre for Joint Warfare Studies, 2023, Available at <https://cenjows.in/>, accessed on 11 March 2025;
- [14] A. Rizescu, *Socializarea profesională și comunicarea în organizația militară*, Army Academy, 2006, Available at https://www.armyacademy.ro/reviste/1_2006_ro/a4.pdf, accessed on 8 March 2025;
- [15] C. Buța, *Educarea liderilor – factor decisiv în conducerea eficientă a organizațiilor*, Gândirea militară românească, 2019, Available at <https://gmr.mapn.ro/>, accessed on 10 March 2025.

THE IMPACT OF DIGITAL LEADERSHIP IN THE AIRLINE INDUSTRY ON EMPLOYEE PERFORMANCE: AN EMPIRICAL STUDY

Salih AYGÜN, Ülkü UZUNÇARŞILI

Beykent University, İstanbul Türkiye

This study examines the effect of digital leadership on employee performance within the context of the airline industry. In today's rapidly evolving business environment, where digital transformation is accelerating, leaders' ability to utilize technology effectively, motivate employees, and strategically guide organizations toward their goals has become crucial. The aim of this research is to statistically test the impact of digital leadership on employee performance among airline industry employees. Data were collected through a survey from 450 participants working in the airline sector in Türkiye. Analyses were conducted using SPSS software, employing descriptive statistics, Pearson correlation, and simple linear regression tests. The findings reveal that digital leadership has a positive and significant effect on employee performance ($\beta = 0.111$, $p < 0.001$). The correlation coefficient between the two variables was found to be 0.214 and statistically significant ($p < 0.001$). These results indicate that managers with higher digital leadership levels have the potential to enhance employee performance. This research contributes to literature both theoretically and offers practical implications for management practices in the airline industry.

Key words: *Digital leadership, employee performance, airline industry, leadership, SPSS.*

1. INTRODUCTION

The digitalization process leads to radical changes in almost every aspect of the business world. In particular, the integration of technology into business processes has transformed the understanding of leadership and brought the concept

of digital leadership to the forefront. Digital leadership encompasses not only the ability to use technology, but also the competence to manage change, encourage innovation and improve employee performance. In this digital age, the ability of organizations to achieve sustainable

competitive advantage is largely directly proportional to the digital competencies of leaders.

Currently, it is recognized that countries have an intense interest in technology as the pioneer of progress and development (“Technology Pioneers,” 2009). Depending on technological developments, digital transformation is an inevitable reality for organizations. However, the business world is changing and developing rapidly. Based on this reality, a new understanding of leadership, digital leadership, has emerged. Digital leadership refers to the ability of visionary, sympathetic, agile, risk-taking and collaborative leaders to manage digital age organizations. Digital leaders must have the ability to understand technology, manage innovation, problem-solving and use digital tools.

Digital leadership is a multidimensional construct integrating technology use, strategic vision, innovation and people management. Digital leaders are expected to transform organizations by fostering innovation and change, thereby enhancing performance and efficiency.

With globalization and technological developments, businesses need to keep pace with digital transformation. Businesses that successfully use technology can

gain competitive advantage more quickly and cause other businesses to become digitalization targets. Businesses need leaders with competencies that make it easier for their staff to adapt to digitalization. In the age of digitalization, in highly competitive areas such as the airline industry, the role of leaders in shaping the sustainable success of businesses is increasing. The airline industry stands out as an area of high competition, rapid changes in customer expectations and intensive use of technology. Therefore, understanding the impact of digital leadership on employee performance in this sector is important both academically and practically. This study contributes to literature by statistically examining the relationship between digital leadership and employee performance and by offering practical implications for the airline sector.

2. LITERATURE REVIEW

2.1. Digital Leadership

Digital leadership is defined as the ability to adapt to technological developments emerging with Industry 4.0, manage change and encourage innovation. Büyükbeşe et al. (2022) it is of great importance to define scalable characteristics of it. In literature, an adequate measuring instrument is not available for assessing the perceptions regarding

digital leadership. This study is about digital leadership characteristics and aims to fill the mentioned research gap by developing a “Digital Leadership Scale” based on an empirical study conducted among 526 people working at different sectors in private and public enterprises in Turkey. After the data were collected, the scope and construct validity of the scale was tested using the statistical programs SPSS and AMOS. The internal consistency coefficient of the scale is .90. As a result of the exploratory and confirmatory factor analysis, the Digital Leadership Scale (DLS) associates digital leadership with elements such as visionary, agility, openness to collaboration, analytical thinking and innovation. Digital leaders optimize business processes, develop innovative solutions and motivate employees by using technology strategically.

Digital leadership has become a crucial element in tackling the complexities of today's business world, especially considering rapid technological advances and digital transformation. Successful digital leaders have a unique set of characteristics that enable them to guide their organizations through this dynamic environment. One of the key characteristics of successful digital leaders is their ability to think visionary. They are able to create and articulate a clear vision that not

only addresses current challenges but also anticipates future trends and opportunities. This strategic mindset enables them to envision how digital technologies can improve organizational performance and foster innovation (Klein, 2020).

In order to be successful in rapidly changing business environments, leaders need to be agile. It is important to be able to adapt to change quickly, adopt new technologies rapidly and act flexibly (Küsbeci & Uzunçarşılı, 2021). Leadership agility is a vital attribute in the digital age where organizations need to adapt quickly to changing environments and market demands. Agile leadership refers to the ability of leaders to respond quickly to changes by fostering a culture of flexibility and innovation in their teams. This leadership style emphasizes collaboration, continuous learning and the capacity to change strategies as needed. Research shows that agile leadership significantly improves organizational performance by promoting responsiveness and adaptability, which are critical in today's fast-paced business world (Khairy et al., 2023).

Rather than a purely technology-focused construct, digital leadership can be understood as a multidimensional leadership approach that integrates strategic vision, change management, and

people-oriented practices with the effective use of digital tools. Scholars link digital leadership to existing frameworks such as transformational leadership, e-leadership and agile leadership, emphasizing its role in fostering innovation, adaptability and collaborative cultures in organizations (Avolio et al., 2000; Banks et al., 2022; Zeike et al., 2019). This perspective moves beyond a simplistic view of digital leadership as merely “using and developing technology” and positions it as a leadership style that strategically leverages digital capabilities to create value, enhance employee motivation, and drive organizational change (Klein, 2020; Tigre et al., 2024). In the airline industry, where rapid technological advances and customer expectations coincide, this broader conceptualization helps explain why digital leadership a critical success factor is.

Digital leaders should be open to collaboration and encourage teamwork. It is important to be able to communicate effectively with people from different areas of expertise to understand the complexity of technology and manage the digital transformation process of the organization (Nambisan, 2017). Openness to collaboration is a key characteristic of digital leadership, especially in today's interconnected and rapidly

changing business environment. This concept emphasizes the importance of transparent communication between team members, shared goals and collective problem solving. As businesses increasingly rely on digital tools to facilitate teamwork, managers who foster a culture of open collaboration can significantly increase team effectiveness and innovation. Openness to collaboration has been shown to not only improve team performance but also contribute to higher employee satisfaction and engagement (Cichor et al., 2023) social robots could be able to take on leadership roles. The aim of our study was to investigate human followers' perceptions and reactions towards robot leadership behavior, and differences based on the robot's displayed leadership style. We implemented a robot to show either a transformational or a transactional leadership style in its speech and its movements. We presented the robot to university and executive MBA students (N = 29).

Analytical thinking is a crucial component of digital leadership, especially in an era characterized by rapid technological advances and the proliferation of data. This cognitive skill enables leaders to interpret complex data sets, derive meaningful insights and make informed decisions that drive organizational success. In a digital environment

where information is abundant and often overwhelming, the ability to think analytically has become essential to overcome challenges and seize opportunities. Leaders who use analytical thinking are better equipped to drive innovation, increase operational efficiency, and improve overall organizational performance (Tigre et al., 2024). Data-driven decision making plays an important role in digital leadership. Leaders should measure their organization's performance, identify trends and make strategic decisions by analyzing data (Aksoy, 2024).

Digital transformation processes involve the integration of technology into business processes and organizations making the most of digital technologies. These processes can help organizations gain competitive advantage and achieve sustainable growth (Kraus et al., 2022). In this context, digital leadership has an important role in managing and successfully implementing the digital transformation process of organizations (Batchelder, 2023). Digital leadership enables organizations to advance technologically, helping them to gain competitive advantage and achieve sustainable growth. Therefore, it can be said that digital leadership is critical for organizations.

Digital transformation is the process of restructuring organizations' business processes and operations with digital technologies to make them more efficient, flexible and customer-centric (Baldassarre & Ricciardi, 2022). Digital transformation is reshaping the business world, creating numerous opportunities for organizations to improve operations, innovate and increase overall efficiency. This process involves integrating digital technologies into all aspects of a business, fundamentally changing the way the business operates and delivers value to customers (Picazo Rodríguez et al., 2024). This process offers organizations many opportunities.

Digital transformation offers numerous opportunities for organizations aiming to increase productivity and competitiveness. By streamlining processes, automating routine tasks, leveraging data for informed decision-making, and improving customer experiences, businesses can more effectively manage the complexities of the modern market. As highlighted in various studies, those that successfully implement digital transformation strategies are better positioned to achieve sustainable growth and innovation in an increasingly digitalized world.

2.2. Employee Performance

Employee performance refers to the effectiveness of an individual's behavior in contributing to organizational goals. Employee performance generally includes performance appraisals by supervisors or managers, which can affect various organizational outcomes such as productivity, job satisfaction and turnover (Ángeles López-Cabarcos et al., 2022a).

In the literature, employee performance can be addressed under different headings. However, it is basically divided into two: contextual performance and task performance (Bağcı, 2014). Task performance is a work process based on the execution of a task, the planned completion required by the task by those who contribute to the technical basis required by the job and formally part of the job. The most important criterion for the success of a task is the existence of a team of people who are deemed suitable for this task (Aslan & Doğan, 2020).

Contextual performance is the activation of the working environment through actions that activate the basic functions of the organization and also by making arrangements that will be positively received by employees in terms of environmental, social, economic and psychological aspects for the organization (Dahir Farah & Aydoğan, 2023). The main source of

difference in contextual performance is the acquisition and desire for the qualities required by the job rather than experience. The concept of context refers to the elements related to the work, not the work itself (Ersan & Süslü, 2022).

The success or failure of organizations is determined by how effectively employees perform their duties and the reward system (Dahir Farah & Aydoğan, 2023). An organization can be considered highly performing if it meets or exceeds its goals while contributing positively to society and the environment. If employees can work creatively, effectively and efficiently, their performance can be considered high (Hidayat et al., 2022). Increasing employee performance has a significant impact on both the employee and the organization. It can also be stated that the increase in employee performance depends on a good leader. Employee performance can generally be seen as the level of relevant output produced by an employee. This is the traditional view of employee performance.

Two features of this traditional view of employee performance, which focus on the quantity and quality of outputs produced in a job, can be stated. First, it focuses on the employee's performance on the job or task. Therefore, it is task performance or on-the-job performance rather than

an employee's overall performance. In addition to task performance, an employee's overall performance also includes extra role performance or contextual performance, such as taking extra responsibility, helping coworkers, and making innovative suggestions (Pawar, 2019). Second, the traditional view of employee performance focuses on the task outcomes achieved by an employee rather than the employee's behavior. However, employee performance can also be viewed as an evaluative judgment about the extent to which an employee's behavior facilitates or hinders the achievement of the organization's goals (Motowildo et al., 1997).

The two characteristics summarized above indicate that employee performance should be viewed as an evaluative judgment about the extent to which an employee's behavior facilitates or hinders the achievement of an organization's goals. Moreover, in the evaluation of employee performance, not only the employee's job- or task-related behaviors but also the employee's extra-role behaviors should be taken into account (Motowildo et al., 1997).

2.3. The Relationship Between Digital Leadership and Employee Performance

Research shows that digital leadership can positively affect

performance by increasing employee motivation, strengthening communication processes and using technology effectively (Banks et al., 2022; Mihardjo et al., 2019). Digital leaders encourage employees to be more efficient in their work processes thanks to their ability to quickly adapt to changing conditions. Digital leadership has emerged as a critical form of leadership that directly influences employee performance amid rapid technological change and digitalization in today's business world. By using information technologies effectively, digital leaders encourage innovative work behaviors of employees and thus provide a significant increase in business performance. Research shows that digital leadership positively affects employees' innovative work behaviors and job performance. For example, a study conducted in Türkiye revealed that digital leadership has a positive and significant impact on job performance (Büyükbeşe & Doğan, 2022).

In the Industry 4.0 era, digital leadership plays a critical role, especially among the factors that enhance individual employee performance. Digital leaders' ability to use various information technologies increases individual employee performance by 59% and this effect shows that the digital leadership model has a significant

explanatory power of 35%. In addition, digital leaders' successful practices in providing information to employees and creating infrastructure are considered among the main factors in the increase in performance (Abbasov, 2021).

The relationship between digital leadership and employee performance is not only limited to direct effects but also shaped by mediating mechanisms such as organizational learning and innovative work behaviors. As digital leadership fosters a culture of learning in the workplace, employees adopt innovative approaches, which in turn contribute positively to organizational performance. In this context, digital leadership not only enhances current performance but also supports innovation and learning processes for sustainable success (Morgül & Ataç, 2024).

Digital leadership affects employee performance through several interrelated mechanisms. First, by strategically leveraging digital tools and platforms, leaders can streamline processes, reduce administrative burdens and provide employees with real-time information, which increases task efficiency and quality (El Sawy et al., 2016; Kane, 2019). Second, digital leaders foster transparent communication and feedback loops, which strengthen employees' sense of inclusion,

motivation and psychological well-being—factors closely associated with higher performance (Zeike et al., 2019). Third, the emphasis on innovation and continuous learning under digital leadership encourages employees to develop new skills and adopt creative approaches, thereby enhancing both task and contextual performance (Mihardjo et al., 2019; Morgül & Ataç, 2024). Finally, digital leaders' ability to support employees' adaptation to rapid change reduces resistance and promotes organizational agility, which in turn contributes to sustained high performance (Khairy et al., 2023). Taken together, these mechanisms explain why digital leadership can have a positive impact on employee performance beyond simple technology adoption.

3. METHOD

3.1. Research Model

Quantitative research method is planned to test the hypotheses formed in the research. In this context, in the research, “digital leadership” is considered as an independent variable, “employee performance” as a dependent variable. The hypothesis will be tested with scales that have been used in previous studies in literature. The hypothesis and detailed information about the scales to be used in the research and the scale questions are presented below.

H1: There is a significant relationship between Digital Leadership and Employee Performance.

Digital Leadership Scale: The 9-question two-dimensional “Digital Leadership Scale” developed by Büyükebeş et al. (2022) will be used. The scale is 5-point Likert type.

Employee Performance Scale: Developed by Kirkman & Rosen (1999), adapted into Turkish by Çöl (2008) and used by Kara (2020) in his study. The scale is a 5-point Likert type consisting of 4 statements.

3.2. Universe and Sample

The population of the research consists of personnel working in the airline sector operating in Türkiye. Convenience sampling method was used in sample selection. A total of 450 employees working in different airline

companies participated in the study. The data for this study were collected using a convenience sampling method and voluntary participation. While this approach enabled access to a large sample of airline employees, it may also introduce potential selection bias. In particular, employees who are more engaged with their work or more interested in digital leadership topics may have been more inclined to participate, which could influence the results (Ángeles López-Cabarcos et al., 2022b). This potential bias should be taken into account when interpreting the findings, and future research employing randomized or stratified sampling methods could help mitigate this limitation and improve the representativeness of the sample. The demographic status of the participants is shown in the table below.

Table 1. Demographic Distribution

Gender	(n)	%	Age	(n)	%
Male	252	56%	18-25	87	19%
Female	198	44%	26-32	98	22%
Total	450	100%	32-40	90	20%
			41-48	95	21%
			48+	80	18%
			Total	450	100%
Institution	(n)	%	Education Status	(n)	%
THY AO	195	43%	Secondary	62	14%
Pegasus	110	24%	Associate	79	18%
Çelebi	75	17%			
Havaş	70	16%			
Total	450	100%			

Marital Status	(n)	%			
Married	224	50%	Bachelor	194	43%
Single	226	50%	Master	63	14%
Total	450	100%	PhD	52	12%
			Total	450	100%

4. ANALYSIS AND RESULTS

Analysis table is shown below.

Table 2. Analysis Table

Model Summary ^b					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	,214 ^a	0,046	0,044	0,28145	1,979
a. Predictors: (Constant), DL					
b. Dependent Variable: EmpPer					

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1,701	1	1,701	21,468	,000 ^b
	Residual	35,487	448	0,079		
	Total	37,187	449			
a. Dependent Variable: EmpPer						
b. Predictors: (Constant), DL						

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
B		Std. Error	Beta			
1	(Constant)	2,665	0,074		36,157	0,000
	DL	0,111	0,024	0,214	4,633	0,000
a. Dependent Variable: EmpPer						

In this study, a simple linear regression analysis was performed to examine the effect of digital leadership (DL) on employee performance (EmpPer). The analysis results show that the established model is generally significant ($F(1,448) = 21.468, p < .001$). Accordingly, the digital leadership variable significantly predicts employee performance. Although the explanatory power of the model is low ($R^2 = .046; \text{Adj. } R^2 = .044$), the effect of DL on EmpPer is statistically significant. This result indicates that DL explains approximately 4.6% of the variance in employee performance. Additionally, the Durbin-Watson value of 1.979 indicates that there is no autocorrelation issue in the model.

When examining the regression coefficients, the constant coefficient is $B = 2.665, p < .001$. The coefficient of the independent variable DL is calculated as $B = .111, \beta = .214, t = 4.633, p < .001$. According to this finding, a one-unit increase in DL corresponds to a .111-unit increase in

employee performance. Based on the standardized coefficient ($\beta = .214$), DL has a positive and moderately significant effect on EmpPer. Therefore, the regression model can be expressed as follows:

$$\text{EmpPer} = 2.665 + 0.111 \times \text{DL}$$

These results show that an increase in the level of digital leadership significantly improves employee performance. Similarly, the literature emphasizes that digital leadership has positive effects on employee job motivation, innovation, adaptation, and performance outcomes (El Sawy et al., 2016; Zeike et al., 2019; Kane et al., 2019). In particular, Zeike and colleagues (2019) note that digital leadership is directly related to employees' psychological well-being and job performance. In this context, the findings support the existing literature and demonstrate that digital leadership plays a significant role in employee performance. The correlation analysis table is shown below.

Table 3. Correlation Analysis Table

Correlations			
		DL	EmpPer
DL	Pearson Correlation	1	,214**
	Sig. (2-tailed)		0,000
	N	450	450
EmpPer	Pearson Correlation	,214**	1
	Sig. (2-tailed)		0,000
	N	450	450

** . Correlation is significant at the 0.01 level (2-tailed).

The results of the correlation analysis indicate a positive and significant relationship between digital leadership and employee performance ($r = 0.214$, $p < 0.01$, $N = 450$). This suggests that higher levels of digital leadership are associated with better employee performance. Consistent with these findings, the literature highlights that digital leadership positively affects employee motivation, innovation, adaptability, and overall performance outcomes (El Sawy et al., 2016; Kane, 2019; Zeike et al., 2019). In particular, Zeike et al. (2019) emphasize that digital leadership is directly linked to employees' psychological well-being and job performance. Overall, these results support existing literature and demonstrate that digital leadership plays a significant role in enhancing employee performance.

These analysis results support the hypothesis and show that digital leadership significantly improves employee performance. The study makes an original contribution to the literature by revealing the positive relationship between digital leadership and employee performance in the context of the airline industry. The research emphasizes that digital leadership is not only technology-focused

but also encompasses human and change management dimensions.

5. CONCLUSION

The main objective of this study is to examine the effect of digital leadership on employee performance in the airline industry. Data obtained from 450 employees working in airlines operating in Turkey through a survey were analyzed using SPSS software. The correlation and simple linear regression analyses conducted revealed a positive and significant relationship between digital leadership and employee performance. The findings show that an increase in the level of digital leadership positively affects employee performance and contributes to business efficiency.

The results obtained are largely consistent with the studies in existing literature. As emphasized in previous studies, digital leadership increases employee motivation, encourages the development of innovative ideas, and facilitates employees' adaptation to change (El Sawy et al., 2016; Kane, 2019; Zeike et al., 2019). The aviation industry's high level of competition, rapid change, and uncertainty further increase the importance of digital leaders. In this context, digital leaders' ability to make quick and accurate decisions in

times of crisis, effectively use digital tools and technologies, manage information flow transparently, and facilitate employee adaptation to new processes emerges as a critical success factor.

Furthermore, research findings show that digital leadership not only improves employee performance but also has indirect effects such as organizational commitment, psychological well-being, and job satisfaction. This highlights that digital leadership is a strategic element in creating a sustainable performance culture and securing long-term competitive advantage in businesses. Therefore, in order to effectively manage digital transformation in the aviation sector, it is necessary to develop leaders' digital competencies, strengthen communication with employees, and support an innovative work culture.

6. DISCUSSION

This study represents an early-stage exploration of the impact of digital leadership on employee performance in the airline industry. While the findings offer valuable initial evidence, they are limited in scope to a single sector and a single national context. Therefore, the generalizability of the results

should be approached with caution. In addition, the relatively low explanatory power of the model ($R^2 = 0.046$) suggests that other factors beyond digital leadership also influence employee performance. Future research could replicate and extend the present model across multiple industries and cultural contexts, or adopt longitudinal and mixed methods designs to better understand the mechanisms linking digital leadership to employee outcomes (Banks et al., 2022; Zeike et al., 2019). Such studies would enhance the reliability and external validity of the findings and help develop a more comprehensive theoretical framework for digital leadership.

This study was conducted to examine the effect of digital leadership in the airline industry on employee performance. The findings reveal that the level of digital leadership has a positive and significant effect on employee performance. According to the correlation analysis results, a moderate relationship ($r = 0.214$) was found between the two variables; regression analysis showed that digital leadership explained 4.6% of the variance in employee performance.

These results are consistent with similar studies in literature.

For example, Mihardjo et al. (2019) found that digital leadership positively affects innovative work behaviors and employee performance. Similarly, Banks et al. (2022) noted that digital leadership increases employee commitment, motivation, and productivity. The findings of this study show that digital leaders optimize business processes by strategically using technology, strengthen communication channels, and facilitate employees' achievement of goals.

The research also provides important findings in terms of the dynamics specific to the airline industry. The airline industry is a sector characterized by high competition, rapidly changing customer expectations, and intensive use of technology. In this context, managers with digital leadership skills play a critical role in making quick decisions during times of crisis, adapting employees to new technologies, and increasing operational efficiency.

Although the results confirm a positive and statistically significant association between digital leadership and employee performance, the relatively low explanatory power of the model ($R^2 = 0.046$) indicates that digital leadership accounts for only a small proportion of the variance in

performance. This finding suggests that while digital leadership is an important factor, employee performance is likely influenced by multiple additional variables such as organizational culture, job design, and individual competencies. Moreover, the cross-sectional nature of the study prevents any causal inference. Compared with previous studies reporting stronger explanatory power in different contexts (Abbasov, 2021; Büyükbeşe & Doğan, 2022) our findings may reflect industry-specific dynamics of the airline sector or differences in measurement scales. These observations highlight the need for more comprehensive models and longitudinal designs to better capture the complex pathways through which digital leadership affects performance outcomes.

When evaluated in terms of practical implications, developing the digital leadership competencies of airline managers can be used as a strategic tool to improve employee performance. In particular, the effective use of digital technologies will contribute to employees conducting their work processes more efficiently and strengthening communication and collaboration.

As recommendation;

- Manager Training: Airlines should offer training

programs to their managers to develop digital leadership skills.

- **Use of Technology:** The effective use of digital tools in operational processes should be encouraged.
- **Motivation and Communication:** Digital leaders should strengthen communication and feedback mechanisms to increase employee motivation.
- The study was conducted only in the airline industry in Turkey; research in other industries could increase the generalizability of the results.
- Since the data was collected using a self-reporting method, there is a possibility of respondent bias.
- Future studies may examine mediating (e.g., job satisfaction, organizational commitment) and moderating (e.g., agility) variables in the effect of digital leadership on employee performance.

Finally, the findings of the study reveal that the concept of digital leadership is not limited to technology management alone, but also encompasses the dimensions of human management, change management, and strategic vision

development. Therefore, developing digital leadership skills has the potential to improve both employee performance and organizational success.

ACKNOWLEDGMENT

The article resulted from the PhD thesis of Salih AYGÜN named “Examining the Effect of Digital Leadership on Employee Performance Through the Mediating Role of Adaptive Performance and the Moderating Effect of Agility: A Study in The Airline Industry”. The thesis was studied in Beykent University, İstanbul between 2021-2025 under the Business Management Department.

REFERENCES

- [1] Abbasov, A. (2021). Endüstri 4.0 Çağında Dijital Liderliğin Bireysel Performans Üzerindeki Etkileri: Azerbaycan’daki Bir Üretim Firmasında Araştırma. Dokuz Eylül University.
- [2] Aksoy, C. (2024). İşletmelerin Dijital Dönüşümü ve Dijital Liderlik Yaklaşımı. Kalite ve Strateji Yönetimi Dergisi, 4(1), 1–29.
- [3] Ángeles López-Cabarcos, M., Vázquez-Rodríguez, P., & Quiñoa-Piñeiro, L. M. (2022a). An Approach to Employees’ Job Performance Through Work Environmental Variables and

- Leadership Behaviours. *Journal of Business Research*, 140, 361–369.
- [4] Ángeles López-Cabarcos, M., Vázquez-Rodríguez, P., & Quiñoá-Piñeiro, L. M. (2022b). An Approach to Employees' Job Performance Through Work Environmental Variables and Leadership Behaviours. *Journal of Business Research*, 140, 361–369.
- [5] Aslan, M., & Doğan, S. (2020). Dışsal Motivasyon, İçsel Motivasyon ve Performans Etkileşimine Kuramsal Bir Bakış. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 11(26), 291–301.
- [6] Avolio, B. J., Kahai, S., & Dodge, G. E. (2000). E-leadership. *The Leadership Quarterly*, 11(4), 615–668.
- [7] Baldassarre, F., & Ricciardi, F. (2022). How Digital Transformation is Changing Business Models and Entrepreneurship. *Knowledge Drivers for Resilience and Transformation*, 2402–2414.
- [8] Banks, G. C., Dionne, S. D., Mast, M. S., & Sayama, H. (2022). Leadership in the digital era: A review of who, what, when, where, and why. *The Leadership Quarterly*, 33(5), 101634.
- [9] Batchelder, C. (2023). Leadership in the Age of Digital Transformation. <https://www.linkedin.com/pulse/leadership-age-digital-transformation-dr-colleen-batchelder/>
- [10] Büyükbeşe, T., Dikbaş, T., Klein, M., & Batuk Ünlü, S. (2022). A Study on Digital Leadership Scale (DLS) Development. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, 19(2), 740–760.
- [11] Büyükbeşe, T., & Doğan, Ö. (2022). Dijital Liderliğin Yenilikçi İş Davranışı ve İş Performansı Üzerine Etkisi. *Akademik Araştırmalar ve Çalışmalar Dergisi (AKAD)*, 14(26), 173–186.
- [12] Cichor, J. E., Hubner-Benz, S., Benz, T., Emmerling, F., & Peus, C. (2023). Robot Leadership– Investigating human perceptions and reactions towards social robots showing leadership behaviors. *PLOS ONE*, 18(2), e0281786.
- [13] Çöl, G. (2008). Algılanan Güçlendirmenin İşgören Performansı Üzerine Etkileri. *Doğuş Üniversitesi Dergisi*, 9(1), 35–46.
- [14] Dahir Farah, M., & Aydoğan, Prof. Dr. E. (2023). Uzaktan Çalışmanın Çalışanların İş Performansı Üzerindeki Etkileri: Somaliland Örneği. 3. Sektör Sosyal Ekonomi Dergisi.
- [15] El Sawy, O., Amsinck, H., Kraemmergaard, P., & Lerbech Vinther, A. (2016). How LEGO Built the Foundations and Enterprise Capabilities for Digital Leadership. *MIS Quarterly Executive*, 15(2).
- [16] Ersan, A., & Süslü, M. (2022). Covid-19 Korkusunun Sağlık

- Çalışanlarının İş Performanslarına Etkileri ve Örgütsel Bağlılığın Aracılık Rolü. Akademik Hassasiyetler, 9(18), 231–266.
- [17] Hidayat, T., Maarif, S., & Asmara, A. (2022). Employee Performance Management Scenarios in the Era of Work from Home. *International Journal of Research and Review*, 9(1), 452–460.
- [18] Kane, G. (2019). The Technology Fallacy: People Are the Real Key to Digital Transformation. *Research-Technology Management*, 62(6), 44–49.
- [19] Kara, A. İ. (2020). Algılanan Liderlik Tarzları, Örgüt Kültürü ve Örgütsel Adaletin İşgören Performansı İle İlişkisi [Yayımlanmamış Doktora Tezi]. Beykent Üniversitesi.
- [20] Khairy, H. A., Baquero, A., & Al-Romeedy, B. S. (2023). The Effect of Transactional Leadership on Organizational Agility in Tourism and Hospitality Businesses: The Mediating Roles of Organizational Trust and Ambidexterity. *Sustainability*, 15(19), 14337.
- [21] Kirkman, B. L., & Rosen, B. (1999). Beyond Self-Management: Antecedents and Consequences of Team Empowerment. *Academy of Management Journal*, 42(1), 58–74.
- [22] Klein, M. (2020). Leadership Characteristics in The Era of Digital Transformation. *Business And Management Studies: An International Journal*, 8(1), 883–902.
- [23] Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital Transformation in Business and Management Research: An Overview of the Current Status Quo. *International Journal of Information Management*, 63, 102466.
- [24] Küsbeci, P., & Uzunçarşılı, Ü. (2021). İşletmelerde Dijital Dönüşüm Sürecinde Dijital İkiz Teknolojisinin Rolü. In *Akıllı Dönüşüme Yolculuk* (pp. 112–129). Artikel Akademi.
- [25] Mihardjo, L. W. W., Sasmoko, S., Alamsjah, F., & Elidjen, E. (2019). Digital leadership role in developing business model innovation and customer experience orientation in industry 4.0. *Management Science Letters*, 1749–1762.
- [26] Morgül, Ü. A., & Ataç, L. O. (2024). Dijital Liderlik ve Yenilikçilik Arasındaki İlişkide Örgütsel Öğrenmenin Aracılık Rolü: Uzaktan Çalışanlar Üzerinde Bir Araştırma. *Journal of Emerging Economies and Policy*, 9(Special Issue), 51–65.
- [27] Motowildo, S. J., Borman, W. C., & Schmit, M. J. (1997). A Theory of Individual Differences in Task and Contextual Performance. *Human Performance*, 10(2), 71–83.
- [28] Nambisan, S. (2017). Digital Entrepreneurship: Toward a

- digital Technology Perspective of Entrepreneurship. SAGE Publications.
- [29] Picazo Rodríguez, B., Verdú-Jover, A. J., Estrada-Cruz, M., & Gomez-Gras, J. M. (2024). Does Digital Transformation Increase Firms' Productivity Perception? The Role of Technostress and Work Engagement. *European Journal of Management and Business Economics*, 33(2), 137–156.
- [30] Technology pioneers: Developers of life-changing technology. (2009). *Strategic Direction*, 25(4), 32–34.
- [31] Tigre, F. B., Henriques, P. L., & Curado, C. (2024). The Digital Leadership Emerging Construct: A Multi-Method Approach. *Management Review Quarterly*.
- [32] Zeike, S., Bradbury, K., Lindert, L., & Pfaff, H. (2019). Digital Leadership Skills and Associations with Psychological Well-Being. *International Journal of Environmental Research and Public Health*, 16(14), 2628.

NATO'S NEW FORCE MODEL: ADAPTING TO A DYNAMIC SECURITY LANDSCAPE

Khayal Iskandarov IBRAHIM*, Piotr GAWLICZEK**

*National Defense University, Republic of Azerbaijan

** University of Warmia and Mazury, Poland

History shows that the Alliances which maintained relevant and timely transformation have outlived others. In this regard, NATO, the biggest political-military organization of its time might undoubtedly be referred as the most successful one of the same nature. The Alliance has managed to conduct proper transformation processes against the backdrop of various claims that it was obsolete or irrelevant at different times. Suffice to say that NATO adopted its New Strategic Concept and introduced its New Force Model (NFM) as a response to Russian war against Ukraine in 2022. The purpose of this paper is to analyze NATO's New Force Model (NFM) and justify its introduction in response to an evolving and dynamic security environment. The paper delineates NATO's NFM as a desperate need after the war between Russia and Ukraine broke out, highlights the main differences from the Old Force Model, since the ongoing processes prompted NATO to take stock of each and every single detail in a dramatically changing security landscape. The Hypothesis of the paper is that NATO's NFM is a necessary and timely transformation in response to the Russia-Ukraine war. The paper tries to find answers to the following research questions: 1. Why was NATO's New Force Model introduced, and how does it differ from the previous model? 2. How does the NFM address the challenges of an ever-changing security environment? To develop this paper, a combination of qualitative and quantitative research methods, such as Comparative Analysis, Synthesis and Case Studies have been used. NATO's adoption of the NFM marks a significant shift in its approach to crisis response, deterrence, and collective defense. In response to the Russia-Ukraine war, hybrid warfare threats, and regional instability, the NFM enhances force allocation, interoperability, and preparedness to address evolving security challenges.

Key words: NATO, transformation, New Force Model, Old Force Model, NRF, ARF.

1. INTRODUCTION

History demonstrates the critical importance of forming alliances against common enemies and highlights that victory is most assured when allied forces operate in complete harmony. Disjointed military efforts among nations often prove less effective than integrated, cooperative strategies. However, over the past century, disparities in equipment, tactics, and a lack of cohesion have significantly weakened many alliances, as seen in conflicts such as the Korean War, the Dominican Civil War, the Vietnam War, and the Gulf War. Since its inception, NATO—the most successful military-political alliance in history—has actively addressed these challenges by developing interoperability frameworks, techniques, models, and measures to enhance unified military effectiveness (Nasirov & Iskandarov, 2017). NATO was once considered a vestige of a bygone era, but it swiftly reaffirmed its relevance—and even its importance—following the 1991 Rome Summit. By adopting a new Strategic Concept, the Alliance initiated a comprehensive transformation, adapting to the evolving security landscape and redefining its role in the post-Cold War world (Iskandarov et al., 2019a). To sustain peace and stability across

Europe, NATO recognized the necessity of expanding beyond its conventional borders following the Cold War. The integration of new members into the Alliance became a strategic priority, sparking extensive debates and leading to increased cooperation with partner countries. Emphasizing the importance of interoperability, NATO sought to ensure that partner forces could operate seamlessly together, enhancing collective security and operational effectiveness (Nasirov & Iskandarov, 2017).

Numerous academic studies explore NATO's transformation, analyzing its evolution from a Cold War alliance to a global security actor. There are plenty of prominent figures which have been both opponents and proponents of NATO enlargement, which in fact highlights the relevance of the topic throughout history. John S. Duffield (1994) aims to explain the factors behind NATO's enduring relevance and resilience right after the Cold War ended. Jamie Shea (2012) tries to justify the relevance of NATO in an entirely different landscape with the fall of the Berlin Wall in 1989. Ruiz Palmer (2019) addresses the aims, achievements and challenges of NATO's post-Cold War transformation. Andrea Gilli et al. (2020) focus on NATO's

technological transformation. In a number of papers dedicated to NATO's transformation and partnerships, Khayal Iskandarov and Piotr Gawliczek highlight the competition for power and influence in different regions and illustrate Russia's security interests in NATO's enlargement policy, examine the extent to which NATO partnership mechanisms contribute to the cooperation in the field of education and interoperability of forces (Nasirov & Iskandarov, 2017; Sadiyev & Iskandarov, 2018; Iskandarov & Gawliczek, 2018; Hasanov, et al., 2019; Iskandarov, 2019a; Iskandarov, 2019b; Iskandarov et al., 2019b; Iskandarov & Gawliczek, 2019; Iskandarov & Gawliczek, 2020; Iskandarov & Gawliczek, 2021; Iskandarov et al., 2023). A book edited by Jason Blessing et al. (2021) – "NATO 2030: Towards A New Strategic Concept and Beyond" provides new insights into NATO's changing threat landscape, shifting internal dynamics, and the evolution of warfare, offering perspectives on the alliance's future strategic direction.

However, only a handful of studies focus on NATO's transformation after 2022. For instance, Zoltan Szenes (2023) examines the Alliance's new perception of deterrence and defence and its planned measures, compares

2010 and 2022 Strategic Concepts, claims that, the latter has brought NATO into a new era of great power competition. The report prepared by Sean Monaghan et al. (2024), takes stock of allied efforts to strengthen collective defense in the face of emerging security threats. The report raises a critical question: while NATO may be prepared for the outbreak of conflict, is it adequately equipped to sustain and ultimately prevail in a protracted war? Based on Madrid commitments, The report assesses whether NATO is prepared to sustain and succeed in a protracted conflict. John R. Deni (2024) examines the rationale behind the launch of the new force model and outlines key elements of it, including force organization, force management, as well as command and control. Jacopo Maria Bosica (2024) presents the aspects of the New Force Model in order to highlight improvements and changes in comparison with the old one. The author claims that New Force Model can support the quick deployment capabilities of European Allies to defend themselves without necessarily waiting for the United States to lead. The literature review shows that, the prospects and challenges with the adoption of the New Force Model have not been extensively studied at all. This paper aims to explore NATO's

New Force Model and validate its implementation in the context of a constantly evolving security landscape.

2. OLD VS. NEW FORCE MODEL: COMPARATIVE ANALYSIS

The new NATO deterrence calls for divisions and brigades that are less mobile and more resilient, with capabilities that can be used in all domains (sea, land, air, cyber, and space). The lightly armed infantry units that NATO formerly used as a “tripwire” on the eastern border and for its crisis-management missions in Afghanistan are clearly no longer in use. The deterioration of Russian land power in Ukraine allows Europe breathing room to bolster their armed forces and modify their industries against the backdrop of radically changing security landscape (Larsen, 2024).

One might question whether NATO needed to adopt a new force model, given that Russian power has been in decline since its involvement in a large-scale war with Ukraine. However, a stark reality must be acknowledged: no matter the level of preparation, armies with combat experience are always more formidable than those without. The Russian military leveraged

its experience in Syria to advance its objectives in Ukraine. Without these lessons, it is likely that Russia would have struggled to maintain its momentum against determined Ukrainian resistance (Hasan, et al., 2024). Therefore, despite its losses, it would be naïve to assume that Russia will remain weak in the foreseeable future or even in the long term. According to Global firepower 2024, Russia still maintains the second strongest military in the world (globalfirepower.com, 2024). The straightforward answer to this question is that NATO is now closer to direct conflict with Russia than at any point since the collapse of the Soviet Union. The perceived threat level is particularly high for allies bordering Russia, necessitating significant adjustments in force composition, defense budgets, operational planning, and broader foreign and security policies. (Iskandarov et al., 2025). It is also worth noting that Russia has doubled its military budget despite only experiencing modest economic growth (Hooker, 2024).

The NFM, introduced at the Madrid Summit in June 2022, is a major adaptation of the alliance's military structure in response to evolving security threats, especially after the war broke out between Russia and Ukraine. The model represents a

significant enhancement of NATO's defense posture, with a particular focus on rapid deployment and scalability across its member states. The NFM includes improvements in NATO's command and control structure to ensure faster decision-making and smoother coordination between member states. Back then, a large theater battle in the North Atlantic was thought implausible, and therefore the current NATO Command Structure is based on perceptions of Russia as a partner. The Command Structure is the backbone of NATO. It is composed of permanent multinational headquarters at the strategic, operational and component levels of command, distributed geographically and commonly funded. It offers the opportunity to all Allies to participate in, and contribute to, the command and control of all Alliance operations, missions, and activities across all military domains (nato.int, 2018). The New Force Model emphasizes integrated operations across multiple domains – land, air, sea, cyber, and space. This ensures NATO can respond to threats that arise in any domain and across geographical regions simultaneously. The new model involves a blend of national forces, which will be placed on high readiness, and multinational

NATO forces that can be deployed together.

By adopting the NFM, NATO aims to ensure its ability to deter and defend against any aggressor, maintain its technological edge, and guarantee the collective security of its member states. The model reflects NATO's commitment to rapid adaptation in the face of changing geopolitical realities. Rather than having to make a political decision to liberate occupied territory against a nuclear-armed adversary, this is essential for maintaining alliance unity during a security crisis. There is a risk of territorial loss from delays, since reinforcements from Western Europe would need to travel almost 1,000 kilometers to reach battle positions in the event of a crisis or conflict on its Eastern flank (Larsen, 2024).

The NFM represents a significant shift from its old force model against the backdrop of sweeping changes in global security dynamics. First and foremost, with this model, NATO aims to increase the number of its high-readiness forces to over 300,000, a significant rise from the previous 40,000 in the NATO Response Force (NRF). These forces will be ready to deploy at short notice in case of a crisis. The NFM will allow for a more flexible and scalable approach, meaning

that NATO can deploy different types and sizes of forces depending on the threat and the geographical location. This includes air, sea, land, and cyber capabilities. The NRF was relatively limited in size and scope, its deployment was slower compared to today's standards, with varying response times depending on the threat, although it included land, air, sea, and special operations components. The readiness levels were generally lower, with fewer forces held on high alert, and most units could deploy within weeks, not days.

Second, in the Old Force Model, NATO's posture was less focused on forward defense, with a greater reliance on a centralized force that would be deployed to different regions if needed. While the eastern flank (Baltic states, Poland) was recognized as vulnerable, there was less emphasis on positioning large, permanent forces or equipment in the region. The NFM significantly strengthens forward defense and deterrence, especially in response to Russia's war against Ukraine. NATO is pre-positioning troops, equipment, and supplies along the eastern flank (Baltic states, Poland, and other Eastern European countries) to respond quickly to any potential threats. This shift reflects the need to deter Russia and respond more rapidly

to any aggression in Eastern Europe or the Baltic region. The new model integrates pre-positioned equipment and infrastructure development for quicker deployment and sustainment of forces in frontline states.

Third, while the Old Force Model was more rigid and focused on large-scale, conventional military operations (less emphasis on hybrid warfare, cyber defense, and multi-domain operations) and NATO's response tended to involve entire units, with less flexibility for small-scale, tailored operations, in the New Force Model, NATO can respond with smaller, specialized units or full-scale forces, depending on the threat level and the specific region involved. The new model emphasizes multi-domain operations, integrating land, sea, air, cyber, and space capabilities into a cohesive force structure that can respond to modern hybrid threats. NATO now has a more robust system for countering cyberattacks, disinformation, and hybrid threats, with dedicated units and frameworks for dealing with these non-traditional forms of aggression.

Finally, since NATO's decision-making process has often been viewed as an Achilles' heel by its adversaries, New Force Model will ensure faster decision-making processes and a smoother flow of information between member states,

unlike the Old Force Model, where command and control were largely centralized, and decisions, especially those requiring the deployment of large forces, could be slow due to NATO's consensus-based decision-making structure. A notable historical example occurred in February 2003, when Türkiye requested NATO military authorities to prepare defense plans against a potential Iraqi attack. However, NATO faced deep divisions and one of its worst crises, as France, Germany, and Belgium firmly vetoed the request, highlighting the challenges of consensus-based decision-making (Edelman et al., 2024). The same scenario is never ruled out when preparing NATO for worst-case scenarios. New Force Model will allow for quicker activation of forces and rapid response in times of crisis, particularly in scenarios that require immediate action. NATO's new regional defense plans outline the necessary steps and resources to protect specific regions of Alliance territory from attack, while also fostering coordination and cooperation among Allies to ensure a unified and effective response in times of crisis. These plans provide detailed strategies for defending the Alliance, including the allocation of specific forces and capabilities and setting readiness levels. A key focus is on enabling rapid

reinforcements. All forces are pre-assigned to specific plans, allowing for a swift response to any threat. However, the successful execution of these plans and the credibility of NATO's deterrence posture depend on the Allies fulfilling their resource commitments and conducting regular exercises (Loorents, 2024).

3. THE NEW FORCE MODEL: FUTURE PROSPECTS AND IMPLICATIONS

According to the New Force Model, the Alliance will have a three-tier readiness system for the forces it will use to fulfill the requirements of the operational plans approved in the three sub-regions of Europe – the Arctic and North Atlantic, Southern Europe and Southeast Europe.

A Tier 1 force of approximately 100,000 troops must be ready within 0-10 days of the onset of a crisis or predicted warning. These forces consist mainly of so-called “in-place” forces, which include both national forces stationed in their own locations and troops from other NATO Allies on mission in an Allied country in crisis. For example, in the case of Estonia, Tier 1 forces include the Estonian Army and a NATO multinational battalion (NATO Enhanced Forward Presence) (around 1,400 troops from the United Kingdom, France and Denmark).

Tier 2 forces consist of approximately 200,000 troops and must be ready within 10 to 30 days. These forces are generally multi-domain in terms of capabilities relative to the lighter, rapid response forces of Tier 1. They are also division and corps level, unlike tier 1 forces.

Finally, Tier 3 forces number around 500,000 and should be operational within 30-180 days (Deni, 2024).

In addition to the three tiers, the new model introduces a crucial component—the Allied Reaction Force (ARF). While this flexible response force bears similarities to the former NATO Response Force's (NRF) Very High Readiness Joint Task Force (VJTF), it would be inaccurate to consider them identical. Because, the VJTF in comparison was pretty slower to deploy than expected and was constantly accompanied by shortcomings depending on logistical challenges, political decisions, and member states' readiness. With about 40,000 troops NRF itself was insufficient to address large-scale crises, particularly in scenarios involving multiple fronts and actors (whose military capabilities could outpace NATO's response) or prolonged operations. The units assigned to the NRF had only been used for disaster

relief and security until February 2022, since its inception in 2003. Very High Readiness Joint Task Force (VJTF) itself was created in 2014 as a measure of the Readiness Action Plan (RAP). NATO deployed high-readiness elements of the NRF for the first time in a deterrence and defense role by placing thousands of additional troops at high readiness earmarked for the NRF, ensuring that it continues to have the speed, responsiveness and capability to defend NATO territory and populations (nato.int, 2023). However, the VJTF was never “fully manned” because the Allies did not contribute it enough (Deni, 2024). It has consistently been perceived as falling short when it comes to the task of rapid deployment and effective employment during times of crisis. The ARF also differs from the VJTF in that it is truly multi-domain, incorporating capabilities in cyberspace and space. It provides NATO with a strategically significant, highly ready, multi-domain, and multinational force that can be rapidly deployed at the command of SACEUR. This enhances deterrence in both peacetime and crisis situations while also reinforcing the Alliance's defenses in the event of conflict. SACEUR has a central role in implementing NATO's military strategy and ensuring the readiness

and effectiveness of NATO forces. SACEUR's priorities typically focus on maintaining the collective defense posture of NATO, enhancing deterrence, and adapting to evolving security challenges. The authorities granted to SACEUR to activate and deploy NFM forces pre-crisis are critical for delivering the Deterrence and Defense of the Euro-Atlantic Area. These authorities are not merely procedural but are instrumental in enabling NATO to execute its operational plans effectively. As SACEUR himself emphasized, such authorities enhance "NATO's ability to execute its plans and helps influence Allies to contribute their own forces" (Monaghan et al., 2024). Some experts, such as Sven Biscop (2022) and Jacopo Maria Bosica (2024) claim that NATO's New Force Model will provide the SACEUR with broader discretionary authority in contingency operational planning, thereby strengthening NATO's overall responsiveness and effectiveness. However, we deem that this process is not without challenges. A key obstacle lies in the reluctance of some allies to grant NATO commanders the "transfer of authority" necessary for optimizing and streamlining force deployments. This hesitancy often stems from concerns over national sovereignty, political considerations, or differing

threat perceptions within the Alliance. This reluctance underscores the importance of ensuring that NFM force composition aligns with regional contingency plans. Often, these plans may require specific capabilities or units that differ from the standard contributions allies typically provide to NATO. For example, a regionally tailored response might necessitate highly mobile mechanized infantry, advanced air defense systems, or cyber capabilities that certain allies are either unwilling or unable to supply on short notice. To address these gaps, NATO must work proactively with member states to build trust and foster greater interoperability. This includes establishing clear frameworks for "transfer of authority" agreements, improving the alignment of national contributions with Alliance priorities, and ensuring that NFM forces are flexible, scalable, and regionally integrated. A case in point is the transfer of authority by Naval Striking Forces NATO, assuming command of over 5,000 U.S. Sailors and Marines assigned to the USS Bataan Amphibious Readiness Group (ARG) (strikfornato, 2024). By doing so, NATO can enhance its readiness and deterrence posture while maintaining the political cohesion necessary for collective defense.

The ARF will be capable of performing functions supporting all of the Alliance's core tasks, not just deterrence and defense. Nevertheless, the focus of ARF training is likely to be on exercises for scenarios involving Article 5. The NATO Rapid Deployable Corps (NRDC-ITA), based in Solbiate Olona, Italy, will lead the ARF for the next three years (2024-2027). In preparation for this role, NRDC-ITA undertook a rigorous series of military exercises, academic research, and personnel training, culminating in the Steadfast Deterrence 24 exercise that confirmed it as the Headquarters of the ARF.

One of the most frequently asked questions in the academic field regarding NATO's force structure pertains to the number of units dedicated or contributed by member nations to the Allied Response Force (ARF) and its respective tiers. This inquiry often reflects a broader interest in understanding the equitable distribution of responsibilities, the operational readiness of multinational forces, and the overall capacity of NATO to respond effectively to crises.

For instance, Germany aims to increase its active armed forces to 200,000 and to contribute 30,000, or ten percent, to the high-readiness NATO Force Model and a

combination of 85 ships and aircraft mobilizable in 30 days (Tier 2) (Monaghan et al., 2024). Poland aims to increase its armed forces to 300,000 and is much further ahead in procuring new battle tanks, artillery, combat airplanes, and air defense systems that are necessary for the land warfare conducted in Ukraine (Hooker, 2024). The United Kingdom offered combat aircraft, ships, aircraft carriers, and "brigade-sized land forces." The United States has also placed much of its 80,000 strong forces in Europe under NATO command, the most connected it has been to NATO structures in decades (Monaghan et al., 2024). It is anticipated that, some other European countries, such as Romania, Estonia, Latvia, Lithuania will increase their troop contributions to NATO's New Force Model, reinforcing the Alliance's capacity for rapid deployment and enhancing collective defense capabilities. However, nations such as Belgium, Canada, Italy, and Spain have been hesitant to meet the defense spending target of 2% of their GDP (Kennedy & Renken, 2025). Indeed, there has been a significant increase in defense spending, with a growing number of NATO member countries meeting or exceeding the Alliance's 2% GDP target in response to evolving global security challenges, even though there

are claims that U.S. disengagement could pose significant challenges for NATO in the foreseeable future, potentially affecting the alliance's cohesion, operational effectiveness, and strategic direction. For instance, in 2024, NATO members collectively allocated \$1.303 trillion to defence expenditures, marking a significant increase from the previous year. According to figures released by the Western military alliance, 22 out of 32 member countries met the benchmark of spending 2% of their GDP on defence. This record-breaking figure includes €412 billion spent by European members and Canada, 38% of which was dedicated to the procurement of major military equipment. The U.S. alone accounted for €720 billion of the total. Comparatively, in 2023, NATO members had spent approximately €176 billion less, reflecting a notable 19% year-on-year increase in overall defence spending. Traditionally underperforming nations such as Belgium (1.29%), Italy (1.5%), and Spain (1.24%) have each pledged substantial financial commitments to reach the 2% threshold. Canada, currently at 1.45%, also falls short of the target. Even some of NATO's principal security actors are facing fiscal challenges in sustaining robust defence investments. For instance, the United Kingdom (2.33%),

Germany (2.1%), and France (2.03%), while meeting the 2% criterion, are reportedly contending with budgetary pressures. The data further indicates that a considerable share of the increased funding is being channeled towards NATO's eastern flank, particularly the border regions adjacent to Russia, encompassing the Baltic States and Poland (euractiv.com, 2025). While the concerns remain speculative, the aforementioned developments are of utmost importance in ensuring NATO's continued strength and unity. Maintaining a robust transatlantic partnership, reinforcing collective defense commitments, and enhancing burden-sharing among member states will be crucial in preserving the alliance's stability and effectiveness in the face of evolving global security challenges.

4. CONCLUSIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

NATO, as the largest political-military alliance, has demonstrated resilience by continuously transforming in response to global security challenges. The introduction of the NFM underscores NATO's commitment to maintaining relevance and effectiveness despite claims of obsolescence. NATO's approach

to crisis response, deterrence, and collective defense has undergone a dramatic change with the adoption of the NFM. NATO wants to respond to a more complex security environment by optimizing force allocation, boosting interoperability among member states, and raising preparedness. In light of Russia-Ukraine war, the difficulties posed by hybrid warfare, and the increasing instability in some regions, the model reaffirms the Alliance's capacity to react swiftly to new threats. The analysis demonstrates that the NFM will enhance rapid deployability, scalability, and multi-domain integration, reflecting a shift from a slower, centralized, and rigid Old Force Model to a flexible and technologically sophisticated structure. By strengthening force integration, operational readiness, and adaptability, NATO ensures its continued relevance in an increasingly complex global security landscape, however, its effectiveness depends on sustained member-state commitment, interoperability, and equitable burden-sharing. The research examines the long-term implications of the NFM for deterrence, alliance cohesion, and transatlantic security. It highlights that high-readiness forces in NATO increase from 40,000 to over 300,000 troops, enabling rapid deployment

across land, air, sea, cyber, and space domains. Pre-positioned troops and equipment along NATO's eastern flank strengthen deterrence and reduce response times. Integration of cyber and space capabilities reflects NATO's adaptation to hybrid and modern warfare. Delegation of authority to SACEUR ensures faster decision-making, addressing prior limitations of consensus-based processes. Despite increased contributions, disparities in capabilities and defense spending may impede full implementation.

Ultimately, the true efficacy of any new model or concept is determined through practical implementation, and the NFM is no exception. Although this study addresses critical dimensions of the evolving security landscape, significant opportunities remain for future research to further evaluate its operational impact, strategic implications, and potential for adaptation in response to emerging threats. Future research should focus on evaluating the operational effectiveness of NATO's NFM, including the readiness, deployment, and scalability of its multi-domain forces, as well as the political and strategic dynamics shaping member states' contributions, burden-sharing and willingness to grant command authority. Studies should also

examine the integration of cyber, space and hybrid capabilities, the long-term implications for deterrence and transatlantic security, and the influence of emerging technologies such as AI and autonomous systems.

REFERENCES

- [1] Biscop, S. (2022). *The New Force Model: NATO's European army?* (Egmont Policy Brief No. 285). Egmont Institute. Available at: https://www.egmontinstitute.be/app/uploads/2022/09/Sven-Biscop_PolicyBrief285_vFinal.pdf (Accessed: February 11, 2025).
- [2] Blessing, J., Elgin, K. K., & Ewers Peters, N. M. (Eds.). (2021). *NATO 2030: Towards a new strategic concept and beyond*. Foreign Policy Institute / Henry A. Kissinger Center for Global Affairs, Johns Hopkins University SAIS. Available at: <https://sais.jhu.edu/sites/default/files/NATO2030AndBeyondAccessibleVersion.pdf> (Accessed: January 11, 2025).
- [3] Bosica, J.M. (2024). *NATO's new force model: A watershed step for the alliance's deterrence, defence and crisis management missions in a complex Euro-Atlantic security landscape*. Atlantic Forum. Available at: <https://www.atlantic-forum.com/atlantica/natos-new-force-model-a-watershed-step-for-the-alliances-deterrence-defence-and-crisis-management-missions-in-a-complex-euro-atlantic-security-landscape>. (Accessed: January 20, 2025).
- [4] Deni, J.R. (2024). *The new NATO force model: Ready for launch?* NATO Defense College. Available at: <http://www.jstor.org/stable/resrep60400> (Accessed: January 30, 2025).
- [5] Duffield, J. S. (1994). NATO's Functions after the Cold War. *Political Science Quarterly*, 109(5), pp. 763–787. doi: <https://doi.org/10.2307/2152531>.
- [6] Edelman, E. S., Manning, D., & Miller, F. C. (2024). NATO's decision process has an Achilles' heel. Atlantic Council. Available at: <https://www.atlanticcouncil.org/blogs/new-atlanticist/natos-decision-process-has-an-achilles-heel/> (Accessed: February 6, 2025).
- [7] euractiv.com. (2025). NATO members spent \$1.3 trillion on arms last year Available at: <https://www.euractiv.com/section/defence/news/nato-members-spent-1-3-trillion-on-arms-last-year/>(Accessed: April 25, 2025).
- [8] Gilli, A., Gilli, M., Leonard, A.-S., & Stanley-Lockman, Z. (2020). “NATO-mation”: preparing for technological transformation. In *“NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence* (pp. 25–28). NATO Defense College. doi: <http://www.jstor.org/stable/resrep27711.10>
- [9] Global Firepower. (2024).

- 2024 military strength ranking: Russia. Available at: https://www.globalfirepower.com/country-military-strength-detail.php?country_id=russia.
- [10] Hasan, A.H., Iskandarov, K., & Gawliczek, P. (2024). Azerbaijan's 2023 counterterrorism operation in Karabakh region: causes and consequences. *Social Development and Security*, 14(3), pp. 1-13. doi: <https://doi.org/10.33445/sds.2024.14.3.1>.
- [11] Hasanov, A.H., Iskandarov, K.I. & Sadiyev, S.S. (2019). The evolution of NATO's cyber security policy and future prospects. *Journal of Defense Resources Management*, 10(1), pp. 94-106. Available at: link.gale.com/apps/doc/A629148092/AONE?u=anon~2949059&sid=googleScholar&xid=b1df5f56 (Accessed: January 30, 2025).
- [12] Hooker, R.D. (2024). *A new NATO command structure*. Atlantic Council. Available at: <https://www.atlanticcouncil.org/wp-content/uploads/2024/05/A-New-NATO-Command-Structure.pdf> (Accessed: January 29, 2025).
- [13] Iskandarov, K. (2019a). NATO enlargement vis-a-vis Russian security policy (1999-2019) in *Security and Russian threats*, pp. 37-70. Uniwersytet Jana Kochanowskiego w Kielcach.
- [14] Iskandarov, K. (2019b). *The South Caucasus-NATO Cooperation*. LAP LAMBERT Academic Publishing.
- [15] Iskandarov, K., & Gawliczek, P. (2018). NATO's role in improving professional military education with a focus on the south Caucasus countries. *The Quarterly Journal*, 18(3-4), 35-44. doi: <https://doi.org/10.11610/Connections.18.3-4.02>.
- [16] Iskandarov, K. & Gawliczek, P. (2020). The "new great game" in the South Caucasus: competition for power and influence. *Social Development and Security*, 10(1), pp. 25-33. doi: <https://doi.org/10.33445/sds.2020.10.1.4>
- [17] Iskandarov, K., & Gawliczek, P. (2019). The south Caucasus and NATO's defence education enhancement programme. Retrospective analysis. *Social development and Security*, 9(5), pp. 3-14. doi: <https://doi.org/10.33445/sds.2019.9.5.1>
- [18] Iskandarov, K., & Gawliczek, P. (2021). The south Caucasus and NATO's defence education enhancement programme. The measurement of its effectiveness. *Social Development and Security*, 11(1), pp. 70-79. doi: <https://doi.org/10.33445/sds.2021.11.1.7>
- [19] Iskandarov, K., Gawliczek, P. & Akbarov, M. (2025). NATO's New Force Model and Partner Engagement in an Evolving Security Landscape. *Social Development and Security*, 15(2), pp. 1-11. <https://doi.org/10.33445/sds.2025.15.2.1>
- [20] Iskandarov, K., Gawliczek, P.

- & Mrozek, J. (2023). *NATO's partnership policy in a dynamic security landscape: A simple look at a complex picture*. Olsztyn: Centre for Eastern Europe Research UWM in Olsztyn.
- [21] Iskandarov, K., Mammadzada, V. & Sadiyev, S. (2019a). Non-Alliance policy as a principle of shaping the national security with a focus on the case of Azerbaijan, *Journal of Defense Resources Management*, 10:2, pp. 62-72. Available at: <https://www.cceol.com/search/article-detail?id=812186> (Accessed: February 11, 2025).
- [22] Iskandarov, K., Simons, G. & Gawliczek, P. (2019b). The South Caucasus: Stage for a 'New Great Game' between NATO and Russia?. *Connections: The Quarterly Journal*, 18, pp. 3-4. doi: <https://doi.org/10.11610/Connections.18.3-4.01>.
- [23] Kennedy, M. & Renken, J. (2025). Preparing for the next conflict: How NATO is fortifying its defenses. Wilson Center. Available at: <https://www.wilsoncenter.org/article/preparing-next-conflict-how-nato-fortifying-its-defenses> (Accessed: February 7, 2025).
- [24] Larsen, H. (2024). *Europe's contribution to NATO's new defense*. Eastern Europe Studies Centre. Available at: <https://www.eesc.lt/en/publication/europes-contribution-to-natos-new-defense/> (Accessed: January 31, 2025).
- [25] Loorents, N. (2024). *NATO's Regional Defence Plans*. Washington Summit Series No. 5. International Centre for Defence and Security. Available at: chrome-extension://efaidnbmninnbpcajpcglclefindmkaj/https://icds.ee/wp-content/uploads/dlm_uploads/2024/07/No-5_NATOs-Regional-Defence-Plans_NeLe-Loorents.pdf (Accessed: February 6, 2025).
- [26] Monaghan, S., Jakobsen, E., Martinez, S., Droin, M., Sanders, G., Velazquez, N., Cook, C., Dowd, A., & Sockwell, M. (2024). *Is NATO ready for war?* Center for Strategic and International Studies. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-06/240611_Monaghan_Ready_War_0.pdf (Accessed: January 26, 2025).
- [27] Nasirov, E. & Iskandarov, K. (2017). The prospects of Azerbaijan to enhance military interoperability with NATO. *Connections*, 16(4), pp. 89-99. Available at: <https://www.jstor.org/stable/26867928> (Accessed: January 12, 2025).
- [28] NorthAtlanticTreatyOrganization. (2018). The NATO command structure. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/1802-factsheet-nato-command-structure_en.pdf (Accessed: January 30, 2025).
- [29] North Atlantic Treaty Organization. (2023). NATO Response Force. NATO. Available at: <https://www.nato.int/cps/>

- en/natohq/topics_49755.htm
(Accessed: January 12, 2025).
- [30] Palmer, D. A. R. (2019). NATO's post-Cold War "out-of-area" pivot (1990-2014). In *A Strategic Odyssey: Constancy of Purpose and Strategy-Making in NATO, 1949-2019* (pp. 73–90). NATO Defense College. doi: <http://www.jstor.org/stable/resrep19967.11>
- [31] Sadiyev, S. & Iskandarov, K. (2018). The evolution of the security environment in the South Caucasus since the end of the Cold War, *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, 14/2018, pp. 47-53. Available at: https://www.academia.edu/37852657/_What_a_New_European_Security_Deal_could_mean_for_the_South_Caucasus_
(Accessed: 01.02.2025).
- [32] Shea, J. (2012). *Keeping NATO Relevant*. Carnegie Moscow Center. doi: <http://www.jstor.org/stable/resrep26708>
- [33] STRIKFORNATO. (2024). NATO Assumes Command of U.S. and British Forces in Eastern Mediterranean. Naval Striking and Support Forces NATO. Available at: <https://www.c6f.navy.mil/Press-Room/News/Article/3686562/nato-assumes-command-of-us-and-british-forces-in-eastern-mediterranean/> (Accessed: February 6, 2025).
- [34] Szenes, Z. (2023). Reinforcing deterrence: assessing NATO's 2022 Strategic Concept. *Defense & Security Analysis*, 39(4), pp. 539–560. Available at: <https://doi.org/10.1080/14751798.2023.2270230>
(Accessed: January 11, 2025).

BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE FOR ENHANCED INFORMATION SECURITY IN MILITARY COMMUNICATION SYSTEMS

Fiodor TIMERCAN

“Alexandru cel Bun” Armed Forces Military Academy,
Republic of Moldova

Emerging technologies such as blockchain and artificial intelligence (AI) are reshaping the landscape of military information security. Blockchain ensures data integrity, prevents unauthorized modifications, and establishes decentralized trust across sensitive communication networks. In parallel, AI enhances cyber defense by enabling advanced anomaly detection, predictive analysis, and automated response to potential intrusions. The combined use of these technologies increases the confidentiality, integrity, and availability of information in command and control systems. Practical applications include secure message exchange, distributed authentication, and early threat identification supported by machine learning. Key challenges remain in areas such as scalability, interoperability, and the efficient use of limited resources within military infrastructures. By integrating blockchain and AI, defense forces can strengthen information resilience, reduce cyber vulnerabilities, and maintain a technological edge in an increasingly contested digital battlespace.

Key words: *blockchain, artificial intelligence, information security, military communications, data integrity, predictive analysis.*

INTRODUCTION

Modern military operations rely on the rapid exchange of accurate and secure information. Commanders, intelligence officers, and operators depend on communication systems that function reliably under cyberattacks, electronic interference, and the physical constraints of the battlespace. As adversaries develop

more advanced capabilities in cyberspace, protecting data and communications has become a central component of national defense. Sophisticated intrusion methods, insider risks, and data manipulation attempts require adaptive, intelligent, and decentralized defense solutions.

Blockchain provides an immutable and verifiable record of transactions and message exchanges,

reducing the risk of data alteration and enhancing trust in distributed systems. AI, through machine learning and behavioral analysis, supports early anomaly detection, predictive threat assessment, and rapid decision-making during cyber incidents [11], [30]. Recent years have seen a growing number of studies and pilot programs exploring this convergence in defense applications, such as NATO's *Emerging and Disruptive Technologies Initiative*, the *British Army's Approach to Artificial Intelligence (2023)*, and the *U.S. Army Data Strategy (2020)*, all emphasizing secure data exchange and AI-assisted situational awareness in joint and coalition operations [3], [18].

Successful integration of these technologies also depends on the training and readiness of personnel who operate, maintain, and interpret AI - and blockchain-based systems. Military communicators, cybersecurity specialists, and system administrators must acquire new technical skills in distributed ledger management, data analytics, and AI model validation. Training programs developed under NATO's innovation initiatives and national defense education frameworks demonstrate the importance of aligning technological adoption with human competencies and doctrinal understanding [15], [17], [29].

Integrating blockchain and AI into military communication

systems thus enhances cyber defense, transparency, and decision superiority across all levels of command. Collaboration among defense research institutions, academia, and the private sector remains essential to adapt these technologies to operational requirements and governance frameworks. Together, blockchain and AI form the foundation for next-generation military communication systems designed to sustain secure, uninterrupted, and trusted information exchange across all domains of warfare.

2. BACKGROUND AND RELATED WORK

Information security has always been a decisive factor in the success of military operations. From encrypted radio transmissions to satellite communication systems, the armed forces have continuously adapted to maintain control over the information domain. However, as digital transformation accelerates, the amount of data exchanged across defense networks has grown exponentially, creating new vulnerabilities and expanding the attack surface available to adversaries.

Blockchain technology emerged as a promising response to these challenges. Its decentralized, tamper – resistant architecture enables secure verification of mission data and communication records without

reliance on a single point of failure. In defense environments, blockchain can support secure message exchange, identity management, logistics tracking, and mission data integrity. Field studies and policy papers, such as the European Defence Agency's *Blockchain in Defence* report (2018), Finabel's *Blockchain in Defence: A Breakthrough* (2020), and NATO's *Technology Strategy towards 2030*, demonstrate increasing interest in operationalizing blockchain for verifiable audit trails, decentralized authentication, and resilience enhancement [7], [8], [13].

Artificial intelligence, in parallel, provides the ability to process large data volumes in real time and detect anomalies within complex communication networks. Machine learning models and AI-driven analytics support intrusion detection, predictive threat assessment, adaptive encryption, and autonomous incident response. Recent military applications include NATO's *AI Strategy* (2024), the UK Ministry of Defence's *Defence Artificial Intelligence Strategy* (2022), and ongoing U.S. Army initiatives on data-centric decision-making under the *Army Data Strategy* (2020). These programs validate the feasibility of integrating AI-enabled security mechanisms within tactical networks operating under high latency, limited bandwidth, and intermittent connectivity [29], [30].

The combination of blockchain and AI thus offers a complementary and mission-relevant approach: blockchain secures data integrity and provenance, while AI enhances situational awareness, automates anomaly detection, and optimizes response time. Together, they support a layered cyber defense architecture that is both dynamic and resilient. Case studies within NATO's cyber range exercises and EU defence innovation projects highlight early-stage deployments of hybrid blockchain – AI frameworks to protect command and control data and authenticate unmanned platforms under constrained network conditions [15], [17], [18].

3. INTEGRATION FRAMEWORK FOR SECURE MILITARY COMMUNICATIONS

The integration of blockchain and artificial intelligence (AI) within military communication systems aims to establish a resilient, intelligent, and self-adaptive defense architecture. Such a framework enhances both technical and operational dimensions of information security, ensuring that data remains protected, verifiable, and reliable across all echelons of command, even in contested or degraded environments.

The framework combines the decentralized trust of blockchain with AI's analytical and predictive capabilities. Blockchain records

every validated communication in an immutable ledger, while AI monitors network behavior and triggers automated defensive actions [11], [13]. Pilot projects under NATO's Emerging and Disruptive Technologies and the European Defence Agency's Blockchain in Defence initiative have demonstrated these concepts in secure message authentication and cyber resilience exercises [7], [17], [18].

3.1. System Components

The framework consists of three main layers:

Data Integrity Layer (Blockchain Core): Maintains a tamper-proof log of all communication events and authentication records. Each node contributes to consensus validation, ensuring transparency and reliability.

Cognitive Security Layer (AI Engine): Uses machine learning and behavioral analytics to detect intrusions, assess risks, and recommend responses. The AI component can adapt based on previous incidents, improving system performance over time.

Command and Control Interface: Connects the technical infrastructure to decision-makers. It provides situational awareness dashboards, alert systems, and automated reporting functions that support operational command structures. Prototype systems tested within the NATO Communications and Information Agency's cyber range

environment demonstrated improved decision cycles and reduced operator workload [17], [19], [29].

3.2. Operational Advantages and Training Considerations

Integrating blockchain and AI strengthens the Confidentiality, Integrity, and Availability (CIA) triad central to military cybersecurity doctrine. Blockchain provides decentralized trust and immutability, while AI improves detection speed, decision accuracy, and adaptive resilience. Together, these technologies enable semi-autonomous defense systems capable of maintaining communication integrity even under jamming, latency, or partial network degradation [5], [16], [21].

Beyond security, the framework enhances interoperability among allied forces through standardized data exchange, cross-domain authentication, and federated situational intelligence. NATO and EU-led demonstration projects have shown that distributed trust mechanisms significantly reduce data synchronization delays between coalition partners. Equally critical are *training and personnel readiness*. Operators must understand distributed ledger structures, AI decision processes, and human-machine teaming principles to maintain trust in semi-autonomous systems. NATO's Defence Innovation Accelerator for the North Atlantic

(DIANA) and national military academies have introduced technical training modules on blockchain-based identity management and AI-driven network defense [15], [17], [29].

4. PRACTICAL APPLICATIONS AND USE CASES

The integration of blockchain and artificial intelligence (AI) in defense communication networks provides tangible operational benefits, enabling trusted data exchange, automated cyber defense, and resilient decision-making. These technologies have already been tested in military pilot programs such as NATO's *Emerging and Disruptive Technologies* trials and the U.S. Army's *Data Strategy* implementation, which explored AI-assisted network monitoring and blockchain-based authentication in field environments.

4.1. Secure Message Exchange

In military communications, confidentiality and authenticity are paramount. Blockchain can act as a secure backbone for exchanging orders, intelligence updates, and mission reports between command units, field operators, and unmanned platforms. Each transmission is cryptographically signed and stored as a blockchain transaction, ensuring traceability even under jamming or interception attempts.

AI enhances this capability by analyzing message flows to detect

spoofing or signal manipulation. NATO's cyber range exercises have demonstrated that AI-assisted blockchain verification significantly reduces false data injection during simulated electronic warfare [15], [17].

4.2. Distributed Authentication and Access Control

Conventional authentication systems depend on centralized servers, vulnerable to compromise or denial-of-service. Blockchain distributes identity verification across trusted nodes, reducing single points of failure and ensuring continuity of access in contested domains.

When combined with AI-based behavioral analytics, the system dynamically identifies irregular access attempts or insider threats. This hybrid model has been evaluated in the British Army's AI experimentation framework to support coalition operations and secure remote access for deployed units [3], [29].

4.3. Intelligent Threat Detection and Response

AI enables real-time anomaly detection and predictive response, essential for maintaining mission continuity during cyber incidents. Machine learning models trained on operational data can autonomously isolate compromised nodes, reroute traffic, and alert operators.

Blockchain complements this process by recording every incident

and response action immutably, ensuring forensic traceability and accountability for command review. Field applications under NATO's Cooperative Cyber Defence Centre have confirmed the efficiency of this combined approach for incident auditing and rapid recovery [16], [18].

4.4. Mission Data Integrity and Auditability

Mission-critical data, such as sensor readings, situational updates, and mission logs, must remain verifiable across all command tiers. Blockchain guarantees the integrity of these records, while AI verifies data consistency and identifies anomalies in near real time.

This integration has been tested in EU research programs on secure logistics and intelligence sharing, where AI-supported ledgers prevented misinformation propagation and improved decision reliability under constrained connectivity [8], [17].

4.5. Operational Benefits and Challenges

Integrating blockchain and AI provides several operational advantages:

Increased Trust: Every data exchange is verifiable and auditable.

Faster Response: AI enables early threat detection and automated counteraction.

Decentralized Security: Reduces vulnerability to single-point failures.

Improved Interoperability: Facilitates secure collaboration between allied forces.

Enhanced Decision-Making: Provides real-time intelligence and system transparency.

Yet, deployment in tactical environments remains constrained by limited bandwidth, computing power, and energy availability. Lightweight consensus mechanisms, compressed AI models, and edge-based processing are essential for operational feasibility.

Equally important is the training of personnel tasked with operating and supervising these systems. NATO's DIANA and national military academies have initiated technical education tracks focused on AI ethics, blockchain management, and autonomous system oversight to ensure safe and doctrinally aligned use [15], [17], [29].

As technologies mature and doctrine adapts, blockchain and AI are expected to become core components of next-generation defense communication infrastructures, ensuring cyber resilience and mission assurance across all domains of warfare.

5. CONCLUSIONS

Blockchain and artificial intelligence (AI) are transforming the security architecture of modern military communication systems. Their combined application enhances data integrity, network

resilience, and real-time decision support, capabilities essential for maintaining operational superiority in the information domain.

Field experiments and research initiatives under NATO, the European Defence Agency, and the U.S. Army have already validated the potential of blockchain-based authentication and AI-assisted threat detection for improving cyber defense efficiency and interoperability in coalition environments. These case studies demonstrate that the fusion of distributed trust and cognitive analytics can sustain mission-critical communications even in degraded or contested networks.

However, effective deployment in tactical environments must address key *resource constraints* such as bandwidth limitation, processing capacity, and energy availability. Adaptive consensus algorithms, compressed AI models, and federated learning architectures offer viable solutions to ensure performance at the tactical edge.

Equally crucial is the *training and readiness* of military personnel responsible for operating these systems. New competencies are required in blockchain management, AI model interpretation, and cyber ethics. NATO's Defence Innovation Accelerator (DIANA) and national defense academies are already developing targeted training programs to integrate these skills into doctrine and operations [15], [17], [29].

In conclusion, the convergence of blockchain and AI establishes the foundation for next-generation secure, autonomous, and resource-aware defense communication networks. Continued collaboration between military institutions, academia, and industry will be essential to translate technological maturity into doctrinally aligned, operationally proven capabilities that enhance information dominance and mission assurance across all domains of warfare.

REFERENCES

- [1] Army University Press, "Modernizing Military Decision-Making: Integrating AI into Army MDMP" *Military Review (Online Exclusive)*, 2025.
- [2] P. Bagga, M. Dave, A. K. Dutta, and M. Chhabra, "Blockchain-envisioned access control for IoT-based healthcare systems" *Complex & Intelligent Systems*, vol. 8, pp. 1723–1740, 2022.
- [3] British Army, "British Army's Approach to Artificial Intelligence" 2023.
- [4] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks" *IEEE Computer*, vol. 36, no. 10, pp. 103–105, 2003.
- [5] ENISA, "Threat Landscape 2024," *European Union Agency for Cybersecurity*, 2024.
- [6] European Commission, "Coordinated Plan on Artificial Intelligence 2021 Review" 2021.
- [7] European Defence Agency, "Blockchain technology in defence" *European Defence Matters*, 2018.

- [8] Finabel, “*Blockchain in Defence: A Breakthrough*” 2020.
- [9] P. Kairouz et al., “*Advances and Open Problems in Federated Learning*” *Foundations and Trends in Machine Learning*, vol. 14, nos. 1–2, pp. 1–210, 2021.
- [10] D. W. Korsak, “*Decrypting Bitcoin and Blockchain for Military Lawyers*” *The JAG Reporter*, 2021.
- [11] I. Kotenko, I. Saenko, A. Branitskiy, and Y. Saenko, “*Survey of Intrusion Detection Systems for Cyber-Physical Systems*” *Sensors*, vol. 21, 2021.
- [12] N. Kshetri, “*The Emerging Role of Big Data in Key Development Issues*” in *Big Data for Development*, Palgrave, 2014.
- [13] R. Kumar and R. A. Khan, “*Securing military computing with the blockchain*” *Computer Fraud & Security*, 2024.
- [14] H. B. McMahan, D. Ramage, and A. Talwalkar, “*Federated Learning: Challenges, Methods, and Future Directions*” *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.
- [15] NATO, “*Summary of NATO’s Revised Artificial Intelligence Strategy*” 2024.
- [16] NATO, “*Cyber defence*,” 2024.
- [17] NATO, “*Emerging and Disruptive Technologies*” 2025.
- [18] NATO ACT, “*Digital Transformation*” 2025.
- [19] NATO Communications and Information Agency, “*Technology Strategy towards 2030*” 2023.
- [20] NCSC, “*Zero Trust Architecture Design Principles*” 2023.
- [21] NIST, “*Artificial Intelligence Risk Management Framework (AI RMF 1.0)*” 2023.
- [22] NIST, “*GenAI Profile for the AI RMF (NIST.AI.600-1)*” 2024.
- [23] NIST, “*Zero Trust Architecture (SP 800-207)*” 2020.
- [24] P. Papadopoulos, S. Diamantopoulos, D. Papadopoulos, and E. Panaousis, “*Blockchain for Secure and Trusted Communication in IoT: A Survey*” *Computer Networks*, vol. 179, 2020.
- [25] I. Politis and P. Kotzanikolaou, “*Security and Privacy for Tactical Wireless Sensor Networks: A Survey*” *Computer Networks*, vol. 147, pp. 134–159, 2018.
- [26] J. Shao, C. You, Y. Sun, Q. Yang, and K. Huang, “*A Survey of What to Share in Federated Learning*” *ACM Computing Surveys* (preprint), 2023.
- [27] J. S. Shor, M. Refaei, H. Saddik, and A. Boukerche, “*Anomaly Detection in Network Traffic: A Survey*” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 303–336, 2014.
- [28] S. Singh and N. Singh, “*Blockchain: Future of Financial and Cyber Security*” *Procedia Computer Science*, vol. 132, pp. 147–152, 2018.
- [29] Y. Sun, Y. Li, S. Wang, Q. Cao, and Z. Han, “*Integrating Blockchain with 6G: A Survey of Challenges and Opportunities*” *IEEE Network*, vol. 35, no. 4, pp. 160–167, 2021.
- [30] UK Ministry of Defence, “*Defence Artificial Intelligence Strategy*” 2022.
- [31] US Army, “*Army Data Strategy*” 2020.
- [32] W. Wu, C. Tan, K. Yang, Z. Shen, Q. Zheng, and J. Jin, “*A Sharded Blockchain-Based Secure Federated Learning Framework for LEO Satellite Networks*” *arXiv preprint*, 2024.

DIGITAL SHIELD: INTEGRATING HEALTH INTELLIGENCE INTO NATO'S DEFENSE STRATEGY

Dimitra BALASKA*, Dimitris KARAFERIS*,

Ioannis REMATISIOS*, Yannis POLLALIS*

*Department of Economic Science-iLEADS Lab,
University of Piraeus, Piraeus, Greece

The COVID-19 pandemic and Russia's war against Ukraine have reshaped how security is perceived, exposing the interdependence of health, defence and digital infrastructures. National security must therefore broaden to include health resilience as a core operational priority. As NATO and the EU move forward with digital transformation, embedding health intelligence becomes essential for readiness, force protection and civil–military cooperation. This paper argues that real-time health data, wearable devices and AI-enabled surveillance can support not only responses to biological threats but also anticipation of vulnerabilities before they escalate. By shifting from reactive to proactive postures, NATO and the EU can build more resilient and human-centred security frameworks adapted to hybrid warfare. Recognising health systems as critical infrastructure, alongside energy and transport, makes integration a strategic necessity. Doing so will shape the credibility, adaptability and resilience of NATO and the EU in decades ahead, strengthening security in an increasingly complex environment.

Key words: health intelligence integration, hybrid security threats, biosecurity, health & safety, quality in health care.

1. INTRODUCTION

The COVID-19 pandemic and the war in Ukraine have revealed something very important: health is no longer distinct from security and defense. When issues of national sovereignty or biological threats arise, defense is immediately

affected. These new realities drive NATO and the EU to quickly embrace the idea of digital transformation. Digital transformation in defense is not just about using better technology. It is about creating smarter, faster, and more integrated systems that help both military and

civilian organizations make better decisions. This includes using real-time data, artificial intelligence, and secure communication platforms that can support everything from military operations to public health emergencies (Anghel and Jones, 2023; Fiott, 2023; Csernatoni and Martins, 2024).

While the term "digital transformation" used broadly, its true meaning goes beyond just adopting new technologies or digitizing old processes. Digitization, converting analog data into digital format, is just the first step. True digital transformation involves redesigning how organizations work, how decisions are made, and how people interact with systems. It is not just about emails, dashboards, modernization or AI deployment. Instead, digital transformation is about building secure, flexible, and interconnected systems that bring together real-time data from various sources. These systems help make faster, better decisions by integrating everything from cloud infrastructure and APIs to AI, sensors, and next-gen communications. For NATO and the EU, this means rethinking how data managed across defense forces, from logistics to battlefield intelligence to health monitoring, and turning it into a strategic asset. Ultimately, digital transformation is about making defense smarter, faster and more responsive, not just through

technology but through cultural, organizational, and procedural change. It is a journey toward an adaptive, data-driven defense model that supports both operational effectiveness and the well-being of personnel. Nevertheless, NATO pursues three additional core tasks in addition to collective defense, namely crisis prevention, management and cooperative security. It may encompass both military and non-military strategies to tackle the entire range of crises—prior to, during, and following conflicts, as well as in reaction to natural disasters, acts of terrorism, technological disturbances, public health crises, or any other situation that could jeopardize the security of Allied nations (Burwell, 2020; Ilangakoon et al., 2022; Mauro et al., 2024).

National initiatives to prioritize the digital transformation of defense and ongoing efforts within NATO and the EU are a step in the right direction. However, the current conception and planning of defense digitalization within national capitals and the two organizations – NATO and the EU – is insufficiently understood, overly incremental, and lacks the necessary scope to transform European defense at a pace that is relevant. Despite the policy narrative acknowledging "the urgency of a digitally-transformed Alliance," NATO's development of its digital transformation agenda has been years in the making.

Furthermore, its implementation process, linked to capability development, is a decades-long effort where 2030 (for NATO, even later for individual allies) is merely the first milestone for basic capability levels. Both NATO and the EU seem to have resigned themselves to a "fast-follower" approach to digitalization, where neither states nor the EU or NATO are leading the way in the digital transformation of defense, but instead responding to much larger structural shifts in the digital revolution within industry. Europe's efforts to transform its defense and become a competitive and credible defense actor are not progressing fast enough. Its poor track record on defense digitalization over the past few decades suggests that its defense leadership has not fully embraced the challenge. Europe has persisted with an approach to digital transformation which characterized by incrementalism and selective implementation. It has done so even in the face of strategic threats to European defense, most notably the aggression from Russia in its war against Ukraine, demonstrating a degree of strategic paralysis in Europe. These challenges are not only affecting military readiness but also the overall health of European defense systems, including the ability to adapt to technological advancements and address critical security and health-related issues

that arise in the digital age (Gilli, 2020; Fasola, 2024; NATO's strategy for digital transformation, 2024).

In recent years, NATO and the EU have both adopted ambitious digital strategies. But while the focus is often on weapons systems or cyber security, there is growing recognition that health intelligence must be part of this transformation. Health data, collected through wearables, field diagnostics, and surveillance systems, can help anticipate crises, protect personnel, and support civil-military cooperation in times of need. Health is becoming an operational concern. Beyond its role in crisis response, robust health data enables better planning, enhances troop readiness, and strengthens supply chains. The ability to predict and respond to biological risks, mental health strain, or logistical gaps in medical support can dramatically impact operational outcomes. As NATO and the EU move forward with their digital ambitions, integrating health intelligence will be essential for creating a comprehensive, human-centered security strategy (Bricknell M. *et al.*, 2020; Mesterhazy, 2020; Policy Department, 2021).

As The COVID-19 pandemic has highlighted the significance of biological agents as a distinct threat vector that poses a risk to the security of NATO member states. This study examines the potential for a more profound integration of health intelli-

gence within NATO's digital defense strategy, particularly in relation to the requirements for medical military support. By doing so, we contend that NATO has the potential to develop a more robust, agile, and adaptable strategy for contemporary security, wherein digital technologies not only improve military effectiveness but also collectively security safeguard the health and welfare of service members and the civilians they are committed to protecting.

2. DEFINING HEALTH INTELLIGENCE AND INTEGRATION CRITERIA

Health intelligence (HI) is widely understood as the systematic collection, analysis and interpretation of data about health, health systems, health threats and the wider determinants of health for the purposes of decision-making and resource allocation. The World Health Organization (WHO) notes that health intelligence involves the systematic collection and analysis of data on health, health systems, health threats and wider determinants of health, while the PanAmerican Health Organization defines it as the analysis of population health, health system performance and health research (Haby *et al.*, 2023). In military contexts, medical intelligence is defined as the collection, evaluation and analysis of foreign medical, bio-scientific and environmental information that informs strategic

planning and medical operations (Bowsher, Milner and Sullivan, 2016). In this paper, the term health intelligence encompasses both public health intelligence and military medical intelligence; it refers to the capability to gather and synthesize timely health-related information in order to protect personnel, anticipate threats and inform operational planning.

To evaluate the successful integration of health intelligence across defense, healthcare and civil-military organizations, we propose several indicative criteria. First, organizations must be able to capture and share multi-sectoral data, including private-sector metrics and subnational capacities, in near real time. Second, the availability and capacity for electronic surveillance and high-quality data must be assessed, including timeliness of routine reporting and data quality scores. Third, integration readiness can be measured by the existence of digital infrastructures and trained personnel capable of collecting, analyzing and disseminating health intelligence across agencies. Fourth, tracking indicators such as internally displaced persons, returnees and other vulnerable groups improves preparedness, as emphasized by public health experts (Erondu *et al.*, 2021). Together these criteria provide a starting point for evaluating the maturity of health intelligence integration.

3. NATO'S DIGITALIZATION OF DEFENSE: PROGRESS AND CHALLENGES

Digitalization in defense is steadily gaining momentum within NATO. In October 2022, Alliance leaders officially endorsed a vision for digital transformation and approved the NATO Data Exploitation Framework Policy (DEFP). This was followed in July 2023 by the adoption of the Digital Transformation Implementation Strategy, which aligns digital transformation milestones with NATO's capability development objectives and interoperability standards. NATO views digital transformation as a fundamental enabler and driver of seamless integration across domains, facilitating Multi-Domain Operations (MDO). As noted by NATO's Digital Transformation Champion and Special Advisor Didier Polomé, the goal is that by 2030, NATO's digital transition will empower the Alliance to execute MDO, ensure interoperability across all operational areas, enhance situational awareness, and support both political consultations and data-driven decision-making. This strategy is rooted in NATO's operational requirements outlined in a range of strategic documents, such as the 2019 Military Strategy, the Warfighting Capstone Concept, the evolving MDO concept, the AI Strategy, and the DEFP. These documents collectively set the path

for NATO's shift toward multi-domain operational capabilities by 2030. Beyond the military dimension, digital transformation is intended to be fully integrated with NATO's Defence Planning Process, capability development targets, standardization efforts, R&D, procurement processes, and high-tech initiatives like DIANA (Defence Innovation Accelerator for the North Atlantic) (NATO, 2021, 2023b, 2023a, NATO STO SET Panel, 2022; Soare, 2023).

As shown in the associated Figure 1, the transformation rests on five core components and three structural pillars. Key technologies include cloud computing, a modular open-system digital infrastructure, a federated synthetic environment, and a smart data fabric that facilitates the processing and sharing of data across platforms and users. Cybersecurity addressed through a "zero trust" approach. However, the greatest challenge may lie not in technology, but in fostering a culture that promotes innovation, experimentation, information sharing, and responsible risk-taking by both American and European companies. This requires a culture change from leaders/governments and decision makers, as they are usually not willing to accept early failures in collaborative R&D initiatives to stay ahead of the innovation curve against their competitors. The return on investment (ROI) for defense technologies at initial TRL levels is

mostly intangible, while Member States usually aim for tangible results (through industrial benefits). This shift also demands a digitally literate workforce, and NATO estimates that by 2030, at least 10% of its personnel must have digital competencies, representing a fivefold increase from current figures (NATO STO SET Panel, 2022; Soare, 2023; Shaun Cannon, 2024, NATO Reflection Group, 2020; Rauch et al., 2024).

While the scale of NATO's digital strategy is ambitious, concerns persist around the complexity of its implementation and the internal division of responsibilities. Operational leadership lies with Allied Command Transformation and Allied Command Operations, while agencies like the NATO

Communications and Information Agency, NATO Support and Procurement Agency, and the Alliance CIO provide support. Political and policy coordination is driven by NATO's International Staff, including the CIO, the Emerging Security Challenges Division, and the Consultation, Command and Control Board. Despite this structure, internal collaboration has occasionally faltered, creating additional hurdles. Furthermore, digital transformation is seen as a continuous modernization process, with 2030 serving as a major milestone. However, the pace of progress remains a concern. Developing digital capabilities in Europe typically takes two to three years for concept development, with procurement often doubling or



Fig. 1 Pillars and building blocks of NATO's Digital Transformation to enable multi-domain operations (Soare, 2023)

tripling that timeline. Full delivery of digital solutions can require an additional three to four years, if not longer. Consequently, a comprehensive digitalization effort in European defense may span over a decade (Haddud and McAllen, 2018; Oberländer, Beinicke and Bipp, 2020; Fiott, 2023, Wolff, 2025).

Consequently, without urgent reforms to streamline procurement, align budgets and defense planning, and dramatically boost digital expertise within both NATO and national defense sectors, achieving the Alliance's 2030 digitalization goals remains unlikely. While incremental improvements may be achieved, the European pillar of NATO is expected to face significant difficulty meeting its digital transformation targets on time (Soare, 2023; Cannon S, 2024; NATO, 2024; NATO Reflection Group, 2020; Fiott, 2023a; Rauch et al., 2024; Haddud and McAllen, 2018; Oberländer, Beinicke and Bipp, 2020; Caliskan and Liégeois, 2021; Wolff, 2025).

4. BUILDING TECHNOLOGICAL SOVEREIGNTY THROUGH HEALTH: EU PROGRESS, CHALLENGES, AND NATO CONVERGENCE

The European Union has made notable progress in enhancing its strategic and technological sovereignty, particularly in the areas of health and security. Since

2019, the European Commission, in collaboration with Member States, has been shaping a robust agenda for the digital transformation of health systems across Europe (Burwell, 2022; Lantzsch *et al.*, 2022; Bocean and Vărzaru, 2025). The emphasis on technological and digital sovereignty, which are essential elements of the EU's strategic autonomy as digitalization gains significance for geopolitical influence and economic objectives, has intensified under the von der Leyen Commission. This focus has emerged in response to the rising significance of the data economy, escalating worries regarding the dominance and power centralization among a limited number of non-EU technology firms, and the potential reliance on external technologies, vital infrastructure, digital services, and the management and safeguarding of data from foreign entities. Key EU bodies, such as the Directorate-General for Health and Food Safety (DG SANTE), the Directorate-General for Communications Networks, Content and Technology (DG CONNECT), and the European Health and Digital Executive Agency (HaDEA), play a central role in advancing various facets of digital health. Their efforts supported through multiple EU-level funding mechanisms, including (Burwell, 2022; Lantzsch *et al.*, 2022; Bocean and Vărzaru, 2025; Odone *et al.*, 2019; Fahy N, 2021; Orăștean,

Sava and Mărginean, 2022; Crespi *et al.*, 2021; Ruohonen and Timmers, 2025; Madiega, 2020; Gallo *et al.*, 2021; Baroncelli, 2024):

- ▶ *EU4Health Programme*: With a €5.3 billion budget for 2021–2027, this programme aims to strengthen health systems and foster digital health transformation.
- ▶ *Digital Europe Programme*: Supports projects in AI, cyber-security, and digital innovation across the EU.
- ▶ *Horizon Europe*: The EU's key research and innovation programme, which includes health-related actions to improve citizens' well-being and care.
- ▶ *Recovery and Resilience Facility (RRF)*: Part of the NextGenerationEU plan, financing reforms and investments including those in digital health.
- ▶ *European Regional Development Fund (ERDF)*: Supports infrastructure and service investments, including digital health initiatives, to promote economic and social cohesion.

In 2019, Finland and Estonia took the lead in advancing digital health integration within the EU, becoming the first member states to enable cross-border electronic prescriptions and patient data exchange. During

Finland's Presidency of the Council of the European Union that same year, the strategic agenda placed strong emphasis on the digitalization of healthcare systems and the adoption of artificial intelligence (AI) to modernize health services. The focus was on creating interoperable digital infrastructures and fostering public-private partnerships to support innovation, enhance citizen wellbeing, and build resilience in European health systems. These early initiatives laid the groundwork for broader EU-level discussions on the integration of emerging technologies, such as AI, into healthcare frameworks and policy planning (Niño Sevilla Palma, 2021; Bocean and Vărzaru, 2025).

Despite progress, significant challenges remain. The European Court of Auditors has noted the complexity in tracking digital health funding and highlighted bureaucratic obstacles that limit the effective access to funds by some Member States. Moreover, while initiatives such as the EHDS promote interoperability and data sharing, critical gaps persist in areas such as cryptography, cloud infrastructure, and next-generation communications. The **EU Strategic Compass** has reaffirmed the importance of investing in digital and emerging technologies as one of the Union's four strategic priorities in health. NATO has also expressed increasing interest in the convergence

of health and digital defense capabilities, particularly considering evolving hybrid threats. However, the EU's investment in digital health transformation currently surpasses NATO's in scope and funding. The management and funding of such new initiatives within NATO are primarily overseen and financed by DIANA and NIF, in close collaboration with the well-established SPS programme. This enhances the partnership between civilian science and technology (S&T) and creates extensive synergies involving NATO OCIO, NCIA, STO panels, academic institutions, and National Research Centers. The focus is on specific areas such as cyber, artificial intelligence, health, climate, and energy, which operate at various classification levels. There is a clear plan aimed at achieving tangible outcomes that lead to innovative solutions, which can be measured and justified to the member nations. DIANA serves as the innovation accelerator, linking innovators globally and utilizing test centers and accelerator sites to create solutions that meet NATO's operational needs, including health intelligence. Meanwhile, the NATO Innovation Fund (NIF) represents the first multi-sovereign venture capital fund dedicated to fostering the development of dual-use technologies that benefit both civilian and military sectors. Yet, implementation within the EU

remains slower and more fragmented. The prioritization of the EU Rapid Deployment Capacity (RDC) further suggests that digital health efforts are still narrowly aligned with specific operational needs, rather than system-wide transformation (Bente *et al.*, 2024; Gaeta *et al.*, 2025).

While the EU has established strong institutional frameworks and funding tools for advancing digital health, coordinated and intensified efforts needed to overcome persistent gaps and ensure the effective implementation of digital health strategies across all Member States. Enhanced civil-military collaboration, including shared lessons with NATO, will be essential to building resilient and technologically sovereign health systems for the future (Bachmann, 2011; Fahy N, 2021).

NATO's Digital Transformation Implementation Strategy emphasizes multi-domain operations, alliance-wide interoperability and data-driven decision-making (NATO, 2023b). It focuses on building a digital backbone, data-sharing ecosystems, synthetic environments and a digitally ready workforce. By contrast, the EU's digital health agenda seeks to achieve technological and data sovereignty, investing heavily in public-sector infrastructure through programmes such as EU4Health, the Digital Europe Programme and the Recovery and Resilience Facility

(Sylvia N., 2025). The EU prioritizes cross-border e-health services, interoperable standards and national digital health ecosystems. These approaches are complementary. NATO's emphasis on operational interoperability and defense planning can benefit from the EU's investments in civilian health infrastructure, while EU initiatives on digital sovereignty and health data spaces can feed into NATO's data exploitation frameworks. Recognizing these synergies can help avoid duplication, align priorities and enhance collective security.

An instructive example of successful integration can be found in Estonia. The country has built a nationwide digital health information system that securely connects hospitals,

clinics, pharmacies and citizens through the X-Road data-exchange platform. As a result, 99 % of patients in Estonia have digital health records and 100 % of prescriptions are issued electronically; the e-Health portal supports millions of queries each year (Enterprise Estonia, 2025). Estonia's Health Information System (EHIS) integrates data from birth to death and provides clear governance, legal clarity and agreed access rights for different actors (J.Metsallik *et al.*, 2018). This integrated infrastructure enables near-real-time health monitoring and improves decision-making for both civilian and military planners.

Nevertheless, it exposes important privacy and ethical considerations. Implementing AI-enabled health surveillance requires robust data

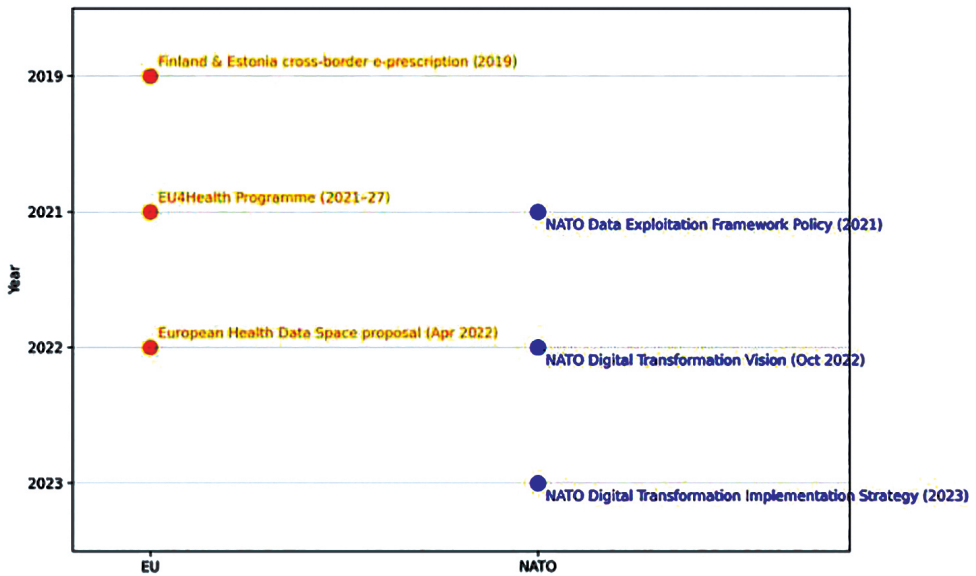


Fig. 2 Chronological milestones of NATO and EU digital transformation and health integration

protection, informed consent, algorithmic fairness, transparency and clear regulatory oversight to ensure public trust (Gerke, Minssen and Cohen, 2020). Estonia's experience also illustrates procurement challenges: replacing legacy systems requires long-term investment and flexible procurement models that prioritize interoperability and open standards. Roles and responsibilities are shared among ministries of health and defense, national cybersecurity agencies, private technology providers and healthcare professionals; establishing clear governance ensures accountability across this ecosystem.

5. EMERGING TECHNOLOGIES AND THE FUTURE OF BIO-DIGITAL THREATS

As NATO charts its trajectory toward 2030 and beyond, the evolving cyber threat environment demands urgent strategic foresight and innovation. Emerging technologies are transforming the operational, tactical, and strategic dimensions of security in cyberspace, reshaping the nature of threats and the methods required to confront them. This transformation is not merely a technological shift but a structural one, where the very architecture of power, deterrence, and resilience are redefined by innovation. Moreover, the forthcoming transformative technological cycle will be propelled

by synthetic biology. Alongside ongoing advancements in associated technological domains (for instance, biodata and biosensors), this trend will elevate concerns such as research security (protecting sensitive research) and regulatory matters to a prominent position. Artificial intelligence, quantum computing, autonomous systems, and the growing interdependence between digital and physical domains converge to create an unstable equilibrium. NATO must prepare for a future in which adversaries exploit speed, ambiguity, and complexity to challenge democratic resilience, strategic cohesion, and military effectiveness (Lucarelli S, 2021). Aside from AI, collaborations between the public and private sectors are crucial to NATO's cybersecurity framework. The private sector, particularly technology firms such as Microsoft, Google, and Cisco, possess the sophisticated technology and threat intelligence capabilities essential for enhancing NATO's defensive stance. This partnership enables NATO to utilize the most effective and up-to-date resources for identifying, alleviating, and addressing threats.

Artificial intelligence (AI) and machine learning (ML) stand at the core of this transformation. These technologies enable faster processing of massive datasets, advanced anomaly detection, predictive threat modelling, and real-time response

automation. While offering remarkable advantages in cyber defense and operational planning, AI also lowers the threshold for executing complex cyberattacks. Adversaries may deploy machine-driven deception, intelligent malware, or autonomous intrusion tools, creating a scenario where human reaction time becomes irrelevant. The danger is not limited to technological superiority but to cognitive asymmetry, where NATO's decision-making processes may lag behind the rapid, AI-enhanced actions of a malicious actor (Ertan A, 2020).

Equally significant is the rise of autonomous and semi-autonomous systems, ranging from unmanned aerial vehicles and robotic platforms to software agents operating in cloud-based infrastructures. These systems increase operational efficiency and reduce human exposure to direct threats, but they also become new targets for cyber intrusion. A compromised autonomous system could be repurposed as a weapon or become part of a coordinated swarm attack. The convergence of autonomy and connectivity introduces vulnerabilities that traditional cybersecurity models are ill equipped to address. The result is a volatile battlespace where the cyber and kinetic realms are increasingly intertwined (Lucarelli S, 2021).

Meanwhile, the rollout of advanced communication's infra-

structure, particularly 5G networks, introduces a broader and deeper digital attack surface. 5G enables massive device connectivity and low-latency data exchange, but it also embeds critical dependencies on software-defined functions, cloud integration, and supplier trust. NATO allies must grapple with the geopolitical implications of technology supply chains and the risks of digital dependencies on non-trusted providers. The security of digital infrastructure is no longer purely technical; it is political, strategic, and transnational. Ensuring the integrity and resilience of communication networks is as vital as defending physical territory (Ertan A, 2020).

Quantum computing, while still in its infancy, poses a looming threat to the cryptographic foundations of modern security. Once scalable quantum machines become operational, they could break widely used public-key encryption schemes, undermining secure communications across military, intelligence, and civilian sectors. The race toward quantum-resistant encryption has begun, but NATO must assume a proactive stance. The Alliance's information assurance models must anticipate the "quantum surprise," investing not only in technological adaptation but also in the human and institutional agility to absorb rapid shifts (Zornetta, 2024). Another

domain of rising concern is the explosive growth of cyber-physical systems and the Internet of Things (IoT), particularly within critical infrastructure. From energy grids and water systems to military logistics and healthcare, increasingly connected environments create complex interdependencies. A cyberattack on one node can cascade across systems, causing widespread disruption or even loss of life. The digitization of society and the militarization of connectivity render cybersecurity not only a technical imperative but also a civilizational one. The protection of public trust, democratic governance, and societal functionality becomes part of NATO's strategic calculus (lessing J, 2021).

Regarding bio-digital threats, NATO has established a network of Centers of Excellence. For example, the Joint Chemical Biological Radiological and Nuclear Defense COE is focused on developing standards and knowledge to enhance interoperability and capabilities among member and partner nations, while maintaining close collaboration with other pertinent COEs, such as the Civil-Military COE, to foster synergies between NATO and the EU through dedicated studies. Simultaneously, the Cooperative Cyber Defense COE located in Estonia serves as a multinational and interdisciplinary cyber defense hub, offering research, training, and

exercises related to cyber technology, strategy, operations, and law. However, there remains significant potential for improvement, particularly in collaboration with EU organizations and agencies like the EDA (and its Technology & Innovation Unit) to better prepare for future hybrid bio-digital threats, including high-impact, low-probability risks that could affect the health systems of both the EU and NATO.

In light of these developments, NATO's concept of deterrence and defense must evolve. Cyber deterrence is inherently different from nuclear or conventional deterrence. It is more ambiguous, harder to attribute, and often operates below the threshold of open conflict. This requires NATO to develop new models of collective resilience, attribution mechanisms, and credible response postures that align with democratic values and international law. Capacity building, information sharing, and real-time coordination among allies will be the backbone of any effective cyber strategy (Lucarelli S, 2021). Ultimately, NATO must embrace a dynamic, forward-looking cybersecurity agenda rooted in technological literacy, strategic foresight, and institutional adaptability. This includes investing in next-generation cyber capabilities, enhancing interoperability among member states, cultivating a skilled

workforce, and fostering innovation through public-private partnerships. In an era defined by digital disruption, the Alliance's strength will depend not only on its military assets but also on its ability to anticipate, absorb, and respond to complex cyber threats with unity and speed (Ertan A, 2020).

6. DIGITAL HEALTH TRANSFORMATION IN EUROPE: CHALLENGES, STRATEGIC INITIATIVES, AND NATO'S ROLE IN SHAPING THE FUTURE OF HEALTHCARE

The digitalization of health is not a recent development in European healthcare systems. The adoption of information and communications technology (ICT) across public health institutions, including the use of secure digital equipment and licensed software outside core hospital infrastructure, has grown exponentially, particularly under the impact of COVID-19 restrictions. Similar trends observed in both NATO and EU health-related initiatives, as most European health systems currently employ at least some level of digital health technologies and enterprise resource planning (ERP) systems. Many also operate partially digitalized healthcare infrastructures and administrative bodies (Bocean and Vărzaru, 2025).

A small number of EU member states are now striving for more

advanced and integrated digital health ecosystems, including real-time data exchange platforms and comprehensive command, control, communications, intelligence, surveillance, and response (C4ISR) systems for health crises. For instance, the United Kingdom is developing a unified and secure 'Digital Backbone' for its National Health Service (NHS), supported by initiatives such as the 'Digital Foundry' and a dedicated 'Digital Function' for healthcare management. This digital transformation aims to replace thousands of outdated legacy systems and applications, serving over 200,000 healthcare personnel across clinical, administrative, and logistical functions. The 2022 Plan for Digital Health and Social Care, along with subsequent health digitalization strategies, reaffirm the UK's commitment to accelerating this shift towards a fully integrated digital infrastructure (M. Honeyman, 2020; Värri, 2020). Similarly, France has established the Health Data Hub (HDH), a national platform designed to facilitate secure and unified access to health data for research and innovation purposes. The HDH aims to consolidate various health databases, enhancing the country's capacity for data-driven healthcare solutions and fostering digital sovereignty in the health sector. This initiative reflects France's commitment to developing a robust

digital backbone for its national health infrastructure (Szeftel *et al.*, 2025). Furthermore, countries such as Estonia, Finland, Italy, the Netherlands, Norway, Spain, and Sweden have also made significant strides in integrating digital technologies into their healthcare systems. For instance, Estonia's implementation of the X-Road platform has enabled seamless interoperability between various health services, while Finland's Digital Health Village provides a comprehensive online portal for patient care. These advancements often involve collaborations with private-sector technology providers, adopting models based on data-, software-, and infrastructure-as-a-service to enhance efficiency and accessibility in healthcare delivery (Vaagan RW, 2021). However, European nations still face substantial obstacles in fully digitalizing their healthcare infrastructures. Most lack fully integrated digital health data management systems or are still in the process of developing them. Many rely on outdated, localized data-storage systems located on-site within hospitals or clinics. Additionally, a large proportion of EU member states struggle to maintain and regularly update their digital health systems. In some cases, security-critical systems have not been upgraded for over a decade, creating major vulnerabilities (Majcherek *et al.*, 2024).

The use of cloud-based healthcare services remains very limited in Europe, with only a few countries, such as France, Germany, and the UK, employing health cloud services at a national level or within federated networks. Although the European Health Fund (hypothetically adapting the EDF) supports projects aimed at cloud-based storage and collaborative digital health networks, less than 1% of cloud-service providers in Europe are European-based companies, raising critical concerns around data sovereignty. Indeed, data sovereignty remains a foundational principle of digital transformation across both EU and NATO health strategies. Despite the availability of technical solutions to safeguard data integrity and ownership, cross-border and cross-sectoral data sharing remains a medium-term challenge for both organizations. For instance, many European health institutions still rely on manual systems for logging staff capacity and equipment readiness. Delays in reporting and updating records on the maintenance of critical medical equipment are common. A recent example is the widespread difficulty EU members faced in providing real-time updates on medical supplies and pharmaceuticals during joint procurement efforts, an initiative that aimed to strengthen EU solidarity in response to the war in Ukraine and its humanitarian health impacts

(Burkadze, 2022; Jain *et al.*, 2022; Kitsos and Pappa, 2024).

7. DIGITAL HEALTH TRANSFORMATION IN EUROPE: THE ROLE OF NATO AND THE EU IN SHAPING SOVEREIGN HEALTH SYSTEMS

While European countries are progressively increasing investments in digital health infrastructure, available data show that healthcare spending specifically allocated to digital transformation, including enterprise IT systems and cybersecurity, remains relatively low compared to total healthcare budgets. Estimates suggest that digital health spending as a share of healthcare budgets among selected European countries ranges between approximately 0.4% and 8.3%. According to Statista (2024), the digital health market in the United Kingdom was valued at around \$5.55 billion in 2024, while in France; it projected to reach approximately €3.75 billion. Spain, by contrast, allocates only about 0.4% of its health budget to digital transformation efforts, trailing behind Italy and Germany (Gallo *et al.*, 2021; Weresa, Ciecierski and Filus, 2024; Statista, 2025). Cross-national cost comparisons are inherently difficult due to the lack of standardized, transparent reporting. Most European governments do not publish separate budget lines

for software, IT, and digital service expenditures, complicating efforts to track spending across investment, maintenance, and system decommissioning categories (Frintrup, Schmidhuber and Hilgers, 2022). For instance, the UK's 2023 health transformation plan allocated \$5.55 billion for digital upgrades, yet previous estimates from 2019 suggested that replacing six major legacy systems in the National Health Service (NHS) could cost as much as \$14.1 billion over the subsequent decade. While it remains unclear whether current annual budgets include costs for ongoing maintenance and decommissioning, some countries, such as France, Italy, and Spain, do distinguish these elements in their financial reporting. Accurate assessments are further impeded by inconsistent disclosure and insufficient granularity in national health budgets. Nevertheless, understanding how nations invest in healthcare digitalization is essential to tracking their progress toward robust, tech-enabled health systems (Frintrup, Schmidhuber and Hilgers, 2022; Damar, Özen and Yılmaz, 2024; (Russell, Bukhari and Galloway, 2019; Galea and Abdalla, 2023; Karaferis, Aletras and Niakas, 2023);).

Notably, the financial structure of digital transformation differs significantly from that of traditional healthcare infrastructure procu-

rement. In digital health, investment and maintenance costs balanced over time. In contrast, traditional medical infrastructure involves high up-front procurement costs but lower long-term upkeep. There is growing recognition that public healthcare systems across Europe lag significantly behind the private sector, especially the tech industry, in fully leveraging data as a strategic asset for value creation and improved outcomes. Industry stakeholders emphasize that digital transformation typically requires three to four years to yield operational results, depending on the complexity and scale of the project. However, outdated procurement models and inflexible budgetary frameworks often result in long-term initiatives that span decades rather than years. For example, digital health projects in Germany, Italy, and Spain are not expected to conclude before 2030 or 2035. Similarly, Norway anticipates a decade-long timeline for its national digital health overhaul. By contrast, digital transformation in leading industrial sectors often occurs within a two-year window. The urgency to accelerate digital health reform has intensified in the wake of COVID-19 and other health crises, which demonstrated the need for rapid transitions from concept to deployment. For example, during emergencies, health technologies such as digital contact tracing,

AI-powered diagnostics, and telemedicine platforms were developed and deployed within weeks. Yet these rapid-cycle innovations remain the exception rather than the rule across European health systems (Gopal et al., 2019; Karaferis D, Balaska D and Pollalis Y, 2024; Brunetti et al., 2020; Karaferis, Balaska and Pollalis, 2024; Dimitris, Dimitra and Yannis, 2025; Pérez Sust et al., 2020; Raja et al., 2023;).

In July 2023, Germany's Chief of Defense (in a parallel domain) acknowledged that traditional procurement and innovation cycles are ill suited to the fast-paced evolution of new technologies. Similar critiques have emerged from within the UK healthcare sector, where the 2023 Health Command Paper committed to reducing the time between identifying a clinical or technological need and the full-scale deployment of a digital solution. The paper proposed a maximum of three years for health-related digital programs, a goal more moderate than some had hoped but still a significant improvement over historical timeline. Across NATO and EU health and emergency response systems, digital health programs that move from initial conception to operational implementation within months remain rare. Bridging this gap is essential for achieving digital sovereignty, operational agility, and improved patient care across

Europe (Begkos, Antonopoulou and Ronzani, 2024; Frassini, 2024).

8. CONCLUSIONS

The evolving security environment of the 21st century challenges traditional defense paradigms by highlighting the convergence of digital, biological, and hybrid threats. As pandemics, cyberattacks, disinformation campaigns, and the weaponization of health infrastructure intersect; it becomes clear that security extends beyond the battlefield into the realms of data, health, and trust. Both NATO and the European Union (EU) must adapt their defense strategies to address these emerging complexities on exploration of dual-use technology (for both military and civilian purpose) for the overall benefit of our societies.

Health intelligence (HI), once considered a peripheral aspect of defense planning, has become an essential strategic asset. The COVID-19 pandemic revealed the vulnerabilities of isolated systems, the impact of delayed coordination, and the lack of preparedness for bio-digital threats. However, it also underscored the importance of data-driven insights, international collaboration, and adaptive digital tools that, when deployed strategically, can significantly enhance defense capabilities.

Digital transformation in defense must go beyond merely adopting

new technologies; it must foster a fundamental shift in mindset, operational strategies, and inter-institutional cooperation. This transformation involves incentivized private R&D, modernizing infrastructures, enhancing cyber resilience, embedding foresight, interoperability, and real-time responsiveness into strategic frameworks. NATO and the EU must work towards creating agile systems capable of functioning seamlessly across civil-military boundaries, ensuring that health systems and data ecosystems integrated into the concept of critical infrastructure alongside energy and transport systems.

Incorporating health intelligence into NATO and EU defense strategies allows for the transition from reactive responses to proactive preparedness. It is vital to align national and supranational strategies, dismantling barriers between public health, national defense sector and enterprises in health industry (including innovative SMEs). This approach not only addresses immediate threats but also prepares for future risks, enhancing the resilience and readiness of both organizations. The successful defense strategies of the future will require more than the ability to deter and defeat threats, they must anticipate and mitigate risks before they materialize. Health intelligence must be viewed as a central pillar

of this strategic foresight. This approach will not only strengthen the transatlantic alliance's resilience but also reinforce the values of trust, solidarity, and collective security in the digital era. Ultimately, the integration of health, digital innovation, and defense strategy is both an operational necessity and a political and ethical imperative. The decisions made today will shape the security landscape of tomorrow. NATO and the EU must lead this transformation with urgency, vision, and unity.

While this paper provides an initial exploration of health intelligence integration, further research is required to address implementation challenges. Future studies should examine procurement models and decision-making frameworks for defence planners, develop assessment tools for measuring integration readiness, and explore the privacy, legal and ethical implications of cross-border health data sharing (Gerke, Minssen and Cohen, 2020). Engaging practitioners will be essential for identifying solutions that are technologically feasible, ethically sound and sensitive to organisational cultures. Such work will ensure that health intelligence integration delivers tangible policy impact and supports transatlantic security.

In conclusion, the integration of Health Intelligence (HI) into NATO's

broader defense strategy marks a pivotal shift in how security is conceptualized and operationalized in the digital age. As modern warfare becomes multidimensional, encompassing biosecurity risks, digital vulnerabilities, and societal fragilities, health must be embedded as a central element of defense and resilience. While the focus of European defense ministries remains on defense innovation and emerging technologies like artificial intelligence (AI), it is the secure, interoperable digital transformation of data that will underpin NATO and EU military power in the future. For effective and impactful digital transformation, NATO and the EU must establish coherent, secure digital infrastructures that promote cross-border interoperability and human-centric designs. The rapid pace of technological advancement makes it essential to act quickly, as the race against evolving threats is both strategic and existential. Health intelligence plays a crucial role as a preventive mechanism and strategic asset by bridging civil and military preparedness, supporting early warning systems, protecting force health, and reinforcing societal trust in institutions. Building a resilient, secure, and technologically advanced European defense requires more than investing in hardware and algorithms. It demands a fundamental shift in mindset, with digital transformation

and health intelligence serving as foundational pillars of NATO and EU strategic readiness.

Declaration of Interest: The authors declare no conflict of interest.

Ethical approval: The ethical approval was not required, as the study conducted did not involve any ethical concerns or issues.

Funding: None.

Author's contribution: All authors were involved in all steps for preparation of this article, including final proofreading and gave final approval of the version to be published.

REFERENCES

- [1] Andrea Gilli. *NATO-Mation: Strategies for Leading in the Age of Artificial Intelligence*. Rome; 2020 Dec.
- [2] Anghel V, Jones E. Is Europe really forged through crisis? Pandemic EU and the Russia – Ukraine war. *J Eur Public Policy*. 2023 Apr 3;30(4):766–86.
- [3] Bachmann SD. Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats - mapping the new frontier of global risk and security management. *Amicus Curiae*. 2012 Jun 28;2011(88).
- [4] Baroncelli S. Recovery and Resilience Facility. In: *Research Handbook on Post-Pandemic EU Economic Governance and NGEU Law*. Edward Elgar Publishing; 2024. p. 110–27.
- [5] Begkos C, Antonopoulou K, Ronzani M. To datafication and beyond: Digital transformation and accounting technologies in the healthcare sector. *The British Accounting Review*. 2024 Jul;56(4):101259.
- [6] Bente BE, Van Dongen A, Verdaasdonk R, van Gemert-Pijnen L. eHealth implementation in Europe: a scoping review on legal, ethical, financial, and technological aspects. *Front Digit Health*. 2024 Mar 8;6.
- [7] Bocean CG, Vărzaru AA. Health status in the era of digital transformation and sustainable economic development. *BMC Health Serv Res*. 2025 Mar 5;25(1):343.
- [8] Bowsler G, Milner C, Sullivan R. Medical intelligence, security and global health: the foundations of a new health agenda. *J R Soc Med*. 2016 Jul; 109(7):269–73.
- [9] Bricknell M., Gad M, Homan Z, Gheorghe A, Quirk E, Kazibwe J. An analysis of the national responses to the COVID-19 pandemic through the lens of medical military support requirements [Internet]. Norfolk, Virginia; 2020 [cited 2025 Sep 7]. Available from: <https://kclpure.kcl.ac.uk/portal/en/publications/an-analysis-of-the-national-responses-to-the-covid-19-pandemic-th>
- [10] Brunetti F, Matt DT, Bonfanti A, De Longhi A, Pedrini G, Orzes G. Digital transformation challenges: strategies emerging from a multi-stakeholder approach. *The TQM Journal*. 2020 Jul 21;32(4):697–724.
- [11] Burkadze K. Trends of Digital Transformation Based on the UN, EU, and NATO Experiences.

- Fletcher F World Aff.* 2022;46(111).
- [12] Burwell FG; PK. *Atlantic Council, Europe Center.* 2022 [cited 2025 Sep 7]. Digital Sovereignty in Practice: The EU's Push to Shape the New Global Economy. Available from: <https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-in-practice-the-eus-push-to-shape-the-new-global-economy/>
- [13] Burwell FG; PK. The European Union and the search for digital sovereignty: building "Fortress Europe" or preparing for a new world? [*Internet*]. Washington, DC; 2020 Jun [cited 2025 Sep 7]. Available from: <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/>
- [14] Caliskan M, Liégeois M. The concept of 'hybrid warfare' undermines NATO's strategic thinking: insights from interviews with NATO officials. *Small Wars & Insurgencies.* 2021 Feb 17;32(2):295–319.
- [15] Cannon S. *JAPCC Journal, Edition 37, Leadership Perspective.* 2024 [cited 2025 Sep 7]. The Alliance's Transition to Multi-Domain Operations: An AIRCOM Perspective. Available from: <https://www.japcc.org/articles/the-alliances-transition-to-multi-domain-operations/>
- [16] Crespi F, Caravella S, Menghini M, Salvatori C. European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics.* 2021 Nov 11;56(6):348–54.
- [17] Csernaton R, Martins BO. Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination. *Geopolitics.* 2024 May 26;29(3):849–72.
- [18] Damar M, Özen A, Yılmaz A. Cybersecurity in The Health Sector in The Reality of Artificial Intelligence, And Information Security Conceptually. *Journal of AI.* 2024 Dec 31;8(1):61–82.
- [19] Dimitris K, Dimitra B, Yannis P. Digitalization and Artificial Intelligence as Motivators for Healthcare Professionals. *Japan Journal of Research.* 2025 Jan 1;6(3).
- [20] Eröndü NA, Rahman-Shepherd A, Khan MS, Abate E, Agogo E, Belfroid E, et al. Improving National Intelligence for Public Health Preparedness: a methodological approach to finding local multi-sector indicators for health security. *BMJ Glob Health.* 2021 Jan;6(1):e004227.
- [21] Ertan A FKPPST. Cyber Threats and NATO 2030: Horizon Scanning and Analysis [*Internet*]. Tallinn, Estonia: *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*; 2020 [cited 2025 Sep 7]. Available from: https://www.ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf
- [22] Fahy N MNPD. European support for improving health and care systems [*Internet*]. Copenhagen (Denmark): *European Observatory on Health Systems and Policies*; 2021.

- [23] Fasola N. Reforming and Enhancing Partnerships to Strengthen NATO's Strategic Posture. *The US Army War College Quarterly: Parameters*. 2024 Nov 21;54(4).
- [24] Fiott D. *European Union Institute for Security Studies*. 2020 [cited 2025 Apr 25]. Digitalising defence: Protecting Europe in the age of quantum computing and the cloud. Available from: <https://www.iss.europa.eu/content/digitalising-defence>
- [25] Fiott D. In every crisis an opportunity? European Union integration in defence and the War on Ukraine. *J Eur Integr*. 2023 Apr 3;45(3):447–62.
- [26] for different actors. e-Estonia guide: the most advanced digital society in the world. Tallinn: Enterprise Estonia [Internet]. 2025 [cited 2025 Sep 7]. Available from: https://e-estonia.com/wp-content/uploads/eestonia_guide_08-04-2025.pdf#:~:text=online%E2%80%93it%20takes%20only%203%20minutes%21
- [27] Frassini J. CIV-MIL integration in the transformation of the EU healthcare network: a dual-gain strategy. *Journal of Integrated Care*. 2024 Aug 8;32(3):252–69.
- [28] Frintrup M, Schmidhuber L, Hilgers D. Towards accounting harmonization in Europe: a multinational survey among budget experts. *International Review of Administrative Sciences*. 2022 Jun 27;88(2):390–410.
- [29] Gaeta E, Salman Haleem M, Lopez-Perez L, Manea M, Fernanda Cabrera Umpierrez M, Teresa Arredondo Waldmeyer M, et al. GATEKEEPER Platform: Secure Processing Environment for European Health Data Space. *IEEE Access*. 2025;13:34627–38.
- [30] Galea S, Abdalla SM. Data to Improve Global Health Equity—Key Challenges. *JAMA Health Forum*. 2023 Nov 2;4(11):e234433.
- [31] Gallo F, Seniori Costantini A, Puglisi MT, Barton N. Biomedical and health research: an analysis of country participation and research fields in the EU's Horizon 2020. *Eur J Epidemiol*. 2021 Dec 17;36(12):1209–17.
- [32] Gendy MEG, Yuce MR. Emerging Technologies Used in Health Management and Efficiency Improvement During Different Contact Tracing Phases Against COVID-19 Pandemic. *IEEE Rev Biomed Eng*. 2023;16:38–52.
- [33] Gerke S, Minssen T, Cohen G. Ethical and legal challenges of artificial intelligence-driven healthcare. In: *Artificial Intelligence in Healthcare*. Elsevier; 2020. p. 295–336.
- [34] Gerke S, Minssen T, Cohen G. Ethical and legal challenges of artificial intelligence-driven healthcare. In: *Artificial Intelligence in Healthcare*. Elsevier; 2020. p. 295–336.
- [35] Gopal G, Suter-Crazzolara C, Toldo L, Eberhardt W. Digital transformation in healthcare – architectures of present and future information technologies. *Clinical Chemistry and Laboratory Medicine (CCLM)*. 2019 Feb 25;57(3):328–35.
- [36] Grgić G. Redefining NATO's Indo-Pacific partnerships: cooperative

- security meets collective defence and deterrence. *Asian Security*. 2024 Jan 2;20(1):39–55.
- [37] Haby MM, Chapman E, Barreto JOM, Mujica OJ, Rivière Cinnamond A, Caixeta R, et al. Greater agreement is required to harness the potential of health intelligence: a critical interpretive synthesis. *J Clin Epidemiol*. 2023 Nov;163:37–50.
- [38] Haddud A, McAllen D. Digital Workplace Management: Exploring Aspects Related to Culture, Innovation, and Leadership. In: *2018 Portland International Conference on Management of Engineering and Technology (PICMET)*. IEEE; 2018. p. 1–6.
- [39] Honeyman MMDEHDA. *Public Health Wales NHS Trust (Research and Evaluation Division)*. 2020 [cited 2025 Sep 7]. Digital technology and health inequalities: a scoping review. Available from: <https://phw.nhs.wales/publications/publications1/digital-technology-and-health-inequalities-a-scoping-review/>
- [40] Ilangakoon TS, Weerabahu SK, Samaranayake P, Wickramarachchi R. Adoption of Industry 4.0 and lean concepts in hospitals for healthcare operational performance improvement. *International Journal of Productivity and Performance Management*. 2022 Jun 24;71(6):2188–213.
- [41] J.Metsallik, P. Ross, D. Draheim, G. Piho. Ten Years of the e-Health System in Estonia. In: Adrian Rutle (Western Norway University of Applied Sciences BNYL (Western NU of ASBNWM (St. FXUACLI (Gran SSILI, editor. *Proceedings of the 3rd International Workshop on (Meta) Modelling for Healthcare Systems (MMHS 2018)* [Internet]. Bergen, Norway: CEUR Workshop Proceedings (CEUR-WS); 2018 [cited 2025 Sep 7]. p. 6–15. Available from: : ceur-ws.org/Vol-2336/MMHS2018_invited.pdf.
- [42] Jain N, Prasad S, Bordeniuc A, Tanasov A, Shirinskaya AV, Béla B, et al. European Countries Step-up Humanitarian and Medical Assistance to Ukraine as the Conflict Continues. *J Prim Care Community Health*. 2022 Jan 23;13.
- [43] Karaferis D, Aletras V, Niakas D. Job satisfaction of primary healthcare professionals: a cross-sectional survey in Greece. *Acta Biomed*. 2023 Jun 14;94(3):e2023077.
- [44] Karaferis D, Balaska D, Pollalis Y. Enhancement of Patient Engagement and Healthcare Delivery Through the Utilization of Artificial Intelligence (AI) Technologies. *Austin Journal of Clinical Medicine*. 2024 Nov 15;9(2).
- [45] Karaferis DC, Niakas DA. Exploring Inpatients' Perspective: A Cross-Sectional Survey on Satisfaction and Experiences in Greek Hospitals. *Healthcare*. 2024 Mar 14;12(6):658.
- [46] Karaferis Dimitris BD and PY. Artificial Intelligence and Robotics:Catalysts or Threats in the Development of Healthcare. *Biostat Biom Open Access J*. 2024;11(5).
- [47] Kitsos P, Pappa P. Cloud Governance in the European Union: Unlocking the Power of Data in the Era of the Digital Economy. In 2024. p. 99–114.

- [48] Lantzsch H, Eckhardt H, Campione A, Busse R, Henschke C. Digital health applications and the fast-track pathway to public health coverage in Germany: challenges and opportunities based on first results. *BMC Health Serv Res.* 2022 Sep 21;22(1):1182.
- [49] Blessing J KEKEPNM (editors); TR (associate editor). NATO 2030: Towards a New Strategic Concept and Beyond [Internet]. *Henry A. Kissinger Center for Global Affairs*; Johns Hopkins SAIS; DAAD (German Academic Exchange Service); 2021 [cited 2025 Sep 7]. Available from: <https://sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>
- [50] Lucarelli S MAMF. NATO Decision-Making in the Age of Big Data and Artificial Intelligence. In NATO Allied Command Transformation; *University of Bologna; Istituto Affari Internazionali (IAI)*; 2021 [cited 2025 Sep 7]. Available from: <https://www.iai.it/sites/default/files/978195445000.pdf> (iai.it)
- [51] Madiega TA. European Parliamentary Research Service (EPRS). 2020 [cited 2025 Sep 7]. *Digital sovereignty for Europe*. Available from: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)
- [52] Majcherek D, Hegerty SW, Kowalski AM, Lewandowska MS, Dikova D. Opportunities for healthcare digitalization in Europe: Comparative analysis of inequalities in access to medical services. *Health Policy* (New York). 2024 Jan; 139:104950.
- [53] Mauro M, Noto G, Prenestini A, Sarto F. Digital transformation in healthcare: Assessing the role of digital technologies for managerial support processes. *Technol Forecast Soc Change.* 2024 Dec; 209:123781.
- [54] Mesterhazy A. The Role of NATO's Armed Forces in the COVID-19 Pandemic [Internet]. 2020 Jun [cited 2025 Sep 7]. Available from: https://www.nato-pa.int/download-file?filename=%2Fsites%2Fdefault%2Ffiles%2F2020-06%2F091%20DSC%2020%20E%20-%20COVID-19%20SPECIAL%20REPORT_1.pdf
- [55] NATO Allied Command Transformation. Empowering NATO's Multi-Domain Operations Through Digital Transformation [Internet]. 2023 [cited 2025 Sep 7]. Available from: <https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/>
- [56] NATO Reflection Group. NATO. 2020 [cited 2025 Sep 7]. NATO 2030: Unity for a New Era – Reflection Group Final Report. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf
- [57] NATO STO SET Panel. NATO Research Lecture Series SET-290: Artificial Intelligence for Military Multiple Sensor Fusion Engines. In: *NATO Science & Technology Organization (STO), Systems and Electronics Technology (SET) Panel* [Internet]. Rome, Wachtberg,

- Budapest: Lecture Series Programme; 2022 [cited 2025 Sep 7].
- [58] NATO. NATO official text. 2024 [cited 2025 Sep 7]. NATO's Digital Transformation Implementation Strategy. Available from: https://www.nato.int/cps/en/natohq/official_texts_229801.htm#:~:text=Strategic%20Outcomes
- [59] NATO. NATO. 2022 [cited 2025 Sep 7]. Summary of NATO's Data Exploitation Framework Policy (DEFP). Available from: https://www.nato.int/cps/en/natohq/official_texts_210002.htm
- [60] NATO's strategy for digital transformation [Internet]. 2024 [cited 2025 Sep 7]. Available from: https://www.nato.int/cps/en/natohq/news_229985.htm
- [61] Niño Sevilla Palma F. Digital Health Beyond Borders: Interoperability Challenges and Critical Success Factors in the Deployment of Cross-border ePrescription in Finland and Estonia. *Westfälische Wilhelms-Universität Münster*; 2021.
- [62] Oberländer M, Beinicke A, Bipp T. Digital competencies: A review of the literature and applications in the workplace. *Comput Educ*. 2020 Mar; 146:103752.
- [63] Odone A, Buttigieg S, Ricciardi W, Azzopardi-Muscat N, Staines A. Public health digitalization in Europe. *Eur J Public Health*. 2019 Oct 1;29(Supplement_3):28–35.
- [64] Orăștean R, Sava R, Mărginean S. Measuring Healthcare Digitalisation in The European Union: Trends and Challenges. *Rev Econ*. 2022 dec 20;74(4):64–74.
- [65] Pérez Sust P, Solans O, Fajardo JC, Medina Peralta M, Rodenas P, Gabaldà J, et al. Turning the Crisis Into an Opportunity: Digital Health Strategies Deployed During the COVID-19 Outbreak. *JMIR Public Health Surveill*. 2020 May 4;6(2):e19106.
- [66] Policy Department DG for EP of the U. How the COVID-19 crisis has affected security and defence-related aspects of the EU [Internet]. 2021 Jan [cited 2025 Sep 7]. Available from: [https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA\(2021\)653623](https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2021)653623)
- [67] Raja M, Kymre IG, Bjerkan J, Galvin KT, Uhrenfeldt L. National digital strategies and innovative eHealth policies concerning older adults' dignity: a document analysis in three Scandinavian countries. *BMC Health Serv Res*. 2023 Aug 10;23(1):848.
- [68] Rauch TM, Daniel JC, Erickson EA, Shiau D, Cincotta J V. US Department of Defense Global Health Engagement: supporting global health security, readiness and interoperability. *BMJ Mil Health*. 2024 Jul;170(e1):e1–3.
- [69] Ruohonen J, Timmers P. Early Perspectives on the Digital Europe Programme. 2025 Jan 6;
- [70] Russell MD, Bukhari M, Galloway J. The price of good health care. *Rheumatology*. 2019 Jun 1;58(6):931–2.
- [71] Shea J. How is NATO Meeting the Challenge of Cyberspace. ImprintPRISM: *A Journal of the Center for Complex Operations*. 2017 Dec;7(2):18–29.

- [72] Soare S. International Institute for Strategic Studies (IISS). 2023 [cited 2025 Sep 7]. Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age. Available from: <https://www.iiiss.org/research-paper/2023/08/digitalisation-of-defence--in-nato-and-the-eu/>
- [73] Statista. Statista Health Market Outlook. 2025 [cited 2025 Sep 7]. Revenue in the digital health market in the United Kingdom. Available from: <https://www.statista.com/forecasts/1436300/revenue-digital-health-digital-health-market-united-kingdom>
- [74] Sylvia N. Emerging Insights Royal United Services Institute for Defence and Security Studies. 2025 [cited 2025 Sep 7]. European Digital Defence Priorities in an Uncertain World. Available from: <https://static.rusi.org/european-digital-defence-priorities-march-2025.pdf>
- [75] Szeftel D, Jouhet V, Duluc G, Charle-Maachi C, Sejourné T, Fabiano J, et al. Health data: Regionalised access is a priority challenge for building a secure, transparent and innovative national health data repository. *Therapies*. 2025 Jan;80(1):125–34.
- [76] Vaagan RW TSSAFJLA. A Critical Analysis of the Digitization of Healthcare Communication in the EU: A Comparison of Italy, Finland, Norway, and Spain. *Int J Commun* [Internet]. 2021 Mar 27 [cited 2025 Sep 7];1718–40. Available from: <https://ijoc.org/index.php/ijoc/article/view/15399>
- [77] Värri AJDPGJDMHKHUMK and LPH. Integrated Citizen Centered Digital Health and Social Care [Internet]. 1st ed. Vol. 12. SAGE; 2020 [cited 2025 Sep 7]. Available from: <https://www.perlego.com/book/5032898/integrated-citizen-centered-digital-health-and-social-care-citizens-as-data-producers-and-service-cocreators-pdf>
- [78] Veronesi G, Kirkpatrick I, Altanlar A, Sarto F. Corporatization, Administrative Intensity, and the Performance of Public Sector Organizations. *Journal of Public Administration Research and Theory*. 2023 Sep 12;33(4):701–15.
- [79] Weresa MA, Ciecierski C, Filus L. Digitalization and Innovation in Health. London: Routledge; 2024.
- [80] Wolff AT. Who Is NATO for? In: *The Oxford Handbook of NATO*. Oxford University Press; 2025. p. 77–93.
- [81] Zorloni L. Europe Is Pumping Billions Into New Military Tech [Internet]. 2024 [cited 2025 Sep 7]. Available from: <https://www.wired.com/story/european-commission-military-tech-spending/>
- [82] Zornetta A. Quantum-safe global encryption policy. *International Journal of Law and Information Technology*. 2024 Jun 1;32.

FOOD SECURITY CONCEPTS: HISTORICAL EVOLUTION AND CURRENT STATE

Vasile SACOVICH*, Vitalii CAZACU**

*Moldova State University, Chisinau, Republic of Moldova

**Chisinau, Republic of Moldova

The article deals with the evolution of the concept of food security and provision of the population with food, which we have classified into five stages. By now, a new direction of security in the system of national security has fully formed - food security, with its categorical apparatus, its theoretical and methodological basis and practical approaches to providing the population with food. It is noted that the peculiarity of all stages of food security is that it is not static, but dynamically developing. The modern, fifth stage of food security development has turned out to be the most complicated and in modern time frames it has become a weapon of global confrontation, food supplies from a number of countries are blocked. In this situation there is only one way out - to ensure food security at the level of national states.

Key words: *Food security, practical approaches, evolution, stages, production, consumption, self-sufficiency*

1. INTRODUCTION

The problem of food security is one of the most significant in the modern world. It affects the interests of all countries, becoming more and more urgent as the food supply worsens, the world trade in agricultural products and food decreases, and the global situation in the world is currently aggravated. In this regard, the issue of food security has become highly politicised and

one of the most debated.

Referring to the complex, multilevel and multifaceted nature of the affected problem, researchers often emphasise that for this reason it is difficult to offer a single definition of the scientific category “food security”. Indeed, the analysis of the evolution of the term “food security” shows that it is not static and has been changing within certain time frames depending on the degree

of development of the world and national economies, the activities of international organisations and national governments and a number of other factors. In our study we presented an approach in which we identified five stages in the evolutionary development of the concept of food security.

Since ancient times, security has been associated with the ability of a state to protect itself and feed its population. One of the first to note the importance of agricultural production for the development of the country was François Kennet, who in the early 18th century declared the real wealth of the nation to be “the products of agriculture” [9].

However, it was scientifically formulated only in the late 18th century after T. Malthus put forward the idea of comparing the dynamics of population and available means of subsistence [7]. To assess food security, T. Malthus suggested using the ratio between the indicators of production and consumption per capita. Later on, this formula formed the basis of modern economic analysis.

T. Malthus's reasoning led to the conclusion that the provision of food for the population is a prerequisite for its existence, and this provision does not always provide the possibility of normal human existence. In other words, the very functioning of a man as a living being is not always

adequate to the availability of food opportunities available in nature, and a simple increase in the number of people undermines the basis of their existence. Malthus attributes the relatively low rates of food growth to the so-called law of diminishing soil fertility [7].

2. STAGES OF EVOLUTION OF THE CONCEPT OF FOOD SECURITY

The first stage in the development of the idea of food security is characterised by the fact that the national economy, its production capacity, i.e. the country's ability to provide the necessary means of subsistence for its citizens regardless of external factors, is considered as the source of its provision. The level of provision of the basic biological human need for nutrition, the quantity of products produced, their qualitative characteristics are an indicator of the maturity and resilience of the state, its ability to feed the growing population and resist disease, which ultimately forms the material basis for the progressive course of the historical process and economic development of the country.

The next second stage in the development of the concept of food security was formed in the 1970s, during the period of tangible food shortages associated with the world food crises, and it is characterised at

its core by the general liberalisation of the economy and increasing volumes of foreign trade, including exports. The biological notion of security was supplemented by economic, and more specifically foreign trade aspects. At this stage, the world food system began to take shape, designed to cover the needs of the world's population in food products, to ensure the movement of food products between countries and regions within the international division of labour, taking into account the factor of comparative advantage.

In the 1970s, the world community came to the realisation that food crises, even those that began within one state, soon acquire an international character, and the conditions for overcoming them are also created by joining efforts at the global or regional level. The world grain crisis of 1972-1973 contributed to the fact that the problem of food supply became an important factor in the national security of all countries [8]. The term food security was first introduced into international circulation at the UN General Assembly in 1974. At that time, world food security was understood as “maintaining stability in food commodity markets with the availability of basic food products for all countries of the world” [6].

During this period, the fight against hunger was proclaimed one of the global problems of mankind,

the concept of “world food security” emerged, and food security criteria were developed, which are divided into physiological (the need of the human body for a certain amount of energy and nutritional elements, the permissible content of substances harmful to the human body in products), economic (the physical availability of food for different categories of the population together with the possibility of purchasing it on the basis of the following criteria [6].

In addition to the realisation of the need to join forces to ensure food security, the idea that national food security is critically dependent on foreign trade revenues has gained ground at this stage. This was prompted by the energy crisis of the 1970s, when the European economy was hit hardest by oil shortages. The restriction and, in some cases, outright embargo on oil supplies to European countries brought them to the brink of economic collapse. This period saw the beginning of numerous studies on the limits to the growth of this kind of dependence, which leads to a critical level of threats to national security, and the notion of food security was supplemented with an aspect of foreign economic relations, analysing the possibility of stable and reliable external food supplies and introducing the concept of “food independence”.

Another change in the approach to food security occurs in the 1990s,

when it turns into a global problem, i.e. it is considered as an element of globalisation, the interconnection of world and national economic development. The third stage of understanding food security has begun. The object of analysis is not national self-sufficiency (production of the necessary amount of food products), but the possibility of using the world market to purchase food. The concept of food security is supplemented by its accessibility for certain groups of citizens.

This approach is reflected in a number of decisions taken at the international level. According to the 1996 Rome Declaration on World Food Security, poverty is recognised as the main cause of food shortages [10].

The UN has formulated the Millennium Development Goals, of which food security is an integral and essential part. The ambitious target is to halve the proportion of people suffering from hunger by 2015. This is to be achieved through the overall development of underdeveloped regions with international support. Signatories to the Declaration and Plan of Action on World Food Security have committed themselves to eliminating hunger, building a fair food trading system, and ensuring equal access to food for all segments of the population. A system of food assistance to countries affected by natural disasters is being developed.

Food security is recognised as an essential part of each country's economic security.

In 1996 in Rome, at the World Conference on Nutrition and Sustainable Agriculture, the term food security was formally defined in the Declaration adopted by the World Conference on Nutrition and Sustainable Agriculture as “the state of the economy in which access to food, drinking water and other nutritional products of a quality, variety and quantity necessary and sufficient for physical and social development of the individual, for health and for the expansion of human life”.

The World Conference on Nutrition (1996) definition of “food security” contains the following essential elements [6]:

1. physical availability of sufficient quantitatively adequate, safe and nutritious food;
2. economic accessibility to food of adequate quantity and quality for all social groups;
3. autonomy and economic independence of the national food system (food independence);
4. reliability, i.e. the ability of the national food system to minimise the impact of seasonal, weather and other fluctuations on the supply of food to the population in all regions of the country;

5. sustainability, which means that the national food system develops in the mode of expanded reproduction.

The global food crisis that emerged in 2004 can be conditionally considered the beginning of a new - the fourth stage of formation of views on the problem of food security. The agro-food crisis affected not only the deterioration of indicators of the global food situation (rising food prices, malnutrition of especially vulnerable segments of the population), but also the decline in the efficiency of the agro-food sector, weakening competition and monopolisation in the food market due to the ruin and withdrawal of small producers.

While at the third stage there was an understanding of the need to provide international food support to countries in need, since 2004 it has become clear that in the context of global agro-food crises arising from unpredictable natural unfavourable natural phenomena, from which no state is insured, it is possible to solve the problems of food security only by coordinating the policies of states and uniting their efforts at the global level.

In contrast to the previous stages, starting from the moment of certain events in the world economy, the process of formation of the fourth stage can be called national. Based on the research conducted

mostly within the framework of international organisations, it can be concluded that mankind began to approach the concept of forming an integrated agro-food market during this period. The food market began to receive special attention from the state regulatory bodies. At the same time, state regulation in agriculture is increasingly influenced by external factors such as international treaties and agreements. This trend faces the problem of national security, the threat of dependence on food imports. The dominant view is that the problem of preserving the position of the national producer in the market is moving to the background. However, by supporting the national producer, countries are able to maintain their position on the world market mainly by increasing their competitiveness. This is the main characteristic feature of the fourth stage in the development of the concept of food security.

Consideration of approaches to the understanding of food security in the historical context allows us to formulate more clearly the concept and essence of such an important economic category taking into account different points of view. In this case, according to the authors, it is necessary to proceed from the generally accepted view of food security as the availability of food in the economic and physical sense. It is worth noting that “physical availability” is a characteristic

of supply in the food market of a particular state. In turn, “economic accessibility” means the possibility and availability of financial security of the population necessary to purchase food at affordable prices and forming consumer demand on the scale of the national food market. In other words, it is a state of the food market in which the ratio of supply and demand for food products forms prices that ensure the ability of the population of all income groups to meet their nutritional needs.

However, this definition of food security does not reveal the sources, in other words, the very factors of ensuring the physical and economic availability of food, whereas this aspect of the issue is the most important and essential for understanding the category of food security. It is a combination of such internal and external factors as national agrarian production, creation of food reserves, export-import supplies of food, international food aid, etc. It is in this dimension that the watershed between different, contradictory approaches to the analysis of the concept of food security lies.

In developed countries (the USA, Germany, France, Japan), the need to address food security issues is given great importance [5, p. 6 - 34]. However, in these countries this issue is considered from the perspective of the achieved high level of food

self-sufficiency, although certain differences in approaches should be emphasised. For example, in Germany, food security is considered an important problem that arises only in conditions when the issue cannot be solved through market regulation. In fact, Germany is dominated by the approach in which this problem is analysed from the point of view of a crisis situation emergence in the country [2, p. 32]. In the USA, food security is regarded, firstly, as support for the stability of sales in the domestic food market (primarily national production), secondly, as a form of implementation of food aid programmes for the poor, thirdly, as a stimulus for agricultural exports and the use of food supplies in the interests of foreign policy [1]. Along with this, food security in the USA is understood as “food safety for human health”. As for the problem of food independence, it remains outside analytical developments and studies of American economic philosophy.

Another approach to the problem of food security is characteristic of countries with economies in transition. Formally, food security is considered in these countries as a means of solving the problem of providing the country with basic food products while simultaneously addressing the problem of quality and access of the population to food. However, in fact, the main emphasis is placed on the problem of self-

sufficiency, when the absolute value of production of basic commodities in the country itself is specified. The modern theory of food independence is not limited to abstract inferences, but is increasingly based on quantitative assessments and various methods of calculations of optimal levels of food supply. In particular, the sufficiency of food self-sufficiency of the country is periodically established in the form of parameters of actually achievable specific weight of the main types of domestic food in the total volume of its consumption and in the commodity resources of the domestic market. It should be stressed that the quantitative parameters of production of food and raw material resources sufficient to ensure domestic consumption are calculated taking into account scientifically justified physiological norms of per capita consumption.

It is necessary to emphasise the significant difference of opinions in the literature in assessing the levels of self-sufficiency. For example, some authors (S.U. Nuraliev and others) note that food dependence can occur when the population is provided with food obtained at the expense of domestic production in the volume of less than 80%, and the presence of imported food products in the domestic market will reach volumes of more than 20%. In their opinion, the critical volume of agricultural production as a whole

should be ensured at the expense of own production by 60 per cent. Otherwise, the state will lose its food independence. It should be borne in mind that the recommended indicator cannot be universal and absolute. The choice of security indicators (food self-sufficiency) is conditioned by the specifics of agrarian production, the degree of economic development of the country, the level of dependence on food imports and other factors.

Important criteria of food security include the availability of strategic food reserves sufficient to provide the population under the norms of a crisis situation for the period of mobilisation measures to restructure the country's life support system in order to overcome or compensate for the damage caused by the crisis situation.

Moreover, strategic food reserves, while occupying an intermediate role in the market mechanism, become one of the first places in ensuring food security almost everywhere (at the global, regional and national levels).

One of the main conditions for food security of the country is sustainable self-sufficiency of the country in grain, rational formation and use of its resources. Such factors as a high share of grain consumption for food purposes, the ability of grain to retain qualitative and quantitative parameters during transportation, suitability for long-term storage

create the possibility of forming insurance and reserve funds, which gives grain a priority in the economic society.

In the concept of food security of the state a special place is occupied by the problem of import, its influence on the system of food supply of the population, on the development of agro-industrial complex of each modern state. In the tradition of Western economic science, import is interpreted as an alternative to food self-sufficiency. The limits of imports are set by market laws taking into account comparative advantages and the level of production of agricultural products and foodstuffs achieved by the country. According to this approach, external (imports) and internal sources of food are equivalent. The problem of food independence in this case remains outside the scope of analysis and discussion.

Such an assessment of food imports is inherent in a number of international organisations and UN programmes that are aimed at fighting hunger in developing countries. For example, FAO experts emphasise the following features of food security:

- food security does not mean self-sufficiency in food;
- a country should endeavour to produce enough food for its needs if it has comparative advantages;

- a country must be able to import the necessary amount of food and meet the food needs of its citizens.

In this interpretation, imports do not harm the food sovereignty of a country, but, on the contrary, strengthen its security in terms of supplying the population with the necessary products. It is characteristic that European and American experts explain the problems with food shortages in many developing countries not by a lack of production and self-sufficiency, but primarily by a lack of funds necessary to pay for the import of food resources.

An important feature of the problem is the possibility of ambiguous, often opposite approaches to the assessment of social and economic consequences of import activities for the national economy. On the one hand, imports are a consequence of natural processes in the world economy, when national markets of individual countries become part of the global market of goods and services, international food trade develops and with it the system of interdependencies in all areas of the economy, including food and agricultural complexes. Imports optimise production costs, contribute to meeting the country's food needs, ensuring rapid saturation of the domestic market and saving public labour.

On the other hand, at a certain stage import activities may lead to a sharp and irrational increase in the share of foreign products in domestic consumption. This is accompanied by a reduction in employment in the sphere of material production, deterioration of the financial condition of local enterprises, up to their bankruptcy. In accordance with researchers' conclusions, in particular, Y. N. Pleskachev, "the systematic increase in the total volume of consumed food products the share of imported food creates a very specific direct threat to national economic security" [6].

As in the case of self-sufficiency, the assessment of food imports is based on a quantitative approach, including certain criterion assessments of such imports from the point of view of maintaining food independence. In particular, world experience shows that a country maintains its independence if the ratio of imports to domestic consumption expressed in per cent (import quota) fluctuates within 20-25%. According to the scientist Nikonov A.A., the threshold of food dependence should not exceed 10-15 % [6]. After this level the pre-crisis state of the food situation comes, when own production is insufficient and there is a complete dependence on imports.

At the same time, the export activities of agro-industrial

complexes provide a very reliable support for food security in the current conditions of the increasing formation of international markets for agricultural products and foodstuffs. Food exports, for example, provide foreign exchange resources, which in turn can be invested in agriculture and the food industry.

Moreover, without expanded external markets in the current conditions of specialisation and intensification of production, progress in the agricultural sector in most countries of the world becomes impossible. The close relationship between production and export activities is evidenced by the fact that the most favourable countries in terms of food security are usually included in the list of net exporters of agricultural raw materials and food (USA, EU countries, Canada, Brazil and others).

According to experts, the main factor for sustainable development of the economy is its "balance between exports, imports, domestic production and consumption". As noted above, if the share of imports of a socially important product in domestic consumption becomes higher than 20-25%, there is a threat to economic and food security. Similarly, the same applies to exports: in the event of global economic shocks, "an economy in which exports and imports of goods are at the level of $\frac{1}{4}$ of national

production will be more resilient". This approach is also justified for the agro-industrial sector, to strengthen the country's food market and its food security as a whole [6].

At present, in our opinion, the fifth - modern - stage of food security has arrived in the period from 2020. It is characterised by the fact that international organisations have signed their impotence to ensure international food security and it has moved to the level of national governments. Therefore, on the one hand, the underdeveloped countries are left alone with the problem of food supply, on the other hand, today the food strategy of states has become focused on achieving food security as the most important condition for preserving their sovereignty and independence, economic stability and social sustainability. The task of governments is to develop long-term goals of food security on the basis of objective economic processes and take appropriate measures of socio-economic regulation [3, p. 3];

3. THREATS AND RISKS TO FOOD SECURITY

The main threats and risks to food security in the world include the following:

- natural and climatic factors (for example, in conditions of crop failure there is a threat of failure to fulfil obligations under contracts for the supply of agricultural products);

- population growth and, against the background of rising living standards in developing countries, an increase in effective demand for food;
- reduced growth rates of investment in the agricultural sector of the economy;
- cyclic nature of the economy (the optimal condition for achieving food security is stability, not only of natural and climatic conditions, but also of economic development.
- price volatility, which plays a special role in the destabilisation of the food market, including in conditions of coincidence of agro-food and general economic crises (volatility is an integral characteristic of food prices. The mechanism of food price volatility was identified back in the 1990s, patterns of its propagation between food commodities were found, and a link was established with oil prices, exchange rates, stocks and yields.
- food supply has become a political international confrontation, hybrid warfare.

Thus, current practice shows that the food sector is highly vulnerable to political and economic shocks.

Economic crises have a negative impact on the financial component of the food sector, leading to destabilisation of the credit system for agricultural producers, who, due to these constraints, are forced to either refuse to expand or reduce production altogether. For the consumer, this means limited supply on the market and, as a consequence, rising food prices. Food problems are also aggravated by the fact that, against the background of general political confrontation, food supply has become one of the factors of hybrid warfare. Accordingly, the essence of food security is the ability of the state to overcome external threats and risks to the functioning of the food system. In other words, food security is understood as independence from internal economic shocks, crises in the agro-industrial complex, as well as from the uncertainties of the global food situation, from political pressure, sanctions and other forms of threats from the outside world. Today's situation with global political confrontation, closure of borders, isolation of states has shown more than ever the importance of self-sufficiency in food supply for the population of each country.

In this unstable situation, the role of the state is more important than ever. Emphasising the role of the state, the authors are of the opinion that private entrepreneurship and market mechanisms cannot ensure

the priorities of food independence of the state. This task is solved only by the state system of economic regulation. In food security issues, the state performs a dual function: on the one hand, it forms the food complex of the country, regulates its activities in the market, and on the other hand, it provides it with favourable legal, political and organisational conditions for sustainable development, protects food security from risks and threats from internal and external factors. The latter circumstance particularly emphasises the regulatory role of the state as a guardian of food independence and security.

To understand the essence of food security in the modern period, along with identifying the factors of instability, it is necessary to focus on the issue of mechanisms that are involved in the fulfilment of food security objectives at the national level. We are talking about the mechanisms of financial assistance and stimulation of agriculture, support of export-import operations in the world food market, etc. The issue of the role of the state in ensuring the physical and economic accessibility of food resources comes to the fore.

4. CONCLUSIONS

Thus, food security is a complex and multifaceted phenomenon of economic life of any state as a

purposeful activity of the state and international organisations in the field of formation of the food base, physical and economic availability of food products, on the one hand, and state protection of food security from numerous risks, challenges and threats. The national agro-industrial complex and its effective functioning to provide the country's population with food in accordance with health standards occupy a leading place among the main factors in achieving food security goals. In modern conditions, the optimal approach to solving the problem of food security should be considered self-sufficiency, which takes into account not only the volume of agricultural products produced, but also the level of their quality and the degree of affordability for all consumers. This approach largely depends on the sustainability of national food security of the country, which is guaranteed by the appropriate dynamics of socio-economic development of the country and the functioning of the agro-industrial complex, which provides the necessary level of production of all major types of products that guarantee food independence.

REFERENCES

- [1] Агропромышленный комплекс США // <https://studopedia.org/1-67136.html> (дата обращения – 6.02.2024 г.).
- [2] Бурдуков П. Т., Саетгалиев Р. З. Россия в системе глобальной продовольственной безопасности. М., 1999. С. 32.
- [3] Концепция национальной продовольственной безопасности. Минск: Институт аграрной экономики, 2004. С. 8.
- [4] Продовольственная безопасность: содержание, оценка и повышение уровня // <https://studfiles.net/preview/1862249/page:7/> (дата обращения – 18.12.2023 г.).
- [5] Попков А. А. Аграрная экономика Беларуси: опять, проблемы, перспективы. Минск, «Беларусь», 2006. С 6 – 34
- [6] Сакович В. А. Продовольственная безопасность Республики Молдова в контексте современной мировой продовольственной проблемы. Академия экономических знаний Молдовы, Институт международных отношений Молдовы. Кишинев, 2020. 544 с.
- [7] Теория классической политической экономии Томаса Роберта Мальтуса // <https://studfile.net/preview/9898391/page:3/> (дата обращения – 18. 02. 2024 г.).
- [8] Обеспеченность продовольствием – экономическая основа продовольственной безопасности // <http://www.jourclub.ru/26/536/> (дата обращения – 03.12.2023 г.).
- [9] Экономическая таблица Ф. Кене "Экономика и социум" №4(13) 2014. 755 с.
- [10] World Food Summit, WFS 96 3 – Corr. 1. Rome, Italy. 1996

SECURITY CULTURE - A NEED OF THE POPULATION

Nicolae CHIMERCIUC

"Alexandru cel Bun" Military Academy of the Armed Forces, Republic of Moldova

This article is dedicated to Security Culture. Security culture represents the active and conscious engagement of citizens in managing the state's problems and supporting institutions in preventing threats to national security. This involves understanding and assimilating information, attitudes and values related to the political, military and economic aspects of society. As a moral, educational and formative guide, security culture aims to prepare citizens to contribute to the protection of national values. National security is not only a concern of the state, but also of its citizens, and security culture plays an essential role in their involvement in ensuring stability and protecting national values. This culture emerges from the experience and consciousness of citizens and encompasses cognitive, evaluative and emotional aspects, influencing the way they perceive and respond to threats. Building a strong security culture requires an education that would enable society to thrive safely and adapt to the rapid changes in the security environment. Close collaboration between education and security institutions is necessary to ensure the relevance, updating and application of education programs in the real context of security threats.

Key words: *Security, security culture, strategic culture, education, civil protection, threats, dangers, safety.*

1. INTRODUCTION

Security is one of the major concerns of humanity, and the recent wave of terrorist attacks on European territory has highlighted to an even greater extent the need for action in this area by the European Union.

But security cannot be effective and sustainable without education and culture in this area.

The classic concept of Johann Gottfried Herder (a German thinker, theologian and cultural historian) suggests that culture is a historical process of development and

ennoblement (elevation) of human abilities. Herder emphasizes the idea of the determining role of "sciences and arts", as well as the connection with the Enlightenment ideal of progress.

In the social systems theory of other philosophers, the concept of "culture" has been used to characterize values and other components of the system of social action. Culture thus guides action by establishing values that guide behavior. For example, the concept of "political culture" of Almond Gabriel (an American political scientist who chaired the Committee on Comparative Politics of the Social Science Research Council for many years and served as president of the American Political Science Association (APSA) from 1965 to 1966. In 1981, he received the APSA's James Madison Award, which recognizes a political scientist who has made "distinguished scholarly contributions" during his career) was based on this understanding of culture. [5, p.8].

Security culture represents the active and conscious commitment of citizens in managing state issues and supporting institutions in preventing threats to national security. This involves understanding and assimilating information, attitudes and values related to the political, military and economic aspects of

society. Being a moral, educational and formative guide, security culture aims to prepare citizens to contribute to the protection of national values. [8].

We are currently witnessing a permanent change in the security environment. This transformation is characterized by the fact that previously the emphasis was on the conventional military dimension. Today this dimension is no longer the only obvious one, even if there are still theaters of war. Threats and risks to the security of states have changed quite a lot, in particular a multitude of risks and threats of asymmetric type have emerged. For example - illegal and secret migration, terrorist threats, hybrid actions, cyber attacks, incidents from within; threats associated with spontaneous new technologies (such as drones, 5G, artificial intelligence); challenges related to climate change; disruption of supply chains; and interference in the electoral process. Speaking about the crisis caused by the COVID-19 pandemic, it has put a strong focus on the security of individual states, but also on European security, testing the capacity of Europe's critical infrastructure, crisis preparedness, strategic value chains and crisis management systems, as well as the ability of our societies to resist manipulative intersections and

disinformation. These challenges also occur beyond our borders, with a clear interconnection between internal and external security.

According to the European Security Strategy at the Romanian Dialogues@MAE, the European Union has sought to adapt to the new security environment and has made a number of significant advances, such as the adoption, in December 2013, of the Comprehensive Approach [4] to external conflicts and crises, which is already being implemented in the Horn of Africa or the Sahel region, the Maritime Security Strategy and the related Action Plan, or the Strategy and Action Plan for the Gulf of Guinea. A Political Framework on Systematic and Long-Term Defence Cooperation, as well as the Political Framework on Cyber Defence, were also adopted, both of which will play an important role in the efforts to strengthen the Union's military and cyber capabilities. Furthermore, in response to concerns over gas supplies, the EU launched its own energy security strategy in 2014. This includes measures such as increasing energy efficiency, producing its own energy and completing infrastructure connections to redirect energy resources in the event of a potential crisis.

But let's talk about national security. National security is not

only a concern of the state, but also of its citizens, and security culture plays an essential role in their involvement in ensuring stability and protecting national values. This culture emerges from the experience and consciousness of citizens and encompasses cognitive, evaluative and emotional aspects, influencing the way they perceive and respond to threats. Along with cognitive and informational aspects, security culture is closely linked to the concept of strategic culture, which refers to ideas, emotional and behavioral reactions related to threats.

2. SECURITY CULTURE

Security culture represents the active and conscious commitment of citizens in managing state issues and supporting institutions in preventing threats to national security.

According to sociological surveys [6], external propaganda is seen as an effective tool of manipulation, especially in the context of the lack of information regarding the real state of affairs in the world, as well as in the immediate vicinity of our state.

Scientific researcher, first degree, National Intelligence Academy "Mihai Viteazul", National Defense University Carol I, Ruxandra Buluc, defines security culture as "the result of social interactions that

take place in groups, organizations, communities, societies concerned with social security issues, which have in common certain learning and knowledge accumulation processes in accordance with the requirements of individuals regarding trust, protection and safety" (Buluc et al. 2019). Security culture is the end result of security education, including through continuing education, by promoting values, norms, attitudes and actions related to the assimilation of the concept of national security.

A good example of education through the practical implementation of security culture within society is Finland. This country has a long history of prioritizing national security and promoting a strong sense of civic duty among its citizens. For example, Finland's Total Defense Concept represents an approach to national security that extends beyond traditional military defense to encompass all aspects of returning to normality in society. In Finland, military service is mandatory for almost all male citizens, which strengthens the country's defense capabilities and cultivates a sense of responsibility among the population. In addition, Finland attaches great importance to the preparation of citizens in the field of civil protection, providing citizens with training in emergency situations and first aid.

The Finnish government invests in public education campaigns aimed at informing citizens about security threats and the importance of preparation. By collaborating with communities and civil society organizations, the Government strengthens the resilience of its society in the face of external threats. [8]. The military conflict in Ukraine directly affects the security of the states in the Black Sea region, as well as neighboring countries. Analyzing the current political and military situation in Ukraine, we come to the conclusion that every state in the world, especially those in the former USSR – must be able to provide guarantees for the security (protection) of its population. But there are 21 countries in the world without armed forces, which have either given up or been forced to disband their own armies, which does not increase the security of the respective states. Many of the 21 countries have typically had a long-standing agreement with a former occupying country; an example of this is the agreement between Monaco and France[10], which has existed for at least 300 years.[1] The Marshall Islands[11], Micronesia, Monaco and Palau[12,13] do not have the right to a say in their country's defense. Thus, they have little influence in international relations.

These are just a series of examples that support the need for a new approach to security culture and the preparation of a nation to cope with the changes generated by the evolution of the security environment.

The basis of building a developed, strong, democratic society is the population of this country. Namely, each individual citizen represents the brick that underlies the fortress and the building of a strong society is done only through education. A society built on values, skills, patriotism, integrity and strategic vision is a society that can guarantee the rule of law, safety and national security. The quality of human capital is the key factor for economic and non-economic development, such as improved health, civic and social involvement, a better climate of security and social comfort. Education is not only a good and an end in itself, but, in the long term, the most important factor for the sustainable development of the country. By virtue of large time lags between the allocation of resources and the achievement of results, the education sector requires interventions and support as early as possible to face the new challenges of the contemporary world. Surely an educated population, with an advanced security culture, will never

be easy to manipulate or lure into the net of lies and threats [9 p.279]. Therefore, the security culture, through understood and correct education, significantly increases national security.

If we refer to the states that have achieved a high level of security culture, then according to the analyses in the field, we can talk about Norway. This country, through large investments in its civil and military training and through close collaboration between the civil community and state authorities, has managed to adapt to regional threats, maintaining a stable balance and strengthening its national security. Poland, in turn, has strengthened its security culture by promoting education and awareness of its importance among the population. Investments in defense and close collaboration with NATO allies have strengthened the country's resistance against external threats, including with regard to challenges in cyberspace and adversary propaganda.

Similarly, Estonia, which was aware of its vulnerabilities, invested heavily in cybersecurity and in strengthening cooperation with NATO and EU partners. Estonia has countered cyber threats and unfavorable external influence, namely through

education, awareness and advanced technologies.

It is interesting how security culture is promoted in neighboring countries, in the immediate vicinity of the Republic of Moldova, for example in Romania. According to the magazine "Security Culture. Sources and Resources". Intelligence at your service. <https://intelligence.sri.ro/cultura-de-securitate-surse-si-resurse>, in Romania, citizens have the opportunity to create a solid security culture both through the use of open sources and thanks to the efforts of an authority such as the Romanian Intelligence Service. SRI is concerned with achieving security education, through the use of several training means, with the involvement of OSINT, but also through concrete actions, such as: meetings with civil society representatives, round tables, conferences, debates or various partnerships with academic or research institutions, scientific communication sessions. The "Terrorism Near Us" campaign, carried out between 2004 and 2010, had as its target audience public authorities, pupils, high school students, students and took place in the form of information sessions both in Bucharest and in other cities, with the aim of presenting the danger of terrorism. The "SRI in 50 minutes" series of meetings, launched by

SRI in 2013, presented students and teachers with new information about SRI, about the risks specific to the current security environment, offering recommendations on how to react in certain risky situations. The round table on the theme "Society, Democracy, Intelligence" (2008) had among its objectives the assessment of civil society's expectations and perceptions of SRI's activity, as well as the need to strengthen public communication in the area of intelligence. We can also mention the debate "Social Media Evolution: A Look into the Future" (2015), on the topic of risks felt at the level of society with the revolutionization of relational thinking and communication under the impact of social media. [7].

The references to the nominated countries provide useful benchmarks for the development of security culture.

State security is an integral part of national security.

An important role in ensuring state security belongs to Civil Protection.

3. STATE SECURITY AND CIVIL PROTECTION

A component of state security is Civil Protection. This essential component of national security has the role of preventing and managing

disasters through organizational, technical and informational measures of a humanitarian nature, aimed at protecting the population and material assets. Civil Protection is not a separate entity, but an integrated pillar in the security strategy of a state, its activities being carried out through a multitude of planned and coordinated actions.

We refer to the state's possibilities to react correctly and promptly in the early phase of the escalation of Exceptional Situations of a conflict nature (combat actions). According to the Law of the Republic of Moldova "On Civil Protection" No. 271-XIII of 09.11.1994, Civil Protection of the Republic of Moldova is a system of measures and actions, undertaken on a state-wide scale in peacetime and wartime, in order to ensure the protection of the population, property in the event of natural and ecological disasters, accidents and catastrophes, epiphytotics, epizootics (ext. some contagious diseases), fires, as well as in the case of the application of modern means of destruction. Civil Protection is organized according to the territorial principle throughout the territory of the Republic of Moldova in accordance with the existing state system and administrative leadership. [1, art.4]. Protection of the population in the event of the occurrence of exceptional situations

(conflict and non-conflict) from the damaging factors of catastrophes natural and technological and uninterrupted work of objects, are tasks of great importance for all local public management bodies, executive bodies and managers of objects of the national economy. The direct management of the civil protection system is the task of the General Inspectorate for Emergency Situations. [2, art.8]. The performance of service within the Service by citizens of the Republic of Moldova is carried out in accordance with the legislation in force [2, art.17]. In the Government Decision № 282 of 14.03.2005 for the approval of the Regulation on training in the field of civil protection, published: 25.03.2005 in the Official Gazette No. 46-50 art. No. 338, the categories of the population mandatorily involved *in the training process in the field of civil protection*, as well as the tasks and basic forms of training the population for actions in case of exceptional situations, this being a component part of national security.

Security culture plays an essential role in involving citizens in ensuring stability and protecting national values. This culture arises from the knowledge, awareness and experience of citizens and includes practical and emotional aspects, influencing the way in which they are likely to respond to potential threats.

Thus: 1. In the process of training in the field of civil protection, the following are trained:

- a. heads of public administration authorities (hereinafter - chairmen of emergency committees);
- b. employees of public administration authorities, including those authorized to resolve issues related to the prevention and liquidation of the consequences of exceptional situations (hereinafter - authorized employees);
- c. persons trained in the sphere of production and service, who are part of civil protection formations (hereinafter - the staff of civil protection formations);
- d. persons trained in the sphere of production and service, who are not part of the governing bodies and civil protection formations (hereinafter - the employed population);
- e. persons not trained in the sphere of production and service (hereinafter - the unemployed population);
- f. persons studying in educational institutions, regardless of their profile, type of ownership and organizational-legal form (hereinafter - pupils and students).

2. The basic tasks of training in the field of civil protection are:

- a. training of all categories of the population on the rules of conduct and the main methods of protection in case of exceptional situations, methods of providing first aid, rules for the use of individual and collective means of protection;
- b. training (advancing) of leaders of all levels on actions related to the protection of the population and the territory in case of exceptional situations;
- c. training of leaders and employees of public administration authorities, enterprises, institutions and organizations in the skills of training and management of forces and means belonging to the civil protection system;
- d. the acquisition by the employees of the civil protection forces of their obligations and their training for actions in case of exceptional situations;
- e. the knowledge by the students of the destructive factors of the possible exceptional situations on the territory of the country, of the rules of conduct, the acquisition of the notions of providing self-help and medical aid;

f. the knowledge by the students of the international conventions and the legislation of the Republic of Moldova in the field of civil protection, of the principles of organizing the protection of the population, material goods and cultural values of the country, the ways and means of functioning of the national economy in exceptional situations. [3,p.1, 2].

Strategic Culture shapes national security concepts, military doctrines, organizational structures of the armed forces, weapons systems, war styles, and almost every other aspect of a state's defense policy and strategic behavior. However, it is difficult to define and identify strategic culture in a systematic way, and researchers discuss several definitions of the concept.

4. STRATEGIC CULTURE

In 1977, the American political scientist Jack Snyder, in his research works, developed the concept of strategic culture, in which he tried to understand and explain the culture and behavior of leaders soviet, compared to American, in the context of the Cold War; this is considered a precursor of the concept of security culture (Lantis 2002, 87-113).

Strategic culture represents a system of strategic values, combined with:

- a system of experiences and realities of present and future requirements;
- a system of projecting the value effect in the dynamics of action and;
- a system of evaluation and forecasting of military action for the implementation of a political decision.

In other words, strategic culture is dependent on political culture, which reflects the aspirations of the people, the specifics of society. If a society does not register its culture, then no achievements take place and no changes occur. Strategic culture is also dependent on economic culture, which refers to the knowledge, beliefs, attitudes and behaviors that influence the economic actions and decisions of individuals and society. It includes not only the technical aspects of the economy, but also the moral and social dimensions, explaining why people act differently in different economic contexts. Strategic culture is also dependent on social culture, which refers to the totality of norms, values, beliefs, customs, knowledge, arts and institutions specific to a human group or society. This not only shapes social behavior, but also influences the

way in which individuals interact, organize themselves and perceive the world around them.

Thus, *Strategic Culture* is presented as a *system of systems*, therefore as a metasystem, with complex functions in: *strategic theory; strategic art; and in strategic practice*.

But, strategic culture is not subordinate to political culture and is not part of it, it is only an instrument of it. Strategic culture is presented as interdisciplinary, dependent on other cultures, resulting from the interconditioning of the three major components of strategy, namely: strategic theory; strategic art and strategic practice.

Strategic cultures have been created by all strategic schools in the world. In the methods of preparing and conducting wars, reference is not always made to the concept of "strategic culture", but this does not mean that without a good strategic culture, there can be something qualitative and sustainable, in terms of the theory, art and practice of war.

In other words, the quality of war depends, to a large extent, on the quality of the strategic culture that supports and sustains it. This connection between security culture and strategic culture highlights the importance of the emotional and behavioral influence on the individual

and collective reactions of citizens to various security situations. But in order to proceed (act) correctly in such situations, permanent training (education) is necessary.

Therefore, education plays a fundamental role in building a culture in general and a security culture in particular, which allows society to thrive safely and dynamically adapt to the rapid changes in the national and international security environment. In this regard, close collaboration between educational and law enforcement institutions is necessary to ensure the importance, updating and application of education programs in the real context of security threats. Therefore, security culture is vital in the information age we are living in, in which we all need orientation points both at the personal and state levels.

5. CONCLUSIONS

According to the security and StratCom expert, Elena Mârzac, in the Republic of Moldova there is a low level of information, poor institutional transparency and inadequate communication in the security sector, which requires better awareness and access to information. It is vital to ensure a general understanding of security and its importance for the democratic development of the state. The involvement of civil society and non-

governmental organizations in the reform of the security sector is also crucial.

Given the linguistic and cultural diversity, communication should be adapted with information available in Romanian and Russian, in order to reach all segments of the population and to promote active participation of citizens. Every citizen can contribute to this effort by adopting preventive behavior and reporting suspicious activities.

To build a strong strategic and security culture, an education is needed that would allow society to thrive safely and adapt to the rapid changes in the security environment. Close collaboration between educational and law enforcement institutions is necessary to ensure the relevance, updating and application of education programs in the real context of security threats. A society built on values, skills, patriotism, integrity and strategic vision is a society that can guarantee the rule of law, national safety and security. Thus, education in the field of national security, through the development and reception of security culture, is a necessity for the population.

Strategic culture and security culture are topics that represent a theme of deep research in the future. Thus, their awareness and correct understanding will allow us to

preserve our national values, ideals, customs and traditions as a nation and as a country for future generations.

REFERENCES

- [1] *Law of the Republic of Moldova On Civil Protection* No. 271-XIII of 09.11.1994;
- [2] *Law on the Civil Protection and Emergency Situations Service* No. 93-XVI of 05.04.2007 Official Gazette No. 78-81/358 of 08.06.2007;
- [3] Decision of the government of the republic of Macedonia for the approval of the *Regulation on the manner of performing the special service within the Civil Protection and Emergency Situations Service* no. 461 of 24.03.2008 Official Gazette no. 66-68/436 of 01.04.2008;
- [4] The Comprehensive Approach to external conflicts and crises, presented in December 2013, aims at the coordinated and coherent use in external theaters and starting from local realities, of all instruments at the disposal of the EU: diplomatic, economic, humanitarian and in the development sphere;
- [5] Almond, G., & Verba, S. (1963). *The civic culture: Political attitudes and democracy in five nations*. Princeton, NJ: Princeton University Press;
- [6] Public Opinion Barometer, *Survey. CBS-Axa Research*, 2023. Available: https://ipp.md/wp-content/uploads/2023/09/BOP_08.2023.pdf and Public Perceptions on the

- Security and Defense System of the Republic of Moldova, *Survey. CBSAxa Research*, October 2022. Available: https://pisa.md/wp-content/uploads/2023/02/6_Studiu-Sociologic-Perceptii-publice-asuprasistemului-de-securitate-si-aparare-al-RM.pdf;
- [7] Calangea, Claudia-Diana. 2017. *Security Culture. Sources and Resources. Intelligence at Your Service*. <https://intelligence.sri.ro/cultura-de-securitate-surse-si-resurse>;
- [8] Elena Mârzac, 2024, *Security Culture. Security Education: An Imperative for Moldovan Citizens*. The material was developed in the context of the project “Information Campaign on the Objectives of Security Policies in the Republic of Moldova” implemented by the Platform for Security and Defense Initiatives and supported by DCAF - the Geneva Center for Security Sector Governance, within the project “Strengthening Security Sector Governance in Moldova”, funded by Sweden.
- [9] Liudmila Curoș, *Education – an instrument in ensuring national security*, in the materials of the International Scientific Conference “European Union Security Strategy in the Context of the Metamorphoses of International Relations” (II) CZU 37:351.86
- [10] *Monaco Signs New Treaty with France*. Consulate of Monaco. Archived from the original on October 21, 2007. Retrieved March 29, 2009.
- [11] *On the Marshall Islands*. U.S. Department of State. Retrieved March 29, 2009.
- [12] *Inspection of the Embassy of Kolonia, Federated States of Micronesia*. U.S. Department of State. Archived from the original on August 29, 2007. Retrieved March 29, 2009.
- [13] *Palau - Defense*. Encyclopedia of the Nations. Retrieved March 29, 2009.

ORGANIZATIONAL RESOURCE MANAGEMENT AND ENVIRONMENTAL SUSTAINABILITY. A TIME-SERIES ANALYSIS OF ICT SECTOR GREENHOUSE GAS EMISSIONS IN ROMANIA (2013-2022)

Cristina ANTONOAIIE, Aura CODREANU

Regional Department of Defense Resources Management Studies,
Brasov, Romania

The impact of the Information and Communication Technology (ICT) sector has a complex nature. While on one hand it boosts the digital transformation of organizations and countries' economic growth, on the other hand it has negative environmental impact as a result of its overall contribution to global greenhouse gas emission. The goal of this paper is to provide insights on how to better reconfigure organizational resource management by marrying environmental sustainability goals with the enhanced usage of information technology and information systems in streamlining and optimizing organizational processes. To this end, it provides a comprehensive literature review that approaches ICT as an organizational resource, as well as a time series analysis of Romania's ICT sector's greenhouse gas emission from 2013 to 2022. Its recommendations underline the ongoing need for Romanian organizations deploying ICT for digital transformation to observe climate objectives concurrently and hence, better integrate ICT as an organizational resource and capability.

Key words: *Information and Communication Technology, ICT environmental impact, greenhouse gas emissions, sustainable ICT, organizational resources, total cost of ownership.*

1. INTRODUCTION

Greenhouse gas emissions and air pollutants resulting from production processes – including those within the Information and Communication Technology (ICT) sector – contribute

to climate change, pose risks to human health, and negatively affect the environment and biodiversity. Therefore, it is essential to create synergies between the digital and green transitions: promoting the

widespread adoption of low-carbon digital solutions across all sectors while simultaneously working to minimize the environmental footprint of the ICT sector itself.

Understanding the ICT sector's contribution to air emissions is a crucial first step in assessing the broader environmental impacts of digitalization.

According to the OECD definition (OECD, 2025:12), the Information and Communication Technology (ICT) sector comprises manufacturing, trade and services industries. In terms of manufacturing, the ICT sector includes the production of components, computers, communication equipment, consumer electronics, and magnetic and optical media, while the trade component focuses on the wholesale of those products. Concerning the services part, ICT includes software publishing, computer programming, consultancy, facilities management, data processing, hosting services, web portals, and repair services for computers and communication equipment. An important component of those is represented by telecommunications activities which include wired, wireless, satellite, and other telecommunication operations.

The ICT sector plays a major role in digital transformation and economic development in countries like Taiwan, Malaysia or India. Additionally, the ICT sector is an

important innovation driver for emerging technologies like artificial intelligence and 5G and renewable energy technologies. All of the above considered, the environmental impact of ICT has become one of the major concerns nowadays. According to World Bank and International Telecommunication Union estimates, the ICT sector contribution to global GHG emissions is between 1.5% and 4% - (World Bank & International Telecommunication Union, 2025), on par with the aviation industry. The increased focus on this issue is justified by the steep rise in digital infrastructure represented by data centers, telecom networks and connected devices as a result of implementation or adoption of IoT, 5G, and edge computing (Grand View Research, 2024; Precedence Research, 2025; IoT Analytics, 2024). Additionally, ICT lifecycle leaves significant environmental footprints (UK Government, 2025; Balde et al., 2023). Nonetheless, ICT plays a dual role and its positive impact is visible in its contribution to energy efficiency and digital innovation (International Telecommunication Union, 2024; The Shift Project & GreenIT, 2019).

All of the above considered, the focus of this study is to analyze the impact of air emissions from the ICT sector in Romania for the 2013-2022 time period. The research question is how ICT environmental

impact can be strategically managed. The objectives are therefore two-fold. The literature review aims at providing a comprehensive outlook on how to balance ICT as a critical resource in organizations from the perspective of its positive and negative impact on environment, the direct, indirect and environmental costs associated with ICT sector's energy consumption, regulatory compliance and reputational risks, structured approaches to establishing cross-functional capabilities and leadership commitment to ensure the success of Green IT and Green IS initiatives in the context of optimized organizational capabilities. The second objective of the study is to analyze the environmental impact of greenhouse gas emissions of the ICT sector in Romania between 2013 and 2022 by using average time series indicators such as mean emissions per capita, absolute changes, dynamic indices, and growth rhythms in order to substantiate future implementation of recommendations on how sustainable ICT practices can mitigate the sector's expanding carbon footprint while supporting the country's digital transformation objectives.

2. LITERATURE REVIEW

In order to understand the environmental impact of ICT sector greenhouse gas emissions

on organizational resources and underpinning management practices, we will focus on four inter-related research strands, namely resource-based view (RBV) and its extension – the natural resource-based view (NRBV), total cost of ownership (TCO), green IT and green IS, and organizational capability development. All of them allow for approaching ICT infrastructure from a strategic perspective that requires complex management strategies. Thus, the RBV and NRBV frameworks allow us to analyze ICT infrastructure as a critical organizational resource that entails both a strategic approach to its management along with the inclusion of environmental sustainability considerations (Barney, 1991; Hart, 1995; Wade & Hulland, 2004). Such a perspective allows for further consideration of how digital resources can be managed not only as productivity boosters, but also as assets whose environmental footprint can impact an organization's long term competitive advantage (Hart & Dowell, 2011). Additionally, we resort to the TCO conceptual framework in order to expand the traditional life cycle approach that focuses on acquisitions and operational costs by showing how greenhouse gas emissions contribute to direct and indirect organizational costs generated by

energy consumption, carbon pricing mechanisms, regulatory compliance, and reputational risks (Ellram, 1995; Curry & Donnellan, 2012). Also, the Green IT and Green IS frameworks contribute to this literature review through the structured approaches by which they enable organizations to decrease their IT and IS related environmental footprint and employ digital technologies for sustainability purposes (Watson et al., 2010; Melville, 2010; Seidel et al., 2013). Last but not the least, the concepts that fall under the umbrella of organizational capability development contribute to identifying the main actions that can be undertaken by organizations to develop and use capabilities that secure environmental sustainability (Teece, 2007; Chen et al., 2015; Nishant et al., 2016). The above proposed theoretical frameworks are aimed at approaching ICT sector emissions as a critical organizational resource that requires a strategic focus, along with comprehensive cost estimates, structured approaches to implementation and a sustainable approach to capability development. They also contribute to contextualizing our findings related to Romania's ICT sector emissions within the debates on sustainable digital transformation and the related environmental responsibility of organizations.

2.1. Resource Based View (RBV) & Natural Resource Based View (NRBV)

According to the Resource-Based View (RBV) perspective, an organization's critical resources and capabilities underpin its competitive advantage as long as the management strategies deployed focus on treating them as valuable, rare, inimitable, and non-substitutable (VRIN) (Barney, 1991). In this context, as literature in the field shows, ICT represents a critical organizational resource (Barney, 1991; Wade & Hulland, 2004) whose major role in achieving competitive advantage is particularly underlined by contemporary concerns regarding the necessity to balance digital transformation objectives with environmental sustainability goals (Dao et al., 2011; Melville, 2010). Nonetheless, ICT represented by its various platforms – hardware (computers, servers, network devices), software (enterprise applications, operating systems), network and telecommunications (internet, WAN, LAN), as well as by data storage systems, cloud services, security infrastructure (firewall, Encryption, antivirus) cannot be treated as a critical organizational resource in the absence of solid management frameworks. What is more, the effective development and consolidation of the latter is very much dependent on contemporary

concerns over environmental sustainability. Henceforth, the conceptual delineations provided by the Natural Resource-Based View (NRBV) approach contribute to refining the management practices aimed at integrating such approaches into competitive advantage focused strategies for managing organizational resources (Hart, 1995; Hart & Dowell, 2011). In this context, the NRBV highlights the ways in which organizations can reduce their carbon footprint by strategically managing their digital resources through the adoption of low-carbon technologies and green innovation.

ICT faces a two-fold imperative: to remain a strategic organizational asset considering the latest developments in IT infrastructure (i.e. data centers, communication networks, computing devices, software systems), while not becoming a liability (Malmudin & Lundén, 2018) as a result of its huge consumption of energy and generation of substantial greenhouse gas emissions. Sustainability commitments, regulatory requirements, environmentally-conscious markets make the NRBV salient for how organizations reconfigure their strategic approach to achieving competitive advantage by leveraging the power of ICT.

As a World Bank 2024 report shows, the ICT sector contributes at least 1.7% of global greenhouse

gas (GHG) emissions, a share comparable to the aviation industry, while between 2018 and 2022, there has been an increase in ICT sector energy demand and emissions as a result of a 72% increase in data center connectivity, 14% increase in broadband subscriptions and 17% rise in the number of internet users. On the other hand, worth mentioning, as the report highlights, 60% of the renewable power purchases in 2021 were made by tech companies which represented some of the top global electricity consumers adopting renewable energy. Also, some of the European Commission's Joint Research Centre (JRC) show mixed data about the Janus like opportunities and challenges raised by ICT. For example, according to the 2021 ICT TASK FORCE STUDY, ICT infrastructure (data centers and telecommunication networks) accounted for 79% of overall ICT emissions in 2020, up from 61% in 2010. Also, the life cycle of ICT devices – from material extraction, manufacturing, use, to end-of-life – generates significant material and emission footprints. The carbon footprint for manufacturing such devices has doubled between 1995 and 2015, accounting for about 2% of global climate impacts in 2015. In relation to that, the number of connected devices is rapidly growing, with an estimated 41.6 billion connected devices worldwide

by 2025, driving increased data production, storage, and transmission. However, ICT has been proven to play a major role in society, especially during the COVID-19 pandemic, by enabling connectivity and supporting economic and social functions. In conclusion, as this study shows ICT has a direct life cycle impact in terms of resource consumption and disposal rate, but also positive and negative effects from its use, as well as systemic socio-economic impacts – all of which underscore its dual nature. Therefore, the management of ICT as a strategic resource organization wide needs to take into consideration both its role as an enabler of future efficiency and effectiveness focused solutions, but also as a driver of environmental changes. Therefore, from such a perspective, integrated policy measures should be envisaged in order to ensure ICT sustainability as a system and across its lifecycle.

2.2. Total Cost Of Ownership (TCO)

The Total Cost of Ownership (TCO) approach represents a comprehensive framework that supports a full scale depiction of the economic implications that the use of ICT resources has across a product's lifecycle (Ellram, 1995; Ellram & Siferd, 1998). Its initial application concerned the direct and indirect financial costs associated with the

acquisition, deployment, operation, maintenance and disposal of assets. Nowadays, TCO also includes environmental factors that account for cost breakdown (Ferrin & Plank, 2002; Heilala et al., 2006), such as energy costs, carbon and emissions taxes, regulatory compliance, reputational risks and uncertainty about the future of technology such as artificial intelligence (Molla, 2009; Curry et al., 2012).

For example, the UK Government's "Total Cost of Ownership" guide emphasizes evaluating not just initial purchase costs of ICT solutions, but also ongoing operational, maintenance, transition, and environmental costs—including energy consumption and disposal—over the entire lifecycle to ensure value for money in public sector investments.

Also, the 2024 United States Data Center Energy Usage Report highlights that data center data center energy consumption continues to be a significant portion of operating expenses, with combined energy use of servers, storage, network equipment, and infrastructure rising steadily. In this respect, energy costs represent a substantial share of total operational costs, driven by growing demand for data services and increased compute workloads. Therefore, as per this report's findings, energy consumption patterns and projections should be

included in comprehensive TCO analyses for data center planning and management. What is more, as per the projections of the International Energy Agency (IEA), global electricity demand from data centers will more than double by 2030 due to AI and other digital services, with renewables expected to supply up to half that energy by decade's end. That is tightly related to the inclusion in the TCO of the operating expenses tied to energy consumption.

Additionally, based on the JRC ICT Task Force report for environmental and operational cost components, ICT contributes to greenhouse gas emissions as a result of its production and use. In terms of the finite resources it uses, their exploitation generates air, soil and water pollution. Its use is heavily dependent on energy consumption, while the fast update and evolution of technology makes the amount of ICT waste increase exponentially. Last but not the least, its disposal is prone to generating potentially hazardous waste since ICT recycling rates are very low globally and 80% of ICT waste worldwide remains undocumented.

Therefore, the integration of environmental costs into the ICT TCO could contribute to informed decision making concerning how to balance expenditures on energy-efficient infrastructure with environmental and energy costs.

Worth mentioning is that investment in renewable energy and technology meant to reduce emissions contribute to reductions in long-term costs (Elliot & Binney, 2008; Dedrick, 2010) and secure against the likely increase in energy prices as a result of foreseeable spikes in the demand.

In conclusion, TCO frameworks need to be updated in order to include environmental costs arising from observing compliance and security regulations on greenhouse gas emissions, sustainable approaches to ICT end of life, risk management plans on direct and ICT indirect environmental impact, direct environmental costs related to carbon pricing, emissions trading, and sustainability reporting. That welcomes an integrated approach that aligns the allocation of organizational resources to the sustainability goal. In this way, ICT can be both a key cost factor, but also an enabler of a sustainable organizational strategy.

2.3. Green IT and Green IS frameworks

The management of organizations' environmental impact as a result of their information technology and information systems is best known by the names of Green IT and Green IS. While the former is focused on practices to manage technology lifecycle, the latter emphasize the role of information systems in supporting sustainable

organizational processes and practices. Green IT models propose solutions aimed at optimizing IT infrastructure through the use of energy-efficient hardware, renewable energy deployment, managing and decreasing the amount of e-waste. From this perspective they are more concerned with technology and operations design, as well as disposal management strategies with a view to diminishing IT environmental footprint. Among the challenges of adopting green IT practices, the most prominent are change management practices and infrastructure compatibility. On the other hand, Green IS models take an organizational and societal approach by integrating behavioral, technological and environmental aspects (Wang et al. 2015; Loeser 2013)

The Green IT Readiness model by Molla et al (2009, 2011) describes an organization's readiness to integrate IT with a focus on its environmental impact across four dimensions: attitudes – the beliefs about and commitment to environment – policy expressed as governance structure and standards, practices that demonstrate the implementation of environmentally focused IT initiatives, and technology – in terms of its availability and use of energy-efficient solutions. According to this model, Green IT initiatives require a coordinated approach

spanning all four dimensions rather than piecemeal, isolated approaches (Molla & Abareshi, 2012).

The Energy Informatics Framework proposed by Watson et al highlights IT's two pronged role: as an environmental challenge – Green IT and as a solution – Green by IT. Consequently, it addresses IT both from the perspective of its impact on environment, but also as a facilitator of solutions organization wide by which organizational processes and societal systems in general can benefit from the use of IT. The framework was subsequently used for enhancing IT lifecycle and end-of-life approaches (Berthon & Donnellan, 2011; Dao et al., 2011).

A framework that links organizational transformation to organizational change theory and that highlights the need for a more comprehensive approach to transformation belongs to Seidel et al.'s (2013). Their research underlines that Green IS needs to be connected to broader organizational practices encompassing people, processes, culture besides technological infrastructure (Seidel et al., 2017). In a transformational context that includes environmental concerns, the role of IS is three fold: to facilitate organizational members' sense making of environmental issues, to ensure transparency of environmental impacts and to support new practices and business models that reduce environmental impact.

Loeser et al. (2017) capitalize on Jenkin et al.'s (2011) research agenda for Green IT and develop a framework for linking Green IT strategies to environmental sustainability strategies. They describe efficiency oriented strategies aimed at reducing resource consumption, effectiveness oriented strategies with a role in securing business models' sustainability and innovation-oriented strategies focused on the development of new green products and services for which IT is an enabler.

The goal of overviewing the key approaches in the field of Green IT and Green IS is to highlight that efficiency and effectiveness approaches need to be part of a joint effort and undertaken strategic wise. Also, Green IT and Green IS as concepts and practices require that besides technical expertise, stakeholder engagement and management commitment are secured.

2.4. Organizational capability development for gas emissions reduction

Development or consolidation of organizational capabilities can be better approached from the perspective of international standards in the field, such as the Greenhouse Gas (GHG) Protocol Corporate Accounting and Reporting Standard (GHG Protocol, 2004)

used by companies to calculate their carbon dioxide emissions, or reports of entities like The International Telecommunication Union (ITU) and the World Benchmarking Alliance (WBA) who issue reports like the Greening Digital Companies 2025: Monitoring emissions and climate commitments, or Measuring the Emissions & Energy Footprint of the ICT Sector. Implications for Climate Actions (ITU & World Bank, 2023; ITU & WBA, 2025).

Digital companies in particular use the Greenhouse Gas (GHG) Protocol Corporate Accounting and Reporting Standard to calculate their carbon dioxide emissions across Scope 1 (direct emissions), Scope 2 (indirect emissions from purchased energy), and Scope 3 (value chain emissions) categories (GHG Protocol, 2004; 2011). The latter looks at organizational capabilities in terms of designing organizational goals and inventory (Chapter 2) organizational boundaries (Chapter 3), and managing inventory quality (Chapter 7). Organizational boundaries support business and not only to identify the specific entities or operations for which an organization accounts for GHG in its inventory. In this respect, capability development concerns the capacity of an organization to report emissions accurately across equity share or control based functional structures. Establishing boundaries

heavily relies on the context in which an organization operates, its legal framework and structure, operational control, company ownership – all of which need coordination across multiple teams – accounting, legal and operational – for GHG accounting purposes (GHG Protocol, 2004, Chapter 3).

The development of a comprehensive GHG inventory for a given organization requires adequate capabilities to monitor, collect, analyze and report data for decision-making purposes. The principles emphasized by the GHG protocol related to the development and maintenance of organizational capability targeting GHG emissions are transparency, completeness, and accuracy and they can be sustained through rigorous data governance, internal controls and emissions reporting. GHG Protocol is supplemented by ISO 14064-1: Organizational-level GHG emissions quantification and reporting (ISO, 2018).

Development or consolidation of organizational capabilities for the ICT sector can be better approached through specialized frameworks that address the unique challenges of digital technologies. The GHG Protocol ICT Sector Guidance (2017) offers methodologies tailored to telecommunications networks, data centers, hardware, and software, recognizing complexities such as extensive supply chains, shared

infrastructure requiring sophisticated allocation methods, and the dual nature of ICT's environmental impact – both its direct emissions and its enabling effects that can reduce emissions in other sectors. Capability development in this context requires expertise in life cycle assessment, allocation methodologies for shared resources, and measurement of both environmental footprint and handprint (GHG Protocol, 2017).

The Science Based Targets initiative (SBTi) further shapes capability requirements by establishing emission reduction targets aligned with limiting global temperature increase to 1.5°C. The SBTi ICT Sector Guidance provides decarbonization pathways specifically for network operators and data center operators, acknowledging challenges like rapid technology evolution and the critical importance of addressing Scope 3 emissions (GSMA et al., 2024). Meeting these requirements involves building capabilities in strategic planning, scenario analysis, supplier engagement, and transparent reporting.

Scope 3 emissions management presents a particularly demanding capability area given that value chain emissions typically represent 80-90% of total emissions for ICT companies. The GHG Protocol Scope 3 Standard outlines fifteen emission categories across upstream and downstream activities (GHG Protocol, 2011),

while the GSMA Scope 3 Guidance for Communication Operators offers practical methodologies for telecommunications companies (GSMA et al., 2023). Capability development here concerns establishing supplier data collection systems, developing product life cycle assessment expertise, creating customer engagement mechanisms, and building collaborative platforms.

Data management capabilities form the foundation of all emissions management activities. Organizations need systems for collecting activity data, applying emission factors, calculating emissions across all scopes, and maintaining data quality through validation processes (GHG Protocol, 2004, Chapter 7). More advanced organizations implement automated data collection, integrate emissions data with enterprise systems, and deploy AI/ML for data quality assurance. The ITU-T L.1410 standard provides specific guidance on data requirements for ICT equipment, networks, and services (ITU-T, 2014).

Beyond technical expertise, organizational capacity requires governance structures, leadership commitment, and cultural transformation. Leading organizations establish dedicated sustainability functions with board-level oversight, integrate climate targets into executive compensation, and embed environmental considerations into procurement and

product development processes (Watson et al., 2010; Jenkin et al., 2011). The Green IT Readiness model emphasizes coordinated development by addressing attitudes, policies, practices, and technology at the same time (Molla et al., 2011).

3. METHOD

For the analysis of the data we used the average indicators of time series for the years 2013 to 2022 in Romania.

We calculated the mean

$$\bar{y} = \frac{\sum_{t=1}^n y_t}{n} \quad (1), \text{ the average of absolute change}$$

$$\bar{\Delta} = \frac{\sum_{t=2}^n \Delta_{t/t-1}}{n-1} = \frac{\Delta_{n/1}}{n-1} \quad (2), \text{ the average of dynamic indices}$$

$$\bar{i} = \sqrt[n-1]{\prod_{t=2}^n i_{t/t-1}} = \sqrt[n-1]{i_{n/1}} \quad (3) \text{ and}$$

the average rhythm of changing

$$\bar{r}_{\%} = \bar{i}_{\%} - 100 \quad (4).$$

4. RESULTS AND DISCUSSION

Air emissions from the ICT sector are divided into five distinct categories, which we will analyze one by one.

4.1. 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) in kilograms per capita

The mean signifies that the average greenhouse gas emissions per capita in the ICT sector is 24.3 kg CO₂ equivalent. This serves as a reference average value for the country analyzed.

Table 1 The average indicators of time series for greenhouse gases

the mean	24.300
the average of absolute change	0.656
the average of dynamic indices	1.028
the average rhythm of changing	2.777

The average of absolute change (0.656) represents the average absolute change in emissions between periods (likely between years). A small value suggests that annual variations in ICT sector emissions are relatively steady and not very large.

The average of dynamic indices (1.028) – a dynamic index above 1 indicates a slight average increase in emissions. Essentially, emissions in the ICT sector are growing on average by about 2.8% annually – idea confirmed also by the average rhythm of changing (2.777%).

We also did a graphic analysis of the evolution of the greenhouse gases air emissions from the ICT sector in Romania. The emissions increased from 21.1 kg in 2013 to 27.0 kg in 2022.

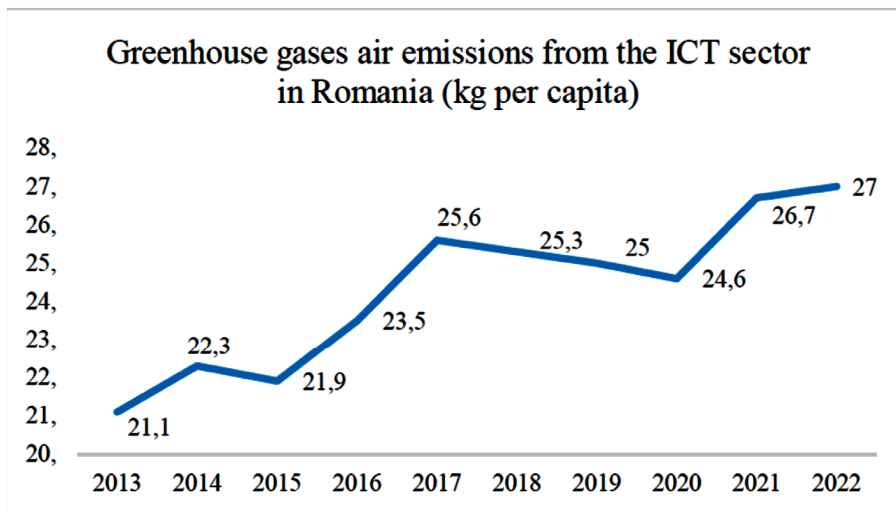


Fig. 1 Greenhouse gases air emissions

There is a slight but consistent upward trend in these emissions. Annual fluctuations are moderate, indicating a stable increase rather than sharp swings. This may signal growing use or impact of the ICT sector on the environment, posing challenges for sustainability.

In the COVID period (2020) we can observe a slight decrease — possibly reflecting reduced activity in offices or shifts to more energy-efficient remote work setups.

The ICT sector in Romania has seen steady growth in GHG emissions per capita over the past decade — likely due to: growth in digital infrastructure (data centers, mobile networks); increased internet and device usage; more energy demand from ICT services and devices.

Despite minor fluctuations, the trend is consistently upward, emphasizing the need for greener ICT practices (e.g., renewable-powered data centers, energy-efficient hardware).

4.2. Carbon dioxide

The average carbon dioxide emissions per capita in the ICT sector is 22.05 kg, which is slightly lower than the previous mean of 24.3 kg. This might suggest some improvement or differences in the dataset or time period.

Table 2 The average indicators of time series for carbon dioxide

the mean	22.050
the average of absolute change	0.522
the average of dynamic indices	1.024
the average rhythm of changing	2.428

The average yearly absolute change in emissions is 0.522 kg CO₂ equivalent per capita, a bit smaller than the previous 0.656, indicating somewhat more stable emissions over time.

The average of dynamic indices: 1.024 indicates an average growth rate of about 2.4% annually (slightly lower than before), showing that emissions are still increasing but at a slightly slower pace.

The average rhythm of changing: 2.428 – this rate shows the overall average change rhythm and confirms the steady but moderated growth in emissions from the ICT sector.

Emissions per capita from the ICT sector are still growing but at a slightly slower and more stable rate compared to the previous dataset. This could reflect progress in sustainability efforts, adoption of greener technologies, or data reflecting a different region or timeframe.

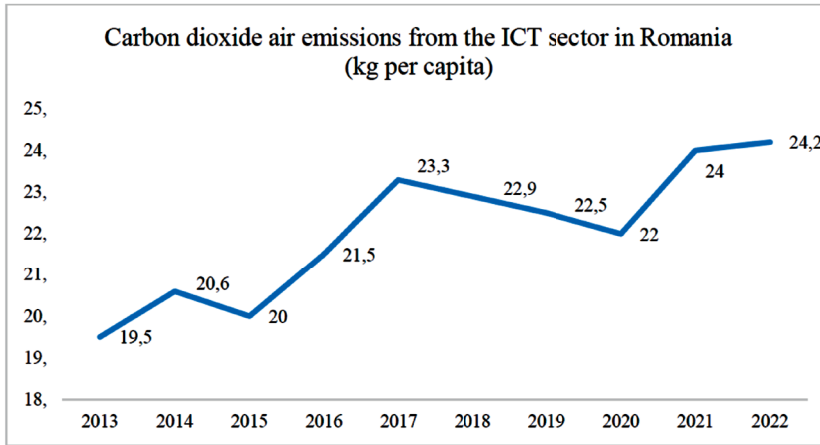


Fig. 2 Carbon dioxide air emissions

We have a noticeable growth between 2015–2017 (+3.3 kg); small plateau from 2018–2020, possibly due to energy efficiency or reduced office activity during the pandemic; second climb from 2020–2022, reaching a new high.

The CO₂ is the dominant greenhouse gas from the ICT sector. The steady increase aligns with: expanded access to internet and digital services; growth of data traffic and cloud computing; larger numbers of personal and business devices. However, Romania's CO₂ emissions per capita in ICT are still moderate by EU standards.

Continued growth without mitigation could push emissions higher — but renewable energy adoption and energy-efficient digital infrastructure could help flatten the curve.

4.3. Methane

The average value here is much lower than the previous ones (around 3.39 kg CO₂ per capita), which suggests this is likely a different indicator or a subset of emissions – maybe a specific gas or a smaller sector within ICT.

Table 3 The average indicators of time series for methane

the mean	3.390
the average of absolute change	0.144
the average of dynamic indices	1.051
the average rhythm of changing	5.104

The yearly absolute change is smaller (0.144), meaning fluctuations are quite modest.

The average of dynamic indices (1.051) indicates a growth rate of about 5.1% annually, which is a faster increase compared to previous data sets. The change rhythm confirms this faster growth trend – over 5% annual increase.

This indicator is growing faster but starts from a smaller base. It could be measuring a more specific emission type or sub-sector within ICT, showing a sharp rise but still at lower absolute emission levels. The faster growth might indicate emerging challenges or expanding activities in that part of the sector.

~25× higher than CO₂ per gram. Likely sources of CH₄ in ICT are natural gas use for powering on-site systems or backup generators and fugitive emissions in energy supply (e.g., gas infrastructure leaks). Also, CH₄ trends often mirror natural gas use and energy grid changes.

4.4. Methane (CO₂ equivalent)

The mean (94.990) – This is a much higher average value, suggesting this dataset measures a much larger quantity, likely total emissions or a broader category within the ICT sector.

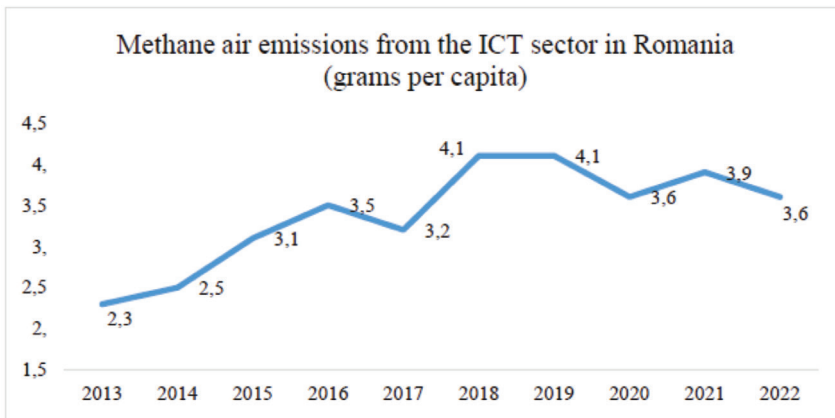


Fig. 3 Methane air emissions

Emissions rose steadily between 2013 and 2016. We have a dip in 2017, followed by a peak in 2018–2019 (4.1 g/capita). Slight decline post-2019, possibly tied to reduced on-site energy use or cleaner fuels during the pandemic years.

Methane is a minor component of total GHG emissions in ICT (in grams), but it has a warming potential

Table 4 The average indicators of time series for methane (CO₂ equivalent)

the mean	94.990
the average of absolute change	4.167
the average of dynamic indices	1.052
the average rhythm of changing	5.211

A relatively large average absolute yearly change (4.167), meaning the emissions vary significantly from year to year.

The average of dynamic indices (1.052) indicates an average growth rate of about 5.2% per year, which is consistent with a steady increase and the average rhythm of changing (5.211) confirms a dynamic growth trend of over 5% annually.

methane's warming impact vs. CO₂. Even though methane is emitted in grams, its CO₂-equivalent impact is substantial.

Romania's methane emissions from ICT (in CO₂-eq) have risen steadily – peaking in 2018–2019, dipping in 2020, and slightly decreasing since. CH₄ contributes more than 100 g CO₂-eq per person annually, making it a non-trivial

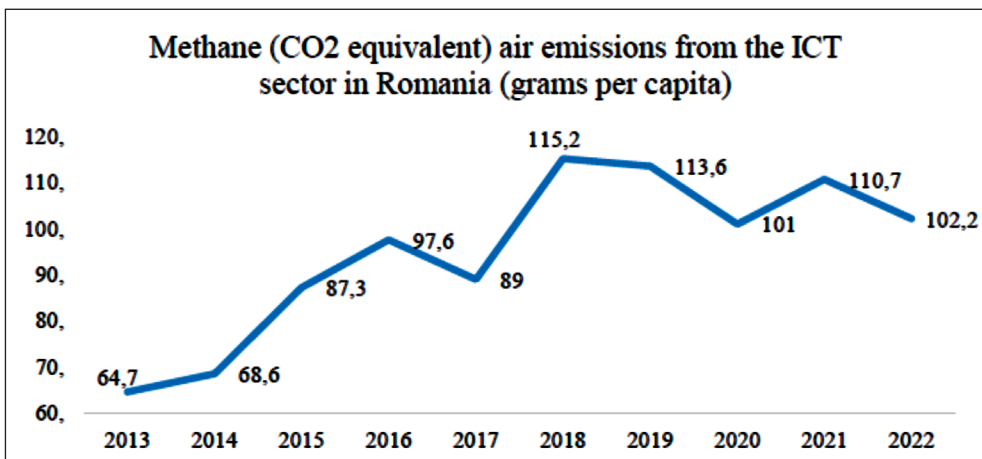


Fig. 4 Methane (CO₂ equivalent) air emissions

This dataset likely reflects a high-volume emission category or total sector emissions per capita. Emissions are growing steadily and significantly each year. The combination of high mean and growth rate points to a sector with considerable environmental impact and increasing pressures over time.

The CO₂-eq Matters because methane (CH₄) is 25× more powerful than CO₂ over 100 years. These values give a true comparison of

part of the ICT sector's climate footprint. Mitigating methane leaks and reducing fossil energy use in ICT infrastructure could meaningfully reduce this figure.

4.5. Nitrous oxide

A quite low average value (around 0.53 kg CO₂ equivalent per capita), which suggests this dataset is focused on a very specific or minor emission source within the ICT sector.

Table 5 The average indicators of time series for nitrous oxide

the mean	0.530
the average of absolute change	0.022
the average of dynamic indices	1.046
the average rhythm of changing	4.608

The average of absolute change (0.022) indicates very small absolute yearly changes, showing quite stable emissions at this scale.

but rapidly growing emission source or subcategory within ICT emissions. The absolute emissions are small, but the growth rate is notable, suggesting increasing attention might be needed here to manage future impact.

Nitrous oxide is a minor but potent greenhouse gas, with ~265× the warming potential of CO₂ per gram. Main sources in ICT likely include semiconductor manufacturing (small-scale in Romania) and electricity production (especially from fossil fuels with N₂O

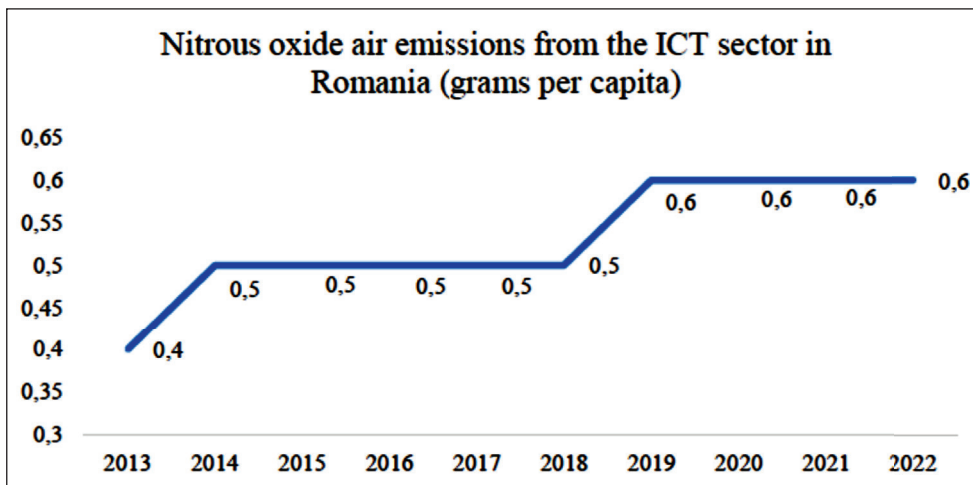


Fig. 5 Nitrous oxide air emissions

The average of dynamic indices (1.046) indicates a growth rate of roughly 4.6% per year, so even though the values are small, they are increasing relatively quickly and the average rhythm of changing (4.608%) confirms this moderate-to-high growth trend annually.

This likely represents a minor

byproducts). Romania’s consistent levels suggest steady infrastructure and energy mix with minimal growth in N₂O-intensive activities.

N₂O emissions from ICT in Romania have been stable and low, averaging around 0.5–0.6 grams per capita. Despite its small share by weight, its warming potential

makes it worth tracking. Further reductions would likely depend on cleaner electricity sources rather than changes in ICT infrastructure.

5. CONCLUSIONS AND RECOMMENDATIONS

The analysis of air emissions from the ICT sector in Romania reveals a steadily increasing environmental footprint, particularly in terms of greenhouse gas emissions. While the absolute values remain moderate by international standards, the consistent upward trends in CO₂, methane (CH₄), and nitrous oxide (N₂O) emissions indicate growing environmental pressures as digital infrastructure and service usage expand.

Despite some temporary reductions during the COVID-19 pandemic, likely due to decreased in-office activity and increased remote work, emissions have generally rebounded and continued to rise. This highlights the dual nature of digitalization: while it offers opportunities for efficiency and decarbonization, it also contributes to increasing energy demand and emissions if not properly managed.

Methane and nitrous oxide, although emitted in smaller quantities compared to CO₂, carry significantly higher global warming potential, making their growth rates especially concerning. These findings underscore the importance

of integrating environmental considerations into ICT development—particularly through the adoption of renewable energy, energy-efficient technologies, and sustainable digital practices.

Ultimately, for digital transformation to truly support climate goals, it must be aligned with environmental sustainability efforts. Romania, like other EU countries, faces the challenge of balancing digital growth with emission reduction, and the findings of this study reinforce the need for targeted policies that promote green ICT innovation while mitigating its environmental impact.

Digitalization is transforming not only people's lives but also the environment. The European Union's digital strategy seeks to ensure that this transformation benefits both individuals and businesses, while also supporting the overarching goal of achieving a climate-neutral Europe by 2050. The use of digital technologies across society and the economy can play a positive role in accelerating the shift towards a climate-neutral economy.

In Romania's ICT sector context, the emission trends documented in this study highlight the need for systematic approaches to emissions measurement, target-setting, and reduction. Romanian ICT based organizations can leverage these international standards to assess

current capability maturity, identify gaps, and develop roadmaps for achieving science-based targets. National policy frameworks can support capability development through mandatory reporting requirements, technical assistance programs, and platforms for knowledge sharing across the sector.

Based on the research conducted in this study a number of recommendations can be identified.

First, sustainable ICT practices across an organization requires a comprehensive approach that moves beyond energy efficiency and encompasses environmental, economic, and social dimensions of a given organization.

Second, alignment to international standards like GHG Protocol and Science Based Targets initiative (SBTi), is mandatory and requires the development of comprehensive measurement and reporting mechanisms.

Third, recognition of the evidence that value chain emissions represent the greatest amount of ICT carbon footprint leads to the necessity to develop capabilities focused on data collection, life-cycle approaches, supplier and customer engagement for Scope 3 emissions reduction.

Also, the digital infrastructure – including data centers and networks – should focus more on renewable and low-carbon energy sources.

A sustainability culture can be developed or sustained via well designed governance structures and accountability frameworks that support the integration of environmental targets related to ICT use into organizational objectives and performance indicators.

At the moment, in Romania there is already a clear move towards aligning organizations and practices in the ICT sector with the EU Digital Decade (European Commission, 2024; Romanian National Action Plan, 2024), as well as green economy strategies (Digital Skills and Jobs Platform, 2024). Also, the the Romanian government relies on European Union funds to support digitalization projects and capacity building (European Commission, 2025; Romania Insider, 2025; AGERPRES, 2025). That is clear evidence as to how policy and funding can act as enablers for cross-functional coordination and capability building or enhancement.

In Romania the private sector has already adopted green IT practices and demonstrated corporate sustainability commitment (EBRD, 2025; TechTalent, 2025; Startarium & Impact Hub Bucharest, 2025; GreenPoint Management, 2025). That can be further leveraged for sustaining future efforts towards employing ICT as an organizational strategic resource for sustainability purposes and cultural transformation.

The sustainment of the aforementioned efforts requires actions like:

- the ongoing integration of renewable energy into ICT infrastructure with a view to directly lowering Scope 1 and 2 emissions. That requires relying on the maturity level of technology, as well as on policy incentives. Also, resource wise, it necessitates agreements with energy providers and investments in the necessary infrastructure.
- establishing or upgrading the necessary capacity to measure greenhouse gas emissions and reporting in alignment with international standards. It requires training, data systems development and ongoing coordination across various functions which inherently translates into multi-year resource allocation and ongoing commitment requirements.

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 (CO₂) [CO2],
- Carbon dioxide from biomass (Biomass CO₂)* [CO2_BIO],

- Nitrous oxide (N₂O) [N2O],
- Methane (CH₄) [CH4],
- Perfluorocarbons (PFCs),
- Hydrofluorocarbons (HFCs),
- Sulphur hexafluoride (SF₆) including nitrogen trifluoride (NF₃),
- Nitrogen oxides (NO_x) [NOX],
- Non-methane volatile organic compounds [NMVOC],
- Carbon monoxide (CO) [CO],
- Particulate matter < 10µm [PM10],
- Particulate matter < 2,5µm [PM2_5],
- Sulphur dioxide (SO₂) expressed in SO₂ equivalent,
- Ammonia (NH₃) [NH3],
- and various air pollutants expressed in equivalents of another air pollutant:
 - CH₄ in CO₂ equivalents [CH4_CO2E]
 - N₂O in CO₂ equivalents [N2O_CO2E]
 - HFC in CO₂ equivalents [HFC_CO2E]
 - PFC in CO₂ equivalents [PFC_CO2E]
 - SF₆ and NF₃ in CO₂ equivalents [NF3_SF6_CO2E]
 - NH₃ in SO₂ equivalents [NH3_SO2E]
 - SO_x in SO₂ equivalents [SOX_SO2E]
 - NO_x in SO₂ equivalents [NOX_SO2E]
 - CO in NMVOC equivalents

- [CO_NMVOCE]
- CH₄ in NMVOC equivalents
[CH4_NMVOCE]
- NO_x in NMVOC equivalents
[NOX_NMVOCE]

REFERENCES

- [1] EBRD. (2025). Romania Country Strategy 2025-2030. https://www.ebrd.com/content/dam/ebrd_dxp/assets/pdfs/country-strategies/romania/romania-country-strategy-2025-30.pdf
- [2] TechTalent. (2025, September 9). Green Software Development in 2025 - Cutting Costs and Carbon in the Digital Era. <https://www.techtalent.ro/green-software-development-in-2025-cutting-costs-and-carbon-in-the-digital-era/>
- [3] AGERPRES. (2025, September 8). No risk for Romania to lose EU funding in 2025. Retrieved from <https://agerpres.ro/english/2025/09/09/interview-minister-of-eu-projects-no-risk-for-romania-to-lose-eu-funding-in-2025--1482795>
- [4] Balde, C. P., Kuehr, R., & Bel, G. (2024). Global e-waste monitor 2024: Electronic waste rising five times faster than data collection. United Nations University. Retrieved from https://ewastemonitor.info/wpcontent/uploads/2024/03/GEM_2024_18-03_web_page_per_page_web.pdf
- [5] Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120.
- [6] Chen, J., Liu, X., & Chen, B. (2015). Organizational capabilities and sustainability strategies. *Journal of Cleaner Production*, 105, 117–128.
- [7] Curry, D., & Donnellan, B. (2012). The role of total cost of ownership in green ICT decision making. *International Journal of Production Economics*, 140(1), 167–177.
- [8] Digital Skills and Jobs Platform. (2024, July 29). Romania country profile. Retrieved October 2025, from <https://digital-skills-jobs.europa.eu/en/european-interactive-map/romania>
- [9] Ellram, L. M. (1995). Total cost of ownership: An analysis approach for purchasing. *International Journal of Physical Distribution & Logistics Management*, 25(8), 4–23.
- [10] European Commission. (2024). Digital decade country report: Romania 2025. Retrieved June 17, 2025, from <https://digital-strategy.ec.europa.eu/en/factpages/romania-2025-digital-decade-country-report>
- [11] European Commission. (2025). Romania 2025 Digital Decade Country Report. Retrieved from <https://digital-strategy.ec.europa.eu/en/factpages/romania-2025-digital-decade-country-report>
- [12] Eurostat. Air emissions accounts - greenhouse gas emissions from the information and communication technologies sector by source and air pollutant (isoc_env_ict_aec). Retrieved October 10, 2025, from 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
- [13] Eurostat. Database – Eurostat – European Commission. Retrieved October 10, 2025, from <https://ec.europa.eu/eurostat/data/database>
- [14] Eurostat. Metadata on air emissions accounts related to ICT

- sector (isoc_env_ict_a_esmip2). Retrieved October 14, 2025, from https://ec.europa.eu/eurostat/cache/metadata/en/isoc_env_ict_a_esmsip2.htm
- [15] Eurostat. Waste generation - waste generated (env_waselee\$dv_3022). Retrieved October 10, 2025, from [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](https://ec.europa.eu/eurostat/databrowser/view/env_waselee$dv_3022/default/table?lang=en&category=isoc.isoc_ad.isoc_env_ict.isoc_env_ict_w)
- [16] Eurostat. Waste generation - waste generated (env_waseleos\$dv_3021). Retrieved October 14, 2025, from [https://ec.europa.eu/eurostat/databrowser/view/env_waseleos\\$dv_3021/default/table?lang=en&category=isoc.isoc_ad.isoc_env_ict.isoc_env_ict_w](https://ec.europa.eu/eurostat/databrowser/view/env_waseleos$dv_3021/default/table?lang=en&category=isoc.isoc_ad.isoc_env_ict.isoc_env_ict_w)
- [17] Ferrin, B., & Plank, R. E. (2002). A total cost of ownership model for supply chain cost analysis. *International Journal of Physical Distribution & Logistics Management*, 32(8), 569–585.
- [18] GHG Protocol (2004). *The GHG Protocol Corporate Accounting and Reporting Standard*. World Resources Institute and World Business Council for Sustainable Development.
- [19] GHG Protocol (2011). *Corporate Value Chain (Scope 3) Accounting and Reporting Standard*. World Resources Institute and World Business Council for Sustainable Development.
- [20] GHG Protocol (2017). *ICT Sector Guidance built on the GHG Protocol Product Life Cycle Accounting and Reporting Standard*. Available at: <https://ghgprotocol.org/sites/default/files/2023-03/GHGP-ICTSG%20-%20ALL%20Chapters.pdf>
- [21] GHG Protocol (2017). *ICT Sector Guidance built on the GHG Protocol Product Life Cycle Accounting and Reporting Standard*.
- [22] GHG Protocol Corporate Standard. (2004). *Greenhouse Gas Protocol: A Corporate Accounting and Reporting Standard (Revised Edition)*. World Resources Institute & World Business Council for Sustainable Development.
- [23] GHG Protocol. *Corporate Accounting and Reporting Standard*. 2004. <https://ghgprotocol.org/>.
- [24] GHG Protocol. *Corporate Value Chain (Scope 3) Accounting and Reporting Standard*. 2011. <https://ghgprotocol.org/>.
- [25] GHG Protocol. *ICT Sector Guidance Built on the GHG Protocol Product Life Cycle Accounting and Reporting Standard*. July 2017. <https://ghgprotocol.org/sites/default/files/2023-03/GHGP-ICTSG%20-%20ALL%20Chapters.pdf>.
- [26] Global e-Sustainability Initiative (GeSI), GSMA, International Telecommunication Union (ITU), and Science Based Targets initiative (SBTi). *Guidance for ICT Companies Setting Science Based Targets*. 2020. <https://www.gsma.com/solutions-and-impact/connectivity-for-good/external-affairs/ict-guidance-report/>.
- [27] Grand View Research. (2024, October 31). 5G edge computing market size | Industry report, 2030. <https://www.grandviewresearch.com/industry-analysis/5g-edge-computing-market-report>

- [28] GreenPoint Management. (2025, October 6). What's Next? Green Transition in Romania by 2030. <https://www.sustainability-today.ro/index.php/2025/10/06/vision-collaboration-whats-next-green-transition-in-romania-by-2030-greenpoint-management-leads-the-way/>
- [29] GSMA, GeSI, & ITU (2023). *Scope 3 Guidance for Communication Operators*, https://www.gsma.com/solutions-and-impact/connectivity-for-good/external-affairs/gsma_resources/scope-3-guidance/
- [30] GSMA, GeSI, & ITU (2024). *Guidance for ICT Companies Setting Science Based Targets*. Science Based Targets initiative, <https://www.gsma.com/solutions-and-impact/connectivity-for-good/external-affairs/climate-company-guidance/>.
- [31] Hart, S. L. (1995). A natural-resource-based view of the firm. *Academy of Management Review*, 20(4), 986–1014.
- [32] Hart, S. L., & Dowell, G. (2011). Invited editorial: A natural-resource-based view of the firm: Fifteen years after. *Journal of Management*, 37(5), 1464–1479.
- [33] International Telecommunication Union. (2024). *Measuring national ICT sector environmental impact: Arcep case study [Report]*. ITU. <http://hdl.handle.net/10986/42934>
- [34] IoT Analytics. (2024, December 4). Number of connected IoT devices growing 13% to 18.8 billion. <https://iot-analytics.com/number-connected-iot-devices/>
- [35] ISO 14064-1 (2018). *Greenhouse gases — Part 1: Specification with guidance at the organization level for quantification and reporting of greenhouse gas emissions and removals*. International Organization for Standardization.
- [36] ISO 14064-3 (2019). *Greenhouse gases — Part 3: Specification with guidance for the verification and validation of greenhouse gas statements*. International Organization for Standardization.
- [37] ISO 50001 (2018). *Energy management systems — Requirements with guidance for use*. International Organization for Standardization.
- [38] ITU & WBA (2025). *Greening Digital Companies 2025: Monitoring Emissions and Climate Commitments*. International Telecommunication Union and World Benchmarking Alliance.
- [39] ITU & World Bank (2023). *Measuring the Emissions & Energy Footprint of the ICT Sector: Implications for Climate Actions*.
- [40] ITU & World Bank. (2023). *Measuring the Emissions & Energy Footprint of the ICT Sector. Implications for Climate Actions*.
- [41] ITU & World Benchmarking Alliance. (2025). *Greening Digital Companies 2025: Monitoring emissions and climate commitments*.
- [42] ITU-T L.1410 (2014). *Methodology for environmental life cycle assessments of information and communication technology goods, networks and services*. International Telecommunication Union.
- [43] ITU-T. *Recommendation L.1410: Methodology for Environmental Life Cycle Assessments of Information and Communication Technology Goods, Networks and Services*. December 2014.

- [44] Melville, N. P. (2010). Information systems innovation for environmental sustainability. *MIS Quarterly*, 34(1), 1–21.
- [45] Molla, A., & Abareshi, A. (2012). Green IT readiness: A framework and preliminary results. *Communications of the Association for Information Systems*, 31(1), 657–676.
- [46] Nishant, R., et al. (2016). Organizational capabilities for sustainability and green innovation. *Business Strategy and the Environment*, 25(7), 489–506.
- [47] OECD. (2025). Measuring the ICT sector: Definition and scope. OECD Publishing, Paris.. retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/oecd-definitions-of-the-ict-sector-the-content-and-media-sector-and-information-industries-based-on-isic-rev-5_455bfea7/b9576889-en.pdf
- [48] Precedence Research. (2025, September 9). 5G edge computing market size and forecast 2025 to 2034. <https://www.precedenceresearch.com/5g-edge-computing-market>
- [49] Romania Insider. (2025, March 5). Romania passes EUR 100 billion mark in EU funds received in 2025. Retrieved from <https://www.romania-insider.com/romania-passes-eur-100-billion-mark-in-eu-funds-2025>
- [50] Romanian Government. (2024). National Action Plan for the Digital Decade for Romania. Adopted October 2024. [Available from Romanian government publications]
- [51] Seidel, S., et al. (2013). Green IS: Building sustainable organizations. *Information Systems Journal*, 23(6), 349–370.
- [52] Startarium & Impact Hub Bucharest. (2025, August 11). Romania’s green startup ecosystem gaining momentum. <https://www.romania-insider.com/romania-green-startup-ecosystem-report-2025>
- [53] The Green Grid (2016). *PUE: A Comprehensive Examination of the Metric*. White Paper #49.
- [54] The Shift Project & GreenIT. (2019). Lean ICT: Towards digital sobriety [PDF]. https://theshiftproject.org/app/uploads/2025/04/Lean-ICT-Report_The-Shift-Project_2019.pdf
- [55] UK Government. (2025). Greening Government Commitments ICT annual report 2023 to 2024. Department for Environment, Food and Rural Affairs (Defra). Retrieved from <https://www.gov.uk/government/publications/greening-government-ict-annual-report-2023-to-2024>
- [56] Watson, R. T., et al. (2010). Sustainable IT and the energy informatics framework. *MIS Quarterly Executive*, 9(3), 177–196.
- [57] World Bank, & International Telecommunication Union. (2025). Measuring national ICT sector environmental impact: Arcep case study. The World Bank Group. <http://hdl.handle.net/10986/42934>
- [58] World Bank. (2024). ICT sector’s contribution to global greenhouse gas emissions.

COMPARATIVE ANALYSIS OF SATELLITE BATTERY TECHNOLOGIES

Andrew H. CHUNG, Michael J. BROWN, Robert D. FASS

Clay M. KOSCHNICK

Department of Systems Engineering and Management,
Air Force Institute of Technology, Dayton Ohio, United States of America

As satellite battery technologies evolve, cost analysts must reassess whether historical subsystem data remain valid for cost estimating relationships (CERs). This study examines whether nickel-cadmium (NiCd), nickel-hydrogen (NiH₂), and lithium-ion (Li-Ion) systems can be commingled for CER development. Using data from the Unmanned Space Vehicle Cost Model (USCM), we compare normalized costs and estimate regression models with and without chemistry-specific interaction terms. The results strongly support excluding NiCd, which exhibits statistically distinct cost behavior. For NiH₂ and Li-Ion, pooled regressions and coefficient stability tests suggest commingling is appropriate when estimating NiH₂ based systems. However, interaction terms reveal significant differences in cost behavior between NiH₂ and Li-Ion suggesting that comingling may be inappropriate when estimating Li-Ion based systems. We conclude that NiCd data should be excluded and recommend continued caution when comingling NiH₂ and Li-Ion, with periodic reassessment as more Li-Ion data become available.

Key words: *satellite cost estimating, battery technologies, cost modeling, CER development, lithium-ion, nickel-hydrogen, USCM, defense acquisition, technological maturity, generalized additive models*

1. INTRODUCTION

Satellite programs remain among the most complex and costly endeavors within modern defense acquisition. As cost analysts supporting these efforts, we rely on robust historical data to inform credible and defensible cost estimates,

especially in early acquisition phases when technical specifications are often sparse. One of the most comprehensive tools available to us is the Unmanned Space Vehicle Cost Model (USCM), maintained by Space Systems Command (SSC). This model aggregates decades of satellite

program cost data—normalized to constant-year dollars and mapped to a standardized Work Breakdown Structure (WBS)—to support the development of cost estimating relationships (CERs) across system and subsystem levels.

In recent years, SSC has observed a discontinuity in the cost behavior of satellite batteries within the USCM dataset. Specifically, data associated with satellite programs from the 1960s through the early 1980s—predominantly reliant on nickel-cadmium (NiCd) batteries—exhibits markedly different cost characteristics than data associated with programs post-1980, which increasingly incorporate nickel-hydrogen (NiH₂) and lithium-ion (Li-Ion) technologies (Kwok, 2023). This divergence in cost behavior prompted the decision to exclude legacy NiCd battery data from electrical power subsystem (EPS) CER development. However, no formal statistical justification for this exclusion has been documented in the literature. Nor has the comparability of NiH₂ and Li-Ion battery costs been rigorously tested.

The objective of this study is to conduct a comprehensive, statistically grounded evaluation of battery cost trends across three major chemistries—NiCd, NiH₂, and Li-Ion—as documented in the USCM database. Our goal is to

provide empirical justification for key data selection decisions in CER construction and to explore whether cost behavior across newer battery technologies warrants separate treatment in modeling. We also aim to assess the broader time trends in satellite battery costs to determine whether technological maturity effects or technology cycles influence CER reliability.

Our study is motivated by both practical and methodological imperatives. From a practical standpoint, battery systems often account for 20–30% of a satellite's total bus weight (Hill, 2011). They are tightly linked to mission duration, payload power demands, and orbital constraints—all of which drive lifecycle cost. As battery technology evolves, so too do these performance characteristics and their corresponding cost implications. Decisions regarding which historical data to include in CERs are methodologically nontrivial. Inappropriate inclusion of legacy technologies can distort parameter estimates, inflate uncertainty, and lead to flawed acquisition recommendations.

We organize our investigation around three research questions:

1. How do the normalized costs of NiCd, NiH₂, and Li-Ion batteries compare and what implications does this have

on data inclusion for CER development?

2. In what ways do the cost behaviors of NiH₂ and Li-Ion battery systems differ after controlling for technical characteristics, and to what extent can these chemistries be jointly modeled in a unified CER framework?
3. How do modern satellite battery costs evolve over time within and across battery types and what role should technological maturation play in CER development?

To address these questions, we analyze WBS Level 4 battery subsystem data from the USCM model, drawing on first unit cost records from 72 satellite programs spanning the 1970s to 2012. We normalize costs by battery weight (T1\$/lbs.) and BOL power (T1\$/BOL), apply statistical comparison tests, and model cost behavior over time using linear regression. We find that battery chemistry significantly influences EPS cost behavior and argue that key assumptions in CER development—particularly those regarding technological maturation effects and the treatment of NiH₂ and Li-Ion data—deserve reconsideration. Our findings carry practical implications for defense acquisition cost modeling.

2. LITERATURE REVIEW

2.1. Space Systems and Subsystems

A space system typically consists of four integrated components: the space vehicle, launch vehicle, ground segment, and orbital transfer system (Department of Defense, 2022). In this study, we focus on the space vehicle which is composed of two primary sections: the Payload and Bus.

The Payload includes mission-specific equipment, such as communications hardware or remote sensing instruments, depending on the satellite's operational role (Ippolito Jr., 2017). The Bus contains the support subsystems that enable the Payload to function, including structure, thermal control, attitude control, propulsion, command and data handling, and electrical power (Department of Defense, 2022). A summary of the bus components and their respective functions is detailed in Table 1.

Of particular interest here is the Electrical Power Subsystem (EPS), which encompasses power generation, conditioning, and storage. Rechargeable batteries are a critical part of this subsystem, providing energy during periods when solar input is unavailable or insufficient. Prior research identifies batteries as a key cost driver within the EPS, contributing substantially to total bus mass and cost (Candella, et al., 2024; Hill, 2011).

Table 1 Bus Subsystems and Their Function. Adapted from Candella et al. (2024) *Journal of Defense Resources Management*

Subsystem	Function
<i>Attitude Control (ACS)</i>	Counteracts gravitational pulls and keeps the antennas pointed in the desired direction
<i>Electrical Power (EPS)</i>	Convert, regulate, store, distribute, and switch the electrical energy to the Bus and Payload elements
<i>Propulsion</i>	Provides the thrust required to make corrections or reposition the satellite
<i>Structures & Mechanisms (SMS)</i>	Structural support, deployment, and locking functions
<i>Telemetry, Tracking, & Command (TT&C)</i>	Control functions to keep the satellite operating safely in orbit. Communicates with an Earth terminal facility to maintain orbit.
<i>Thermal Control (TC)</i>	Controls the different temperature environments and keeps it stable

2.2. Cost Estimating Relationships and Subsystem-Level Modeling

Satellite cost modeling has historically emphasized high-level metrics such as launch mass or payload weight. Hadfield (1974) and Koelle (1984) developed some of the earliest cost estimating relationships (CERs), focused primarily on recurring versus nonrecurring cost behaviors. These models were useful for broad system-level estimation but failed to account for the unique cost characteristics of specific subsystems.

As smaller and more modular spacecraft became common in the 1990s and early 2000s, researchers recognized the limitations of mass-based models. Bearden (2001) and Mahr and Richardson (2003) highlighted how newer platforms leveraged commercial-off-the-shelf (COTS) technologies, reducing both acquisition timelines and costs. This shift prompted the development of subsystem-level CERs, especially within the Small Satellite Cost Model (SSCM), which estimates bus costs using subsystem performance

attributes such as pointing accuracy and power (Fox, et al., 2008).

Drenthe, Zandbergen, Curran, and Van Pelt (2019) extended this trend by creating subsystem CERs for commercial satellites in early design stages, using hybrid models based on both historical costs and first unit data, also called T1 data. Still, guidance on data inclusion—particularly for legacy subsystems like NiCd batteries—remains sparse. Inappropriate data selection can undermine CER accuracy and lead to flawed acquisition decisions.

2.3. Chemistry Transitions and Costs

Battery technologies used in satellites have evolved considerably. The earliest missions employed silver-zinc (AgZn) batteries, followed by nickel-cadmium (NiCd) in the 1960s and 70s. Halpert, Frank, and Surampudi (1999) traced the progression of NiCd cell formats from cylindrical to prismatic, noting improvements in energy density and packaging efficiency. However, NiCd cells are sensitive to overcharging, display memory effects, and degrade under high temperature—factors that increased life-cycle costs and complexity.

In response, satellite designers adopted nickel-hydrogen (NiH₂) batteries in the late 1970s (Halpert, et al., 1999). NiH₂ batteries featured sealed pressure vessels and offered

higher cycle life and energy density, albeit at greater weight and structural complexity. Hill (2011) noted that while NiH₂ was an improvement over NiCd, its weight and volume remained limiting factors.

Lithium-ion (Li-Ion) batteries entered satellite use in the 2000s, offering further gains in energy density, weight reduction, and design flexibility. Although they require careful charge management and thermal protection, their adoption has been rapid due to size and mass advantages (Altemose, et al., 2011). These differences in physical and chemical characteristics directly influence the cost profiles of each battery type.

Yet no prior study has statistically tested whether these chemistries differ significantly in unit cost behavior—nor whether historical NiCd data remains suitable for use in modern CERs. We investigate this question to inform more defensible cost estimating practices.

2.4. Trends and Maturity-Cost Relationship

A foundational assumption in many cost estimating relationships is that unit cost declines as a technology matures. This idea, formalized in learning curve theory and embedded in models like the NASA Air Force Cost Model (NAFCOM), suggests that production efficiencies, design refinement, and accumulated

expertise lead to lower costs over time (Winn & Hamcher, 2002). Technological maturation is often operationalized as the number of years since a technology's first fielding and is treated as a monotonic driver of cost reduction.

However, we question whether this relationship holds for space-qualified batteries. Our initial visual analysis of USCM data suggests that while cost per unit tends to decrease shortly after a battery chemistry is introduced, this decline may plateau or even reverse. These patterns raise important questions about whether the conventional maturity-cost relationship holds for long-lived, mission-critical components like spacecraft batteries.

Despite the centrality of this assumption in CER construction, we find little prior literature that evaluates it empirically in the context of satellite subsystems. The potential for nonlinear or non-monotonic cost behavior as technologies age—whether due to obsolescence, diminishing economies of scale, or shifts in supplier dynamics—has not been sufficiently examined. We therefore include this question in our investigation.

In summary, prior research has advanced our understanding of satellite CER development, particularly at the system level using gross metrics like payload weight or total mass. However, the cost

behavior of specific subsystems—such as the Electrical Power Subsystem—has received limited attention, despite its critical role in platform design and lifecycle cost. Furthermore, while the evolution of battery chemistries is well documented in the technical literature, few studies have examined whether these transitions carry statistically distinct cost implications. Finally, the widely held assumption that cost declines with maturity remains largely untested for space-qualified batteries. This paper addresses these gaps by evaluating cost trends across battery chemistries and maturity levels within the USCM dataset, with the goal of informing more defensible data selection practices in subsystem-level CER development.

3. METHODOLOGY

Our methodology is designed to test whether satellite battery chemistries differ meaningfully in cost behavior and to evaluate how cost trends evolve over time. To do this, we extract battery subsystem data from the Unmanned Space Vehicle Cost Model (USCM), conduct comparative analysis across three major chemistries (NiCd, NiH₂, and Li-Ion), and assess temporal cost patterns using normalized metrics. Because this research is exploratory in nature and intended to inform cost estimating relationship (CER) development rather than establish

definitive performance differences, we adopt a significance threshold of $\alpha = 0.10$ throughout our analysis.

3.1. Data Source and Cleaning

We begin with the latest release of the Unmanned Space Vehicle Cost Model (USCM), focusing specifically on WBS Level 4 element “Rechargeable Batteries.” This element captures subsystem-level costs for battery systems across a wide range of satellite programs dating from the early 1970s through the 2010s. The raw dataset includes 73 satellite entries with battery subsystem records.

To ensure consistency and accuracy in our analysis, we apply the following data methods and exclusions:

- *Dual Chemistry Systems:* One program includes both NiH₂ and Li-Ion cells in a hybrid configuration. Since this violates the assumption

of mutually exclusive chemistries, we exclude it from all comparative analyses.

- *Interpolation for BOL Values:* Eight programs are missing BOL power values but include complete T1\$ and weight data. For these programs, we interpolate BOL using regression-based estimation from similar programs of matching chemistry and mass.

After exclusion and interpolation, we retain 72 of the 73 programs: 26 using nickel-cadmium (NiCd), 38 using nickel-hydrogen (NiH₂), and 8 using lithium-ion (Li-Ion) batteries. For research questions 1 and 3, we analyze the full data set. Since research question 2 investigates NiH₂ and Li-Ion only, we exclude the 26 NiCd data points and analyze the remaining 46. Table 2 summarizes our data by chemistry, date range, and research questions.

Table 2 Data Exclusion and Sample Sizes by Battery Chemistry

Battery Type	Earliest Date	Latest Date	Observations	Research Questions
NiCd	4/1/1971	2/1/1996	26	1, 3
NiH ₂	10/1/1997	1/1/2012	38	1, 2, 3
Li-Ion	3/1/2002	6/21/2012	8	1, 2, 3
Research Question Observations				
<i>Research Question 1</i>				72
<i>Research Question 2</i>				46
<i>Research Question 3</i>				72

3.2. Variables

Our analysis considers three categories of variables: cost metrics, classification indicators (primarily chemistry), and continuous program-level descriptors such as weight, power, and maturity. We divide our approach into two phases of analysis, each using different subsets of these variables.

In the first phase, we focus on normalized cost metrics to evaluate whether battery chemistries differ significantly in cost behavior. Specifically, we calculate two dependent variables: T1\$/lbs., which normalizes first-unit cost by battery subsystem weight in pounds, and T1\$/BOL, which normalizes cost by beginning-of-life (BOL) power in watts. Prior studies and standard cost modeling practice emphasize weight as the dominant cost driver in satellite subsystems, so normalization by weight facilitates a like-for-like cost comparison across systems of varying size. Normalizing by power, meanwhile, offers a complementary perspective—one that emphasizes operational output instead of physical mass. These two metrics serve as the basis for our nonparametric comparisons and summary trend statistics.

In the second phase, we model the raw first-unit cost (T1\$) using a combination of technical and temporal predictors. These regressions allow us to assess whether Li-Ion and

NiH₂ follow similar cost behavior after controlling for confounding programmatic and physical factors. Unlike the normalized metrics, raw T1\$ retains scale sensitivity and reflects the actual dollar cost observed in historical data.

Independent variables used in our regression models include battery subsystem weight (in pounds), BOL power (in watts), and a maturity variable representing the number of years since the first documented use of each chemistry. Following published aerospace battery histories, we define NiCd maturity as years since 1962 (Halpert, et al., 1999), NiH₂ since 1966 (Halpert, et al., 1999), and Li-Ion since 2001 (Smart, et al., 2004). These dates do not reflect the individual programs in our dataset but rather represent fixed technological baselines intended to proxy overall system maturity at the time of use. They are applied uniformly across each chemistry.

We also include design life (in years) as a continuous variable in our regression models. This variable reflects the programmatic design duration for which the satellite is intended to operate. We consider this an important driver of cost, as longer design lives often require more robust energy storage solutions, higher depth-of-discharge tolerances, and added redundancy. Finally, we interact chemistry with weight and maturity to test whether Li-Ion

deviates from NiH₂ in statistically meaningful ways when controlling for these variables.

Table 3 defines each of the variables used in our statistical analysis, including their units and expected relationships with cost.

after accounting for technical and programmatic characteristics.

3.3.1. RQ 1 - Cost differences among chemistries.

To evaluate whether normalized cost behavior differs across battery

Table 3 List of Variables and Definitions

Variable	Definition
Battery Type	The type of battery used in the satellite (NiCd, NiH ₂ , Li-Ion)
BOL	Beginning of Life power - power at start of mission, in watts
Contract Award Date	Date contract awarded and authority to proceed granted
Design	Design life of the battery, measured in months
Lithium	Dummy variable indicating satellite program with Li-Ion battery
MaturityHist	Battery type maturity measured in years from first use in satellites
MaturityUSCM	Maturity of the battery, measured in years from first documented use in the USCM database
T1	Satellite first unit costs in thousands of dollars
T1\$/lbs.	T1 costs in thousands of dollars per pound for the battery (CP16\$)
T1\$/BOL	T1 costs in thousands of dollars per BOL (CP16\$)
Weight	The weight of battery used in the satellite, measured in pounds

3.3. Statistical Methods

Our statistical approach consists of two primary components: comparison analysis of normalized cost metrics and regression modeling of raw first-unit cost (T1\$). These methods allow us to evaluate whether battery chemistries differ significantly in cost behavior and whether lithium-ion (Li-Ion) and nickel-hydrogen (NiH₂) systems exhibit distinguishable cost patterns

chemistries, we begin with a one-way analysis of variance (ANOVA) on both T1\$/lbs. and T1\$/BOL. This serves as our primary method for detecting overall group-level differences in cost. Because Levene’s test identifies unequal variances among the three chemistry groups, we use Welch’s t-tests for pairwise post-hoc comparisons. These are appropriate under conditions of heteroskedasticity and provide

greater robustness than standard t-tests.

To assess the robustness of the ANOVA under potential violations of normality, we conduct both Kolmogorov–Smirnov and Anderson–Darling tests for each chemistry group. While the Kolmogorov–Smirnov test supports normality in all three groups, the Anderson–Darling test indicates that only NiCd satisfies the normality assumption for T1\$/BOL, and none of the groups satisfy it for T1\$/lbs. Based on this mixed evidence, we supplement the ANOVA with Kruskal–Wallis tests as nonparametric robustness checks.

For post-hoc comparison of individual groups under nonparametric assumptions, we apply Wilcoxon rank-sum tests to all pairwise combinations of chemistries. These tests function as distributional analogues to the Welch t-tests. To control for family-wise error across multiple comparisons, we apply a Bonferroni correction. All comparison tests are evaluated at a significance threshold of $\alpha = 0.10$, consistent with the exploratory nature of this study.

By using both parametric and nonparametric methods—along with corresponding post-hoc procedures—we ensure that our conclusions about cross-chemistry cost differences are robust to distributional assumptions and sample size imbalances.

3.3.2. RQ 2 - Nesting of NiH₂ and Li-Ion Data.

Next, we model raw T1\$ using ordinary least squares (OLS) regression with robust standard errors. Explanatory variables include subsystem weight, BOL power, design life, and maturity, all defined in Section 3.2. We first estimate separate models for NiH₂ and Li-Ion entries to evaluate cost behavior within each chemistry.

We then pool the NiH₂ and Li-Ion observations and estimate a nested model in which interaction terms between Li-Ion and each independent variable are included. This allows us to formally test whether the cost behavior of Li-Ion systems deviates from that of NiH₂ systems after controlling for observable characteristics. Following Clogg, Petkova, and Haritou (1995), we use a difference-in-coefficients Z-test to evaluate whether each pooled coefficient significantly differs once the interaction term is introduced. This approach serves as a scalar analogue to a Wald test for coefficient equality and provides an intuitive measure of whether the Li-Ion and NiH₂ regressions are statistically distinguishable allowing us to determine whether combining Li-Ion and NiH₂ data for CER development is appropriate.

3.3.3. RQ 3 - Maturity effects within and across chemistries.

Finally, we interpret the maturity variable coefficients from the NiH₂ and Li-Ion regressions to assess whether cost behavior changes over time. While we make no assumption of a monotonic trend, the maturity variable provides a controlled test of whether technological age corresponds to reductions in subsystem cost when accounting for weight, power, and design life. NiCd is excluded from this portion of the analysis, as it has been largely phased out and is no longer considered relevant for modern CER development despite its continued presence in a small number of legacy systems.

4. RESULTS

4.1. Comparison of Cost Across Chemistries

A one-way ANOVA detects a statistically significant difference in T1\$/BOL ($p = 0.0003$) and a marginal difference in T1\$/lbs. ($p = 0.0962$). Levene's tests confirm unequal variances for both metrics, motivating the use of Welch's t-tests for pairwise post-hoc comparisons. Welch's tests show that NiCd differs significantly from both NiH₂ ($p = 0.0011$) and Li-Ion ($p = 0.0029$) on T1\$/BOL, and from NiH₂ on T1\$/lbs. ($p = 0.0502$), all well below the $\alpha = 0.1$ threshold. However, NiCd and

Li-Ion do not differ significantly on T1\$/lbs. ($p = 0.1413$), and Li-Ion and NiH₂ are not significantly different on either metric.

Because we could not definitively establish normality, as discussed in Section 3.3, we run the Kruskal–Wallis test as a nonparametric robustness check. The results support a strong difference in T1\$/BOL ($p = 0.0004$), while the result for T1\$/lbs. is more conservative ($p = 0.128$). Although this exceeds our alpha threshold, the divergence is modest. Taken together with the ANOVA and Welch results, we find sufficient justification to proceed with post-hoc comparisons of both T1\$/lbs. and T1\$/BOL.

We apply Wilcoxon rank-sum tests as a nonparametric analogue to the Welch tests. These results mirror the Welch tests: NiCd is significantly different from both NiH₂ and Li-Ion on T1\$/BOL ($p = 0.0003$ and $p = 0.0059$, respectively), and from NiH₂ on T1\$/lbs. ($p = 0.034$), but not from Li-Ion on T1\$/lbs. ($p = 0.619$). Even after applying a Bonferroni correction for family-wise error, the results remain consistent. As with the Welch results, Li-Ion and NiH₂ remain statistically indistinguishable on both metrics.

While T1\$/lbs. comparisons do not consistently show divergence between NiCd and Li-Ion, the strong and consistent results from T1\$/BOL support the conclusion that

NiCd behaves differently in terms of normalized cost. Meanwhile, the lack of divergence between NiH₂ and Li-Ion in both metrics suggests that these two chemistries may exhibit similar cost behavior, justifying further investigation. This result establishes the foundation for research question two. Tables 4 and 5 summarize the results.

ordinary least squares (OLS) with heteroskedasticity-robust standard errors. While the comparative analysis in Section 4.1 did not reveal statistically significant differences between these two chemistries, that result alone does not confirm that they may be reliably combined for CER development. A more detailed analysis is required to determine

Table 4 Comparative T1\$/BOL Results

Test	Method	p-value ($\alpha = 0.10$)
ANOVA	Means Test	0.0003
Kruskal-Wallace	Rank-Based Test	0.0004
Battery Pair	Welch's ($\alpha = 0.10$)	Wilcoxon ($\alpha = 0.10/0.033^1$)
Li-Ion & NiH ₂	0.516	0.270
NiCd & NiH ₂	0.0011	0.0003
NiCd & Li-Ion	0.0029	0.0059

¹Bonferroni correction controls Type I error by dividing α by the number of comparisons

Table 5 Comparative T1\$/lbs. Results

Test	Method	p-value ($\alpha = 0.10$)
ANOVA	Means Test	0.0962
Kruskal-Wallace	Rank-Based Test	0.128
Battery Pair	Welch's ($\alpha = 0.10$)	Wilcoxon ($\alpha = 0.10/0.033^1$)
Li-Ion & NiH ₂	0.382	0.787
NiCd & NiH ₂	0.0502	0.034
NiCd & Li-Ion	0.829	0.619

¹Bonferroni correction controls Type I error by dividing α by the number of comparisons

4.2. Regression of NiH₂ and Li-Ion Costs

To evaluate whether Li-Ion and NiH₂ exhibit similar cost behavior when controlling for observable characteristics, we estimate two regression models using

whether their cost drivers behave similarly when modeled explicitly.

We begin by pooling the NiH₂ and Li-Ion data and regressing the raw T1 costs (*T1\$*) on the subcomponent characteristics of weight (*weight_i*), Design Life (*Design_i*), and

technological maturity from first documented use at the time of contract award (*MaturityHist*). We repeat the regression while adding interaction terms with Li-Ion to isolate the Li-Ion data in the regression. This specification allows cost behavior to differ across chemistries and serves as the basis for applying the method developed by Clogg, Petkova, and Haritou (1995) which tests whether the inclusion of interaction terms leads to a statistically significant change in the regression coefficients. This provides a formal mechanism for determining whether Li-Ion systems behave differently from NiH₂ after accounting for observable drivers of cost, allowing us to determine whether or not Li-Ion and NiH₂ data can be comingled in CER development. The two estimated regression equations are:

Pooled Model (No Interaction):

$$T1_i = \beta_0 + \beta_1 \text{Weight}_i + \beta_2 \text{Design}_i + \beta_3 \text{MaturityHist}_i + \varepsilon_i$$

Nested Model with Interactions:

$$\begin{aligned} T1_i = & \beta_0 + \beta_1 \text{Weight}_i + \beta_2 \text{Design}_i + \beta_3 \text{MaturityHist}_i \\ & + \beta_4 (\text{Li-Ion}_i \cdot \text{Weight}_i) + \beta_5 (\text{Li-Ion}_i \cdot \text{Design}_i) \\ & + \beta_6 (\text{Li-Ion}_i \cdot \text{MaturityHist}_i) + \varepsilon_i \end{aligned}$$

Two NiH₂ entries were removed from the regression sample prior to estimation. These points were flagged as outliers with undue influence based on standard diagnostic tests. Upon further investigation, both corresponded to satellite systems with atypical design lives, one particularly long, the other short. This

suggests that the electrical power subsystems (EPS) in these missions were fundamentally different and not representative of typical spacecraft, making their inclusion in the regression inappropriate.

Table 6 presents the results of the pooled and nested regressions. The pooled model assumes shared cost behavior across NiH₂ and Li-Ion systems and yields an R² of 0.59. The nested model, which includes Li-Ion-specific interaction terms, increases the explanatory power yielding an R² of 0.64. More importantly, the nested model allows for direct estimation of whether Li-Ion cost behavior differs meaningfully from NiH₂.

To formally test whether the introduction of interaction terms materially alters the regression coefficients of our main variables of interest when estimating NiH₂

based systems, we apply the method developed by Clogg, Petkova, and Haritou (1995). This approach evaluates whether the coefficients from the pooled model (β_1 through β_3) are statistically distinguishable from those in the nested model when the Li-Ion interaction terms are included. By design, β_1 - β_3 in the nested model

correspond to NiH₂ specifically since Li-Ion is fully captured in the interactions. The results of this test are presented in Table 7. None of the Z-statistics approach significance, suggesting that the slope coefficients remain stable even after allowing Li-Ion to diverge.

While the Clogg test implies that commingling the Li-Ion and NiH₂ data does not result in statistically significant distortions to the pooled model's slope estimates, indicating that pooling is appropriate when estimating NiH₂ based systems, the interaction terms in the nested regression suggest more caution. All three interactions—Li-Ion × Weight, Li-Ion × Design, and Li-Ion × MaturityHist—are large in magnitude and individually

significant at the 90% confidence level. The interaction of Li-Ion on weight is even more pronounced with significance at the 95% confidence level. These coefficients suggest that Li-Ion subsystems follow materially different cost dynamics, particularly with respect to how maturity and size translate into cost. Thus, when estimating Li-Ion based systems, the evidence suggests that NiH₂ based data should not be mingled with Li-Ion for accurate CER development.

The apparent contradiction between the coefficient equivalency test and the nested regression results likely stems from the small sample size of Li-Ion systems (n = 8), which reduces the statistical power of the pooled coefficient comparison.

Table 5 Pooled and Nested Regression Results

	(1) Pooled	(2) Nested
Weight	6.56*** (1.25)	6.75*** (1.39)
Design	-11.50** (5.14)	-11.69 (8.01)
MaturityHist	61.61*** (18.10)	76.48 (54.61)
Li-Ion × Weight	-	-4.43** (1.52)
Li-Ion × Design	-	14.15* (8.47)
Li-Ion × MaturityHist	-	-113.55* (57.57)
<i>R</i> ²	0.59	0.64
Observations	44	44

* p < 0.10, ** p < 0.05, *** p < 0.01 (two-tailed)

Table 7 Equality of Coefficients

Variable	β Pooled	β Nested	SE β Pooled	SE β Nested	Z-Score	p-value
Weight	6.56	6.75	1.25	1.39	-0.10	0.92
Design	-11.50	-11.69	5.14	8.01	0.02	0.98
MaturityHist	61.61	76.48	18.10	54.61	-0.26	0.80

4.3. Comparison of Maturity across Chemistries

Our final research question examines how technological maturity—defined as the number of years since first documented use at the time of contract award (MaturityHist)—relates to cost across battery chemistries. In the pooled model, the MaturityHist coefficient is positive and statistically significant at the 99% confidence level, indicating that first-unit costs increase as battery technologies age. This result is unexpected, as technological maturity is typically associated with learning, standardization, and cost reduction over time.

When interaction terms are introduced in the nested regression, the picture becomes more nuanced. The MaturityHist coefficient for NiH₂ rises slightly higher than the pooled model but loses statistical significance, while the interaction term for Li-Ion \times MaturityHist is large, negative, and significant at the 90% confidence level. This suggests that the positive maturity effect

observed in the pooled model is not generalizable across chemistries. Instead, it is likely driven by NiH₂ systems, which dominate the sample and exhibit more complex lifecycle dynamics. Indeed, the NiH₂-only regression produces a positive but statistically insignificant maturity trend, while the Li-Ion-only regression reveals a negative and statistically significant slope at the 90% confidence level.

5. CONCLUSION AND RECOMMENDATIONS

This study provides statistical validation for a set of data selection practices that are increasingly relevant in modern satellite cost estimating. Our analysis confirms that legacy nickel-cadmium (NiCd) battery data should be excluded from modern CER development. NiCd subsystems exhibit statistically distinct cost behavior across both normalized cost metrics—T1\$/lbs. and T1\$/BOL—and diverge consistently from both NiH₂ and Li-Ion systems. This finding reinforces recent decisions by Space

Systems Command and supports their permanent removal from future EPS cost modeling efforts.

The comparison between NiH₂ and Li-Ion systems yields more nuanced results. While comparative analysis of normalized metrics revealed no statistically significant differences, our regression results suggest that Li-Ion subsystems may follow a distinct cost trajectory. The pooled regression treats NiH₂ and Li-Ion as a single population and estimates a positive and statistically significant cost increase with maturity. This is counterintuitive and inconsistent with established expectations about technological learning and cost reduction over time.

However, when the regression is disaggregated via chemistry-specific interaction terms, the maturity trend disappears for NiH₂ and reverses direction for Li-Ion. The Li-Ion interaction term is large, negative, and significant at the 90% confidence level—precisely the relationship we would expect from a newer, rapidly maturing technology. In contrast, the NiH₂-only regression shows a weak, statistically insignificant positive trend, suggesting that within-chemistry variation in NiH₂ systems may reflect evolving configurations and complexity that offset any learning-curve effects. This divergence in cost behavior further supports the argument that

NiH₂ and Li-Ion systems should not be treated as interchangeable in CER development.

Still, caution is warranted. The formal test for coefficient stability developed by Clogg et al. (1995) finds no statistically significant difference between the pooled and nested models when estimating NiH₂ based systems. While this may appear to contradict the regression findings, it is almost certainly an artifact of limited statistical power, as the Li-Ion sample includes only eight observations. Indeed, all three interaction terms in the nested model—Li-Ion × Weight, Li-Ion × Design, and Li-Ion × MaturityHist—are both large in magnitude and statistically significant, indicating that Li-Ion cost drivers differ in meaningful ways from NiH₂ systems. We therefore interpret the null result of the coefficient equivalency test not as evidence of true equivalence *per se*, but as a reflection of the current data limitations.

Taken together, these results indicate that while the current practice of commingling Li-Ion and NiH₂ data in CER development is not invalidated by statistical evidence, the underlying behavior of Li-Ion systems may differ in ways that merit future separation—especially as more data become available. The pooled maturity result, in particular, appears to be an averaging artifact that masks opposing trends across

the two chemistries. As more Li-Ion programs are added to the USCM database, it will be critical to revisit this assumption and re-evaluate whether continued commingling is justified.

We conclude with two primary recommendations:

1. *Exclude NiCd systems entirely from future CER development.*

Their cost behavior is statistically and operationally distinct and no longer representative of current satellite platforms.

2. *Exercise caution when pooling NiH₂ and Li-Ion data.*

While current evidence does not prohibit their combination, it also does not affirm their equivalence. The burden of proof should fall on continued statistical validation, especially as the Li-Ion dataset grows. Cost analysts and model developers should remain attentive to interaction effects and test for chemistry-specific cost behavior regularly. The evidence suggests that NiH₂ and Li-Ion may not follow the same cost dynamics, and that mingling them may obscure the unique cost profiles of emerging technologies like Li-Ion.

These findings reaffirm the need for data discipline and ongoing validation in subsystem-level CER development. Our analysis provides clear support for excluding NiCd

systems and offers early, though inconclusive, evidence that Li-Ion and NiH₂ may follow distinct cost trajectories. With only eight Li-Ion observations, we stop short of recommending disaggregation, but we emphasize the need for continued monitoring as additional data become available. CER developers should revisit these assumptions regularly and remain open to chemistry-specific modeling if warranted by future trends. Doing so will improve the fidelity of subsystem cost estimates and better align them with the technologies now shaping the future of satellite power systems.

Disclaimer: The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

REFERENCES

- [1] Altemose, G., Hellermann, P. & Mazz, T., 2011. *Active Cell Balancing System Using an Isolated Share Bus for Li-Ion Battery Management: Focusing on Satellite Applications*. Farmindale, NY, IEEE.
- [2] Bearden, D. A., 2001. Small-Satellite Costs. *Crosslink*, pp. 33-44.
- [3] Candella, R. A. et al., 2024. Informing Data Selection for Satellite Subsystems Cost

- Estimating Relationships. *Journal of Defense Resources Management*, 15(2(29)), pp. 92-109.
- [4] Clogg, C. C., Petkova, E. & Haritou, A., 1995. Statistical Methods for Comparing Regression Coefficients Between Models. *American Journal of Sociology*, 100(5), pp. 1261-1293.
- [5] Department of Defense, 2022. *Work Breakdown Structures for Defense Materiel Items. Mil-Std-881F*. Washington D.C.: United States.
- [6] Drenthe, N. T., Zandbergen, B. T., Curran, R. & Pelt, M. O. V., 2019. Cost Estimating of Commercial Smallsat Launch Vehicles. *Acta Astronautica*, Volume 155, pp. 160-169.
- [7] Fox, B., Brancato, K. & Alkire, B., 2008. *Guidelines and Metrics for Assessing Space System Cost Estimates*, Santa Monica, CA: RAND Corporation.
- [8] Hadfield, B. M., 1974. Satellite-Systems Cost Estimation. *IEEE Transactions on Communications*, p. 1540-1547.
- [9] Halpert, G., Frank, H. A. & Surampudi, S., 1999. Batteries and Fuel Cells in Space. *Interface - The Electrochemical Society*, 8(3), p. 25-30.
- [10] Hill, C. A., 2011. Satellite Battery Technology — A Tutorial and Ov. *IEEE Aerospace and Electronic Systems Magazine*, 26(6), p. 38-43.
- [11] Ippolito Jr., L. J. J., 2017. Satellite Subsystems. In: *Satellite Communications Systems Engineering: Atmospheric Effects, Satellite Link Design and System Performance*. West Sussex, UK: John Wiley & Sons Ltd, pp. 35-48.
- [12] Koelle, D. E., 1984. CostReduction Trends in SpaceCommunications by LargerSatellites/Platforms. *Acta Astronautica*, 11(12), pp. 785-794.
- [13] Kwok, B., 2023. *Space System Command Financial Management Cost Research Task Lead/Tecolote Chief Scientist [Interview]* (5 April 2023).
- [14] Mahr, E. & Richardson, G., 2003. *Development of the small satellite cost model (SSCM) Edition 2002*. Big Sky, MT, IEEE, pp. 8_3831 - 8_3841.
- [15] Smart, M. C. et al., 2004. Lithium-Ion Batteries for Aerospace. *IEEE Aerospace and Electronic Systems Magazine*, 19(1), pp. 18-25.
- [16] Winn, S. D. & Hamcher, J. W., 2002. *NASA/Air Force Cost Model*, Versailles: Science Applications International Corp. United States.

THE EVOLUTION OF SOCIAL MEDIA PLATFORMS AS INSTRUMENTS OF PROPAGANDA, DISINFORMATION AND MEDIA SUBVERSION IN MODERN CONFLICTS

George-Adrian AIONESEI

“Henri Coandă” Air Force Academy, Brasov, Romania

Over the past two decades, social media platforms have evolved from simple means of communication into critical infrastructures of modern conflicts. Existing literature has documented the roles of propaganda, disinformation and media subversion, but often through isolated case studies (Gaurino, et al. 2020) or one-dimensional analyses (Marigliano, Hui Xian Ng and Carley 2024). Although valuable, these approaches fail to capture the evolutionary dynamics and interconnections of these phenomena across time and space. On this matter, this article proposes a comparative analysis of six key-events in recent history: jihadist propaganda in Iraq and Afghanistan, the mobilizations during the Arab Spring, the hybrid campaign in Ukraine (2014), the U.S. presidential elections (2016), the COVID-19 infodemic, and the full-spectrum information warfare between Russia and Ukraine. This article is intended to offer an evolutionary comparative framework of disinformation, propaganda and media subversion, with both academic and practical values.

Key words: social media, disinformation, propaganda, media subversion, modern conflicts.

1. INTRODUCTION

Once Russia’s full-scale invasion of Ukraine started in February 2022, the world witnessed not only a conventional military conflict, but also the emergence of the digital domain as a central component of warfare. On social media platforms, millions of users around the world followed in real-time videos and

posts presenting military convoys, missile attacks and strong emotional reactions. Both sides disseminated contradictory narratives through pro-Russian and pro-Ukrainian channels, manipulated images, stories and rumors at an uncontrollable pace, making the phenomenon difficult to manage. For the first time, social media platforms were more than

secondary means of communication; they were a central battleground, where public opinion has become a strategic target.

This new reality was not a technological revolution, but an evolution, where different situations added to social media platforms new dimensions, tactics and strategies (Benkler, Faris and Roberts 2018). In the era of traditional mass media, where propaganda was linked more to state actors and centralized channels, social networks changed this dynamic and created opportunities for multiple actors to participate, including civic movements, terrorist organizations or authoritarian governments. Traditional propaganda, viewed by Ellul (1965) as a systemic process of shaping opinions, was redefined in modern times. It is no longer acting vertically, from the powerful elite downwards, but also generates horizontal and viral narratives across all user levels (Bösch and Divon 2024). Nowadays, there are no issues regarding who produces the messages, but rather the ways used by media entities and partisan networks to create fertile environments for content amplification and polarization.

Disinformation, a phenomenon that took multiple forms throughout history (Rid 2020), can be simply defined as the deliberate creation and dissemination of false content for strategic purposes. It has become one

of the main interests in information research, especially after 2016, when there was a massive interference in the US presidential elections (Vosoughi, Roy and Aral 2018) (Howard, Woolley and Calo 2018). More recently, the COVID-19 pandemic demonstrated that disinformation affects not only politics, but also other aspects of everyday life, such as public health and social trust (Ferreira Caceres, et al. 2022). Disinformation can be analyzed from different points of view, such as the actors that disseminate it and the impact that it has on people. When we think about actors, there are studies that show that digital bots and automated networks play an essential role in accelerating the spread of false information (Zannettou, et al. 2019) (Chengcheng, et al. 2018), and other studies that show the opposite, that humans themselves are the ones that spread false content more, because they find it more attractive, shocking and impactful than fact-checked information (Vosoughi, Roy and Aral 2018). Switching to the impact that disinformation might have on people, studies such as of Ferreira et al. (2022) present clear effects on trust in public institutions and on health system.

If propaganda focuses on persuasion and disinformation on deception, media subversion aims to manipulate the truth in order to control and erode the functions

of main institutions in a state. Researchers such as Pomerantsev (2019) or Rid (2020) emphasize the idea that in current times, the main objective of information operations is not necessarily to convince, but rather to spread confusion and cynicism, creating an appropriate environment for narrative domination. One of the best strategies in this regard is the *firehose of falsehood*, attributed to Russia's strategic actors. They do not seek coherence, but saturation and repetitiveness, flooding the information space with so much content that users can no longer distinguish between truth and falsehood.

These phenomena are an important element of the social media platforms today, they mediate them; each platform shapes content flows and the methods used for propaganda and disinformation. For example, TikTok uses its algorithmic feed and focus on short-form video content to enforce emotional reactions and to weaponize audio-visual narratives in conflict. The encrypted channels and fast-spreading mechanisms of Telegram are the ideal infrastructure for coordinated campaigns to control digital communities, whilst Twitter (X) remains a relevant public visibility space. These approaches of different platforms demonstrate that there are no universal formula for digital propaganda, and that its techniques work to the extent that they align

with the attention architecture and community rules of each platform (Marino 2024) (Schrijver 2025). This system where the three phenomena are involved must keep pace with the latest technology in order to be effective and efficient, therefore there is a new dimension that needs to be taken into account: artificial intelligence and synthetic content. If initially deepfakes (Atlam, et al. 2025) were generating sparks of alarmism, recent studies (Diel, et al. 2024) (Ching, et al. 2025) show that their impact mostly depends on the audience biases and context. When spreading around key events, such as elections, they can destabilize and create confusion around users, however, their effects intensify where trust is already fragile. From this perspective, AI and its products (e.g., deepfakes) do not fundamentally change the way information operations work, but rather amplify existing vulnerabilities in the digital space.

Another aspect that is constantly changing lies in digital regulations. The European Union, through the Digital Services Act (DSA), and the Code of Conduct on Disinformation, introduced mandatory mechanisms for transparency and online responsibility, yet EDMO reports (Botan and Trisha Meyer 2025) show that there is a significant gap between norms and their application, while NATO StratCom Center of Excellence

emphasizes the capacity of both state and non-state actors to adapt faster to changes than regulatory frameworks. All these adaptations in real time and the applicability of norms push the actors to constantly find new ways and tactics that can be used in digital operations.

All these aspects put together create a broad picture of what digital environment has become over the last few years, and also it raises a question of *How have social media platforms evolved to become the strategic instruments in modern conflicts?* There are no straightforward answers for this, yet it has become clearer that propaganda, disinformation and media subversion cannot be treated as separate phenomena, but rather as a range of interconnected practices that overlap and complete one another. Another important aspect is that all these phenomena do not concern only the content's value of truth, but the focus is directed more on the institutions, the place where information gets validated, channels it goes through and what techniques are appropriate for what audience. Also, each phase of social media evolution added a new layer of sophistication, instead of entirely changing the way information operations unfold. What once served as an environment for civic interactions has been transformed into a conflictual informational space, where the rush for attention, high

intensity emotions and polarization shape the stability of current society.

2. COMPARATIVE ANALYSIS

In order to have a clearer picture of the way social media platforms have evolved into the instruments of propaganda, disinformation and media subversion as we know it today, we will use the comparative analysis method. The choice of this method is grounded in the very nature of the object of study: the phenomenon cannot be understood by analyzing a single case, but only by comparing multiple historic moments throughout past years that served as milestones regarding social media implications in modern conflicts. In this regard, we are able to capture both, what is specific for each event and the continuities that shape an evolutionary path.

For this comparison, we chose six representative cases: the jihadist propaganda in Iraq and Afghanistan (2003-2010), civilian mobilization during Arab Spring (2011), hybrid campaigns in Ukraine (2014), online interference during US presidential elections (2016), infodemic during COVID-19 (2020) and full-spectrum informational warfare in Ukraine (2022-2025). All of these were chosen based on three main criteria:

- Historical relevance – each event marked a significant change in the use of social media;

- Contextual diversity – the cases cover different situations – from conventional conflicts to hybrid warfare, up to political and worldwide health crises. This variety of situations emphasizes continuous adaptability of social media;
- Documentary availability – the selected episodes were well documented because of their importance for each period, providing a solid analysis.

In this sense, we opted for a comparative analysis between key-events, guided by an analytical matrix, approaching dimensions inspired both from earlier studies and from contemporary debates regarding informational security: *conflictual context, dominant platforms, main actors involved, tactics, target audience, impact on social cohesion, institutional responses* and lastly *evolutionary stage*. This structure offers a comparative framework that goes beyond the descriptive style and focuses more on pattern identification, and also, encompasses the complexity of this phenomenon on every layer, from the geopolitical context to the social and institutional effect. This approach allows us to articulate an evolutionary narrative and highlights the ways in which conflicts and crises have reshaped the use of social media instruments.

This helps to view social media differently, from a simple passive communication environment, to a strategic vector that transforms from one situation to another.

Conflictual context is a mandatory element, since neither propaganda nor disinformation operate randomly in a vacuum. Classical literature (Lasswell 1938) and current one (Benkler, Faris and Roberts 2018) show that the nature of the conflict, either conventional, hybrid or global, determines the way social media instruments are used. When we refer to an insurgent warfare, a protest movement or a global sanitary crisis, we also refer to the reasoning of what platforms become dominant and why specific informational tactics are preferred over others.

The second dimension of the matrix consists of the **dominant platforms**, because each social network has its technical and cultural characteristics, which for the most part conditions the flow of content. Recent studies show that TikTok promotes emotional behaviors (Bösch and Divon 2024), or that Telegram creates confused and decentralized information campaigns (Schrijver 2025). These environments have their own logic, presenting the fact that algorithms, networks and norms can drive to different results even though they are being used the same way.

A third dimension is represented by the **main actors** that use these platforms. Studies from Oxford Internet Institute (Bradshaw and Howard 2019) (Howard, Ganesh and Liotsiou 2019) highlighted that various actors involved in campaigns (state, non-state or hybrid) approach differently the coordination of resources for the same objective. State-sponsored troll farms, decentralized networks such as ISIS or spontaneous civic movements differentiate through strategies and capabilities, based on the actors involved, which justifies their part in this analysis.

Disinformation, propaganda and subversion cannot be possible without the use of specific **informational tactics** by these actors. Academic literature (Vosoughi, Roy and Aral 2018) (Chengcheng, et al. 2018) has shown that fake news spreads six times faster than the fact-checked news, due to the use of cognitive and emotional tactics, and most importantly the use of automated networks. Additionally, tactics have become layered: from rudimentary audio-video messages and influencing forums, to memes, micro-targeted elections, viral conspiracies and artificial intelligence deepfake content.

Also, this study needs to focus on **target audience** in order to justify the effort of the actors. This dimension derives from the psycho-

social literature on persuasion and polarization (Pasquetto, Lim and Bradshaw 2024) (Yang, et al. 2021). Disinformation and propaganda are chose based on the audience predisposition such as: local combatants, global population, political elite, institutional parties. The evolution of all cases, based on other dimensions too, shows a clear shift from small audiences to global masses, fact that amplifies more and more the complexity of the phenomena.

The sixth dimension defines the **impact on social cohesion**, which represents the objectives to attain through the other dimensions. Pomerantsev (2019) and Rid (2020) highlight that the central objective of current informational operations goes beyond the mere persuasion, but rather on controlling the population, undermining collective trust and diminishing the trust in legitimate institutions. Measuring this impact is not easy, but is mandatory to understand the effect on political and social stability in the long term.

After impact, there come the **institutional responses**, which constitute a crucial variable. As Carnegie Endowment (Bateman and Jackson 2024) or EDMO reports (EDMO 2023) show that technological companies, international organizations and state governments react to disinformation and propaganda campaigns,

supported by subversion techniques, they also reconfigure the war field in order to limit the phenomena. The results are not always what they expect, but rather push the aggressors toward new and more sophisticated alternatives.

Finally, the **evolutionary stage** dimension integrates the others above into a chronological and comparative frame. Its role is to describe the shift from the rudimentary dissemination (broadcast), to civil mobilization (weaponization) and ultimately to full cognitive battlespace. This dimension shows a longitudinal evolution, focusing on how each case not only reflects a particular

moment, but also adds a new layer to the digital threats.

The eight dimensions are not chosen randomly, but emerge from an integration of multiple literature sources, which helps construct a methodological framework, capable of capturing the evolution of the social media phenomena shown below Table 1.

Based on this matrix, the six case studies will be analyzed in order to identify and understand how social media has evolved and how propaganda, disinformation and media subversion have grown to the phenomena that define the informational warfare today.

Table 1 Comparative analysis matrix

Dimension	Key-questions / Indicators	Analytical relevance
Conflictual context	- What type of conflict is being analyzed (asymmetric, conventional, hybrid, global)?	Situates digital propaganda, disinformation and media subversion in their historical and geopolitical context.
Dominant platforms	- What are the main platforms used? - What are the key characteristics of the platform? - Were any other platforms involved?	Highlights the role of the platforms in attaining the objective and its relevance for the situation.
Main actors	- Who did create/distributed the content (state, non-state)? - What was the coordination regarding resources?	Clarifies the source/ sources of the content.

Dimension	Key-questions / Indicators	Analytical relevance
Tactics	<ul style="list-style-type: none"> - What type of content was used (written, video, meme, deepfake)? - What techniques were used (bots, trolls, algorithms, microtargeting)? 	Allows the comparison of sophistication levels across cases.
Target audience	<ul style="list-style-type: none"> - Who was the main target (local, regional, global)? - Why was the target selected? 	Shows the evolution from small to global audiences.
Impact on social cohesion	<ul style="list-style-type: none"> - What were the effects on trust on institutions? - Was there polarization, mobilization, radicalization? - What consequences have been documented? 	Shows the links between tactics and final objectives of each case.
Institutional responses	<ul style="list-style-type: none"> - What was the reaction of the governments? - Have there been any international initiatives? 	Assesses the degrees of institutional implication on resilience and adaptation.
Evolutionary stages	<ul style="list-style-type: none"> - Where does the case fit into: broadcast, mobilization, weaponization, cognitive battlespace? 	Integrates each case into a comparative evolutionary framework.

2.1. Afghanistan and Iraq (2001, 2003)

Conflictual context – Afghanistan (2001) and Iraq (2003) wars took place in a geopolitical context dominated by “war against terrorism”, launched after 9/11 attacks and were the first global conflicts of the digital era: The USA and other allies were promoting narratives related to democracy and national security, whilst insurgent and jihadist groups were fighting to demonstrate the legitimacy

of resistance and recruiting new members.

Dominant platforms – YouTube, jihadist forums, blogs and other independent websites were the main channels for this conflict. The content dissemination was based mainly on open access to forums and viral audio-video materials, rather than sophisticated algorithms.

Actors – *State actors*: The USA and other countries (the United Kingdom, Germany, Australia and

others) used strategic communication campaigns to justify war and maintain the public support. *Non-state actors*: Jihadist groups (Al-Qaeda, and later ISIS) used forums for recruitment and video content dissemination (taped executions, leaders' messages). *Global mass-media*: Al-Jazeera played an important hybrid role, spreading images and messages, that later went online.

Tactics – Jihadist groups introduced propaganda videos and motivational religious messages on a large scale. On the U.S. side, there were digital campaigns focused on positive narratives regarding the intervention and counter-messages against insurgent propaganda.

Target audience – *Local and Regional*: Iraq and Afghanistan population. *Globally*: international jihadist audience for propaganda and recruitment. The USA aimed for the Western countries.

Impact – Jihadist propaganda amplified radicalization and international recruitment fluxes, but at the same time fear and insecurity in the West. In western countries, continuous exposure to violence images led to political polarization and diminishing trust in official justifications of the war.

Institutional responses – The USA and others developed strategic communication programs and counter-narrative initiatives, but most of them were reactive. Social

media platforms did not have specific regulations against violent content, and the responses were more of a censorship than a specific strategy.

Evolutionary stage – This case relates more to a *broadcast*, where social media is used as a megaphone for visual propaganda and mobilization messages. Still rudimentary (absence of algorithms) the two conflicts have laid the groundwork for the use of social media instruments.

2.2. The Arab Spring (2011)

Conflictual context – Between 2010-2011, a series of protests unfolded in Tunisia, Egypt, Libya, Syria and other Arab states. The initial purpose was socio-economic (corruption, unemployment), but it switched quickly to political protest movements and civilian conflicts. The geopolitical context was one of authoritarianism where regimes had full control of traditional media.

Dominant platforms – Facebook and Twitter were the main platforms, completed by YouTube with videos. Hashtags such as #Jan25 became international symbols. In addition to the previous conflicts, the platforms were also used for direct coordination between protesters.

Actors – *Civilians and activists* used platforms for mobilization and protest organization. *Authoritarian regimes* tried to block Internet access. *Mass-media*: CNN, Al-Jazeera

amplified the visibility of protests.

Tactics – The use of hashtags was the new way to synchronize collective actions, spread images and send appeals for international solidarity. The focus was on visual authenticity.

Target audience – *Local* – local population. *External* – international community, for political support and movement legitimacy.

Impact – Social media was for the first time a parallel communication space, that destabilized state control over information. The civilian mobilization expanded rapidly, whilst the state-citizen relations were strongly affected.

Institutional responses – Local regimes tried to block Internet access and the functioning of networks. During that time, platforms still did not have robust mechanisms for moderation and presented the protests with minimal moderation and little censorship.

Evolutionary stage – This conflict marks the *mobilization* phase, where social media becomes an instrument for organization and coordination for people.

2.3. Ukraine – Crimea annexation and Donbas conflict (2014)

Conflictual context – In 2014, Russia annexed Crimea and supported the separatist conflict in Donbas. It was a hybrid confrontation, where conventional

and irregular military operations were combined with massive disinformation and propaganda campaigns, aimed at undermining the Ukrainian government and justifying the Kremlin actions. There were also tensions between NATO/EU and Russia, Ukraine being caught in the middle.

Dominant platforms – Facebook, Twitter and VKontakte were the main channels. VKontakte was very popular in the post-soviet space, and was used for aggressive pro-Russian propaganda. Also, YouTube and different forums were used to disseminate video and written content.

Actors – *State actors* – Russian government orchestrated propaganda campaigns. *Troll farms* (Internet Research Agency) created false networks to amplify messages. *Ukrainians (government and civilians)* replied with counter-narratives. *International mass-media*: western press documented the phenomenon.

Tactics – Kremlin used the “firehose of falsehood” strategy (multiple contradictory narratives, disseminated rapidly and repetitively, to create confusion and diminish trust in institutions. Also, news fabrication was used, imitating western press articles.

Target audience – *Internal* – Ukrainian population through “liberation” messages. *External* –

Russian population, for legitimacy. *Global* – international public opinion, bombarded with alternative narratives, creating confusion of what was actually happening in Ukraine.

Impact – Russian propaganda managed to destabilize Ukrainian informational space, enforce separatism in the East and diminish trust in national institutions. Globally, it created various perceptions about the Russian intervention legitimacy. For the first time, social media was considered a strategic weapon.

Institutional responses – Ukraine responded slowly through counter measures regarding propaganda and disinformation. EU and NATO started developing dedicated entities to combat these phenomena.

Evolutionary stage – Ukraine conflict marks the *weaponization* phase where social media platforms are considered part of the hybrid weapons used by a state.

2.4. US Presidential Elections (2016)

Conflictual context – The US presidential elections campaign (Trump vs. Clinton) took place in a polarized climate, marked by social tensions over immigration, globalization and national identity. On the other side, Russia conducted a systemic campaign of digital interference to create confusion and polarization.

Dominant platforms – Facebook and Twitter were the main channels

for disinformation. The algorithms were used more on these platforms and also on YouTube for aggressive content recommendation. Platforms became instruments for political micro-targeting.

Actors – *Internet Research Agency (IRA)*, based in Russia, with thousands of fake accounts and web pages managed to influence discourse. *Botnets* on Twitter amplified hashtags and attacked both candidates. *Internal actors*: partisans that amplified digital content.

Tactics – Fake pages that mimicked American organizations (veterans, minority groups, religious groups). Visual disinformation (memes, fake images). Micro-targeting through advertisements on Facebook for specific groups (based on occupation, beliefs or affiliation).

Target audience – Local: American electorate – amplify polarization. *Global*: creating an image of USA as unstable politically and socially.

Impact – This campaign amplified political polarization and diminished trust in the electoral process and traditional mass media. Social cohesion and democratic legitimacy have been affected.

Institutional responses – The interference triggered federal investigations and official reports that confirmed Russian presence in the process. Social media platforms introduced stricter regulations regarding political content and fake

accounts.

Evolutionary stage – This event marks the consolidation of *weaponization* stage, with different focus than before. Rather than focusing only on external destabilization, platforms are now considered means for manipulating internal affairs.

2.5. COVID-19 Pandemic (2020)

Conflictual context – The global 2019 pandemic was accompanied by a massive informational crisis. The lack of scientific certainties in the beginning meant that digital environment could easily be flooded by conspirative theories, rumors and deliberate disinformation campaigns. The World Health Organization (WHO) called this phenomenon an **infodemic**, an informational oversaturation, where there are no limits between truth and falsehood.

Dominant platforms – Facebook, Twitter and YouTube were the main dissemination spaces, alongside WhatsApp and Telegram (private channels) and TikTok, which grew bigger amongst young generation.

Actors – *Individual users* – millions of people distributed conspirative content voluntarily. *State actors* – Russia and China were accused of disinformation campaign in order to erode trust in public institutions.

Tactics – Infotainment – viral memes and videos with fake content. Image and video manipulation to

create panic. Conspirative theories (laboratory-made virus, Covid caused by 5G), fear and anger appeals.

Target audience – *Local* – particular communities, especially vulnerable and skeptical groups. *Institutionally* – WHO, EU, national governments for eroding legitimacy. *Global* – worldwide population, targeted according to cultural specifications.

Impact – Massive confusion, polarization and resistance to public-health measures. Many conspirative anti-vaccination campaigns provoked violent protests against authorized institutions.

Institutional responses – WHO, helped by national governments globally, launched fact-checking campaigns and collaborated with social media platforms to eliminate fake content. Not all platforms responded the same, Telegram and WhatsApp remaining difficult to regulate.

Evolutionary stage – This case marks the switch to cognitive battlespace phase, where social media instruments are considered beyond their potential to manipulate public opinion, but rather to undermine state capacity for crisis management.

2.6. Russia's invasion of Ukraine (2022-present)

Conflictual context – Initially perceived as a conventional war, the Russian invasion unfolded an unprecedented informational

warfare. Unlike the 2014 situation, the new digital confrontation is officially part of the military and diplomatic strategy. Both parties use social media as a parallel battlefield.

Dominant platforms – TikTok has become a crucial dissemination platform, either for propaganda or disinformation. Telegram represents the main channel of communication on the battlefield and worldwide. The rest of the platforms contribute to one side or the other, or neutrally, just presenting the situation.

Actors – *State actors* – Russian state – official and non-official campaigns of propaganda, trolls, botnets, pro-Kremlin Telegram channels. Ukrainian state – proactive digital campaigns (strategic communications). *Non-state actors* – civilians and journalists – videos from the battlefield; influencers – memes, campaigns, crowdfunding.

Tactics – Visual disinformation – reuse of older conflict images to spread confusion; divergent narratives – Russia promotes ideological ideas of “denazification” “NATO challenges”, whilst Ukraine focuses on narratives of resistance and victimization: deepfakes and AI generative content.

Target audience – *Locally* – Russian and Ukrainian populations for mobilization and justification. *Globally* – worldwide public opinion.

Impact – In Russia, digital propaganda consolidated

authoritarian control over population. In Ukraine, social media became a social resiliency instrument, creating a strong sense of unity.

Institutional responses – Platforms introduced new rigid measures, such as eliminating Russian media accounts, labeling manipulative content, collaborating with governments towards countering disinformation.

Evolutionary stage – This event marks the maturity of cognitive battlespace, where the main objective is to shape each user’s perceptions through strong emotions and cognitive behavior.

3. EMERGENT PATTERNS IN DIGITAL WARFARE

The analysis of the six cases, from jihadist propaganda in Iraq and Afghanistan, to informational full-spectrum Ukraine war, provides a detailed picture of how social media platforms have been instrumentalized in various warfare contexts. Besides each conflict particularities (culture, geopolitics, technology), a set of recurring dynamics emerges, adapted and refined over time, but also significant differences that mark the transition between particular phases. From a comparative point of view, the six cases present a series of common features that reveal the logic of how disinformation, propaganda and media subversion works, as well as the constant vulnerabilities of society

exposed to these phenomena.

Looking across the six cases chronologically, we can observe that alongside the evolution of tactics used in these conflicts, platforms also adapted accordingly in order to meet the new standards and expectations. Social media can no longer be considered a neutral entity, but it must be understood as an active actor that both shapes and is shaped by contemporary conflicts (Table 2).


The first common element is that social media has been used as the *main information infrastructure* in all cases. From the jihadist forums, to Telegram and TikTok, social networks have been used as a vector of amplifying messages, rising the visibility of actors, and challenging the informational power of states, regardless of the nature of the conflict.

The *dependence of emotions* was another fundamental aspect for communication on social media.


Fear and anger were exploited by jihadists, hope and solidarity during Arab Spring, resentment and confusion in Ukraine, identity rage and polarization during U.S. elections, anxiety and distrust during COVID-19 and both empathy and hatred in current Ukraine war.

Another common aspect is the *asymmetry* between offensive and defensive actions. In each case, the aggressors exploited platforms characteristics before official institutions did. The new hashtags were difficult to be countered initially, western countries have discovered election interferences too late, and fact-checking during the pandemic was not able to keep the pace with conspirative theories. Therefore, the *responses* to these new threats such as education, regulations or counter narratives were always **reactive**, giving the attackers a clear advantage.

Table 2 Evolution of social media aspects in modern conflicts



Case	Dominant platforms	Actors	Tactics	Objectives	Impact level
Iraq-Afghanistan	Forums, rudimentary websites, early YouTube	Non-state insurgents	Extreme videos, forum discussions	Radicalization and recruitment	Local
Arab Spring	Facebook	Civil activists, local citizens	Hashtag activism, viral posts	Mobilization and opposing regimes	National, regional



Case	Dominant platforms	Actors	Tactics	Objectives	Impact level
Ukraine (2014)	Vkontakte, Facebook	State actors (Russia)	Troll farms, fake news, coordinated campaigns	Destabilization, justification of Crimea annexation	Regional destabilization with global effect
U.S. Elections	Facebook, Twitter	State actors (Russia), private intermediaries	Micro-targeting ads, bots	Undermine trust in democracy	Electoral legitimacy with global concern
COVID-19	WhatsApp, Telegram	Transnational groups, influencers, conspiracy groups	Conspirative theories, memes	Undermine science, promote distrust	Global, institution trust
Russia invasion in Ukraine	TikTok, Telegram	Poly-actors: state, non-state, platforms, influencers, AI	Deepfakes, coordinated narratives	Perception control, polarization	Direct effect on regional, with global resonance

On the same note, we can observe a gradually *tactics stratification*. No technique has disappeared entirely, instead, it has been added to the existing collection. The extreme videos of jihadists were not replaced entirely, but rather are combined with trolling, activism, electoral micro-targeting or deepfakes. All of these tactics together create the stratified informational arsenal that can be adapted to current times based on objectives.

Besides disinformation and propaganda, social media has employed *subversion* throughout all

cases. In each scenario the indirect objective was to delegitimize a form of authority, from western military authority in Iraq and Afghanistan, to Ukrainian government, democratic institutions in the U.S. and scientific authority around the world.

On the other hand, if similarities of the six cases confirm transversal logic of propaganda, disinformation and media subversion on social media, the differences highlight a dynamic evolution of the three phenomena.

Firstly, the *main actors* have changed radically; from non-state

insurgent groups (Iraq-Afghanistan), civic activists (Arab Spring), and state actors (Russia), to multi-actor groups where states, technological platforms, civilians, influencers and AI algorithms work together.

The *objectives* have evolved from local recruitment and mobilization (2001) to state and electoral destabilization (2014 - 2016). The pandemic was the opportunity to undermine trust in science (2020) and the Russian invasion in Ukraine showed the power of perception controlling through parallel realities (2022-present).

Dominant platforms have undergone the most substantial evolution, due to technology advancement: starting with forums and YouTube videos as simple dissemination platforms, continuing with message viralization on Facebook and Twitter, up to globally and instantaneously distribution on TikTok and Telegram in the present.

Finally, the *degree of visibility* of operations has changed from explicit propagandistic messages, to covert and ambiguous campaigns (trolls, fake news, masked political advertisements), making it impossible in the present to distinguish a clear line between reality and manipulation.

4. CONCLUSIONS

This comparative analysis of the six cases shows not just similarities, differences, or patterns, but also a conceptual evolution that requires

rethinking how we conceptualize propaganda, disinformation and media subversion. In academic literature, the three phenomena are usually addressed separately: propaganda as a persuasion instrument, disinformation as false news spreading and subversion as a process to erode authority legitimacy and social cohesion. However, this comparison suggests that this separation is no longer relevant in the context of modern conflicts. They need to be seen as an informational ecosystem that provides the basis for threats identification and anticipation. We do not need to focus on propagandistic messages and fake news, but on how these phenomena are part of a long-term cognitive erosion strategy.

The main takeaway of this study is that *cognitive dimension* of modern conflicts must be treated the same as the military one. Actors that control digital narratives influence directly regimes legitimacy, social cohesion and states capacity to act accordingly. In this sense, there is a need for institutional mechanisms to monitor, anticipate and react to informational campaigns.

Also, the results show the fact that *late defensive actions* are not sufficient. All six cases present that offensive actors have exploited platforms faster than institutional authorities could respond. This leads to the need of a change in strategy, from mere reactive cognitive defense, to a proactive strategy

of *cognitive resilience*, based on digital education, regulations and collaboration between governments, platforms and civilians.

Additionally, the three phenomena have been studied and approached separately for specific contexts. Current reality suggests that *propaganda, disinformation and media subversion function as a unit* in the big picture of social media, creating the need for predictive instruments capable to identify not only fake content, but also patterns regarding emotions, algorithms and social vulnerabilities. This approach could serve as basis for new early warning models, useful for research, and most importantly national security policy.

REFERENCES

- [1] Atlam, El-Sayed, Malik Alamliki, Ghada Emarhomy, Abdulqader Almars, Awatif Esiddieg, and Rasha ElAgamy. 2025. "SLM-DFS: A systematic literature map of deepfake spread on social media." *Alexandria Engineering Journal* 446-455.
- [2] Bateman, Jon, and Dean Jackson. 2024. *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. Carnegie Endowment for International Peace.
- [3] Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. *Network Propaganda - Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.
- [4] Bösch, Marcus, and Tom Divon. 2024. "The sound of disinformation: TikTok, computational propaganda, and the invasion of Ukraine." *Sage Journal* 5081-5106.
- [5] Botan, Madalina, and Trisha Meyer. 2025. *Implementing the EU Code of Practice on Disinformation*. European Digital Media Observatory.
- [6] Bradshaw, Samantha, and Philip Howard. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation*. Oxford UK.
- [7] Chengcheng, Shao, Giovanni Luca Ciampaglia, Onur Varol, Kai-Cheng Yang, Alessandro Flammini, and Filippo Menczer. 2018. "The Spread of Low-credibility Content by Social Bots." *Nature Communications*. doi:<https://doi.org/10.1038/s41467-018-06930-7>.
- [8] Ching, Didier, John Twomey, Matthew Aylett, Michael Quayle, Conor Linehan, and Gillian Murphy. 2025. "Can deepfakes manipulate us? Assessing the evidence via a critical scoping view." *PLOS One* 20 (5).
- [9] Diel, Alexander, Tania Lalgı, Isabel Carolin Schröter, Karl MacDorman, Martin Teufel, and Alexander Bäuerle. 2024. "Human performance in detecting deepfakes: systematic review nad meta-analysos of 56 papers." *Computers in Human Behavior Reports* 16.
- [10] EDMO. 2023. *European Digital Media Observatory D.17 Public Report*. EUI - School of Transnational Governance.
- [11] Ellul, Jacques. 1965. *Propaganda - The Formation of Men's Attitudes*. New York: Vintage Books.
- [12] Ferreira Caceres, Maria Mercedes,

- Juan Pablo Sosa, Jannel Lawrence, Cristina Sestacovski, Atiyah Tidd-Johnson, Muhammad Haseeb UI Rasool, Vinay Kumar Gadamidi, et al. 2022. "The impact of misinformation on the COVID-19 pandemic." *AIMS Public Health* 262-277.
- [13] Gaurino, Stefano, Noemi Trino , Alessandro Celestini, Alessandro Chessa, and Gianni Riotta. 2020. "Characterizing networks of propaganda on twitter: a case study." *Applied Network Science*.
- [14] Howard, Philip, Bharath Ganesh, and Dimitra Liotsiou. 2019. *The IRA, Social Media and Political Polarization in the United States, 2012-2018*. University of Oxford.
- [15] Howard, Philip, Samuel Woolley, and Ryan Calo. 2018. "Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration." *Journal of Information Technology and Politics* 81-93.
- [16] Lasswell, Harold. 1938. *Propaganda Technique in the World War*. New York: Peter Smith.
- [17] Marigliano, Rebecca, Lynnette Hui Xian Ng, and Kathleen Carley. 2024. "Analyzing Digital Propaganda and Conflict Rhetoric: A Study on Russia's Bot-Driven Campaigns and Counter-Narratives during the Ukraine Crisis." *Social Network Analysis and Mining* 14 (1).
- [18] Marino, Sara. 2024. "Refugees' Storytelling Strategies on Digital Media Platforms: How the Russia-Ukraine War Unfolded on TikTok." *Social Media + Society* Sage Journals 10 (3).
- [19] Pasquetto, Irene, Gabrielle Lim, and Samantha Bradshaw. 2024. "Missinformed about misinformation: On the Polarizing Discourse on Misinformation and its Consequences for the Field." *Harvard Kennedy School Misinformation Review*.
- [20] Pomerantsev, Peter. 2019. *This is Not Propaganda*. London: Faber & Faber.
- [21] Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.
- [22] Schrijver, Peter. 2025. "Ukrainian Intelligence's Use of Telegram in Wartime." *International Journal of Intelligence and Counterintelligence* 1-27.
- [23] Vosoughi, Soroush, Deb Roy, and Sinan Aral. 2018. "The Spread of True and False News Online." *Science* 359: 1146-1151. doi:https://doi.org/10.1126/science.aap9559.
- [24] Yang, Kai-Cheng, Francesco Pierri, Pik-Mai Hui, David Axelrod, Christopher Torres-Lugo, John Bryden, and Fillippo Menczer. 2021. "The COVID-19 Infodemic: Twitter versus Facebook." *Big data & Society* 1-16.
- [25] Zannettou, Savvas, Tristan Caulfield, Emiliano Cristofaro, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn. 2019. "Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and their Influence on the Web." *Companion The 2019 World Wide Web Conference*.

KEEPING THE BALANCE BETWEEN ETHICS AND EFFECTIVENESS IN COMMUNICATION

Brîndușa Maria POPA

Regional Department of Defense Resources Management Studies,
Brasov, Romania

Today's geopolitics has become more and more complicated, alliances change and the geopolitical actors shift from the background to the spotlight very quickly. In such a volatile environment, communication is a critical tool wielded by states and non-state actors alike. The tension between maintaining communication ethics—grounded in truth, transparency, and respect—and the urgent demand for communication efficiency—speed, clarity, and impact—has become increasingly pronounced. This article analyzes the complex interplay of these forces, with a focus on the influence of digital technologies, social media and information warfare. Drawing on case studies of the Russia-Ukraine conflict and global COVID-19 messaging, it tries to illustrate how ethical compromises can undermine efficiency in the long term and argues for a balanced communication strategy that upholds ethical standards without sacrificing strategic effectiveness.

Key words: communication, geopolitics, ethics, efficiency, effectiveness.

1. INTRODUCTION

In the interconnected, information-saturated era, geopolitical communication has become both a battlefield and a bridge. Nations and political entities depend on timely and persuasive communication to assert influence, shape narratives and mobilize support domestically and internationally (Nye: 2004; Pamment: 2013). However, the need for rapid and

impactful messaging often collides with communication ethics, which demand honesty, accountability and respect for audiences (Simons: 2008; Waisbord: 2018).

This article explores how the pressure for communication effectiveness and efficiency can both complement and conflict with communication ethics in geopolitical contexts by examining the role of technological advancements and

providing examples to illustrate the consequences of this balance or imbalance.

2. COMMUNICATION ETHICS IN THE GEOPOLITICAL ARENA

For the article, we used a qualitative research methodology based on two primary methods: literature analysis and organizational observation.

2.1. Literature Analysis

Ethical communication in geopolitics refers to adherence to universal principles such as truthfulness, transparency, fairness, respect for sovereignty and human rights. (Habermas: 1984; Simons: 2008)

These principles are vital for:

- Building trust between nations and publics;
- Supporting legitimacy in diplomatic actions;
- Facilitating constructive dialogue and conflict resolution.

In the following paragraphs, we will examine each of these principles individually:

Building trust between nations and publics

Trust is the cornerstone of any effective communication, especially in geopolitics, where misinformation or deception can

have far-reaching consequences. Ethical communication — based on honesty and transparency — creates a foundation of credibility between states and their publics, both domestically and internationally. When governments communicate truthfully, it reduces suspicion and fosters a cooperative atmosphere. For example, during diplomatic negotiations, when parties share accurate information about their intentions and capabilities, it prevents misunderstandings that could escalate into conflict. The establishment of trust also enhances the ability to form alliances and joint initiatives, as seen in longstanding partnerships such as NATO, where transparent communication maintains cohesion among member states (Habermas: 1984; Simons: 2008; Nye: 2004).

Supporting legitimacy in diplomatic actions

Legitimacy in diplomacy hinges on the perception that a state's actions and communications are honest, fair and respect international norms. Ethical communication contributes to this legitimacy by ensuring that states do not resort to propaganda, deceit or manipulation. For instance, a country that transparently explains its foreign policy decisions, even when controversial, is more likely to gain respect and understanding from the international community. This legitimacy is essential for enforcing

treaties, securing international support and engaging in multilateral organizations like the United Nations or the World Trade Organization. Conversely, when states disseminate false narratives or conceal critical information, they risk diplomatic isolation and the erosion of their global standing (Simons: 2008; Pamment: 2013; Rid: 2020).

Facilitating constructive dialogue and conflict resolution

Ethical communication is vital in creating conditions conducive to dialogue and the peaceful resolution of conflicts. By committing to truthfulness and respect for all parties, communicators reduce hostility and open channels for negotiation. For example, during peace talks, unbiased and transparent information sharing helps build mutual understanding and allows conflicting parties to find common ground. This was evident in the Camp David Accords between Egypt and Israel in 1978, where direct and honest communication facilitated one of the most significant peace agreements in the Middle East (Bratic & Schirch: 2007; Habermas: 1984).

Additionally, during humanitarian crises, ethical communication ensures that all stakeholders have accurate information, preventing misinformation that could exacerbate tensions or lead to harmful

interventions (Simons: 2008; WHO: 2020). For example, during peace negotiations or humanitarian crises, ethical communication helps prevent misinformation that could escalate tensions or harm vulnerable populations. (Bratic & Schirch: 2007). The United Nations often stresses the importance of ethical communication to maintain international peace and security.

2.2. Effectiveness and efficiency in geopolitical communication

In the study of geopolitical communication, the distinction between communication effectiveness and communication efficiency offers a critical analytical lens for understanding how state and non-state actors construct, disseminate and manage strategic narratives on the global stage. Although frequently conflated, these two concepts represent distinct dimensions of communicative practice, each with implications for international relations and foreign policy outcomes.

2.2.1. Communication effectiveness

Communication effectiveness refers to the extent to which geopolitical messages achieve their intended strategic and policy objectives. It emphasizes not only the accurate transmission and

reception of information but also the message's capacity to influence perceptions, attitudes, and behaviors among target audiences (Nye: 2004; Miskimmon, O'Loughlin, & Roselle: 2013). Within a geopolitical context, effectiveness may be assessed through the lens of strategic narrative theory, which posits that actors seek to shape shared understandings of international order and legitimacy through carefully crafted storytelling (Miskimmon et al. : 2013).

For instance, when a state publicly frames a territorial dispute as a defense of international law rather than a unilateral land grab, the effectiveness of this communication lies in its ability to garner diplomatic support and legitimize its actions in the eyes of global audiences. Similarly, soft power campaigns aimed at building long-term international goodwill rely heavily on sustained, effective communication to embed favorable images of a state within foreign publics (Nye: 2008).

2.2.2. Communication efficiency

Conversely, communication efficiency pertains to the optimal use of resources—time, economic costs, technological tools—in disseminating geopolitical messages.

Efficiency focuses on the operational aspects of communication: the speed of delivery, the breadth of reach and

the minimization of material and symbolic costs (Entman: 2008). In an era characterized by instantaneous digital connectivity and global media networks, geopolitical actors increasingly prioritize rapid, scalable and cost-effective messaging strategies.

Social media diplomacy (“Twitter diplomacy”), for example, allows leaders to broadcast official statements to global audiences in real time, bypassing traditional intermediaries and reducing logistical constraints. However, while such channels enhance efficiency, they also risk sacrificing nuance and context, potentially undermining overall effectiveness if the message is misinterpreted or generates unintended backlash.

2.2.3. The tension and interdependence between effectiveness and efficiency

While analytically distinct, effectiveness and efficiency are deeply interdependent in practice. A communication strategy that is highly efficient but fails to resonate with its intended audience ultimately lacks strategic value. Conversely, a highly effective campaign that requires disproportionate resources or lengthy timelines may prove unsustainable or vulnerable to counter-narratives.

From a constructivist perspective, where the power of ideas

and narratives shapes international outcomes, both effectiveness and efficiency are central to a state's ability to enact "discursive power" (Hopf: 1998; Wendt: 1999). Actors must continually balance these dimensions to maintain credibility, respond rapidly to crises and adapt to evolving geopolitical landscapes.

3. THE INFLUENCE OF TECHNOLOGY ON COMMUNICATION ETHICS, EFFICIENCY AND EFFECTIVENESS

3.1. The impact of technological advancements and AI driven tools

Technological advancements, especially social media and AI-driven tools, have transformed geopolitical communication. The following paragraphs will examine these factors in detail.

Social Media Platforms: Enable real-time dissemination and direct engagement with global audiences, but also facilitate the spread of misinformation and propaganda. (Waisbord: 2018; Wardle & Derakhshan: 2017). Algorithms often prioritize sensational content, risking ethical breaches for efficiency gains.

Deepfakes and AI-generated content: they present new ethical dilemmas by creating realistic but false images and videos that can deceive and manipulate public

opinion (Rid: 2020).

Surveillance and data analytics: Governments may use data-driven insights to tailor messages effectively, but risk violating privacy and ethical standards. (Zhao: 2007)

While technology boosts communication efficiency by enhancing reach and immediacy, it simultaneously complicates adherence to ethical standards, demanding vigilant oversight and responsible use.

3.2. Tensions and trade-offs between ethics and effectiveness

The relationship between ethics and effectiveness in geopolitical communication represents a core tension that shapes strategic decision-making and public diplomacy outcomes. While the ultimate goal of communication campaigns is often to achieve effectiveness — that is, to influence target audiences, shape narratives and accomplish political or strategic objectives — this imperative frequently conflicts with ethical considerations rooted in norms of transparency, truthfulness and respect for audiences.

In practice, states and other geopolitical actors are often tempted to prioritize persuasive impact over moral integrity. For example, during international crises or conflicts, strategic communication campaigns may rely on selective presentation

of facts, emotional appeals or even disinformation to achieve rapid mobilization of public support or to undermine adversaries. These approaches might be highly effective in the short term, but can erode credibility, undermine democratic values and damage long-term legitimacy (Bjola & Holmes: 2015; Nye: 2008).

Moreover, effectiveness-driven strategies can conflict with the principle of respecting audience agency. When states frame messages using fear, threat inflation or other manipulative techniques, they deprive audiences of the ability to make informed, autonomous judgments (Gilboa: 2008). This tension is further complicated by the affordances of digital platforms, which favor emotionally charged and simplified content, amplifying the trade-off between reach and ethical responsibility (Manor: 2019).

From an ethical standpoint, geopolitical communication should ideally strive for a balance that upholds normative commitments to accuracy and respect for human rights while, still pursuing strategic objectives. This notion is reflected in the emerging concept of “ethical effectiveness,” which emphasizes that durable strategic gains are more likely to be achieved through credible and morally sound communication

(Seib: 2012).

Ultimately, the question is not whether effectiveness or ethics should be prioritized absolutely, but how they can be integrated in a manner that reinforces both immediate objectives and long-term trust. Scholars argue that credibility, once lost, is difficult to regain and that ethical lapses may produce counterproductive effects, such as backlash from domestic or international audiences (Cull: 2009). Thus, sustainable geopolitical communication requires navigating these trade-offs carefully, recognizing that effectiveness achieved at the expense of ethics can ultimately undermine strategic interests.

The urgency of geopolitical crises often compels state and non-state actors to make difficult communicative choices, frequently privileging speed and strategic advantage over ethical considerations. In moments of heightened tension—such as military conflict, international sanctions or regime change—governments may feel pressured to act decisively and communicate rapidly, even if doing so requires compromising foundational democratic principles. One of the most common trade-offs is the sacrifice of transparency in favor of effectiveness. Faced with the risk of public panic or adversarial exploitation, authorities

may withhold critical information or selectively frame narratives. While such actions can produce short-term stability and operational clarity, they often erode long-term public trust and institutional credibility. This dynamic reveals a central dilemma in crisis communication: the need to manage immediate threats while preserving the legitimacy of democratic governance.

In addition to withholding information, some actors actively disseminate propaganda or disinformation to shape public perception or undermine opponents. Disinformation, as Rid (2020) notes, often blends truthful and false elements in ways that obscure fact from fiction, making it especially potent in the digital age. Similarly, Pomerantsev (2019) highlights how contemporary regimes use emotionally charged narratives to confuse audiences and solidify domestic control. Such tactics may produce short-term strategic gains—rallying nationalistic sentiment, justifying policy actions or discrediting foreign adversaries, but they also compromise the ethical foundations of public discourse. The normalization of disinformation can lead to increased polarization, cynicism, and the delegitimization of objective truth, particularly in democratic societies.

3.3. Tensions and trade-offs between ethics and efficiency

Another trade-off in times of crisis involves the simplification of complex geopolitical issues for the sake of public comprehension.

Communicators often distill intricate international dynamics into clear-cut narratives that audiences can readily grasp. While this can improve message penetration and coherence, it risks misrepresentation and manipulation. As Tuchman (1978) argues, the media's tendency to "frame" stories in a way that fits pre-existing templates often strips away nuance and context. Similarly, Hall's (1980) encoding/decoding model suggests that meaning is frequently constructed through dominant ideological positions, which can marginalize alternative interpretations. In simplifying the message, essential truths may be omitted, leading to misunderstanding and the reinforcement of uncritical national or ideological biases.

These patterns point to a broader ethical tension between effective crisis communication and the values of accountability, transparency and truth. Communicators in geopolitical crises are often caught in a balancing act, where the urgency of action conflicts with the deliberative nature of ethical engagement. The cumulative effect of prioritizing

efficiency over ethics can be profound, reshaping public trust, media landscapes and institutional norms. As such, understanding these trade-offs is essential for evaluating not only the strategic outcomes of crisis communication, but also its moral and democratic implications.

The urgency of geopolitical crises often forces actors into difficult choices:

- Compromising transparency for speed: Governments might withhold sensitive information to control narratives or avoid panic, which improves short-term efficiency, but damages long-term trust.
- Using propaganda or disinformation: States may deliberately distort facts to weaken adversaries or bolster domestic support, compromising ethics to achieve rapid persuasion. (Rid: 2020; Pomerantsev:2019)
- Simplifying complex issues: To ensure quick comprehension, messages might omit nuance, risking misunderstanding or manipulation. (Tuchman: 1978; Hall: 1980)
- These trade-offs highlight the complex balancing act

between communicating ethically and efficiently.

3.4. Case Studies

3.4.1. The Russia-Ukraine Conflict

The Russia-Ukraine conflict offers a vivid example of the struggle to balance ethical communication and efficiency:

Information Warfare: Both Russia and Ukraine engage in strategic messaging campaigns to influence global and domestic audiences. Russian state media has been accused of spreading disinformation, including false narratives about military actions, which challenges ethical norms, but aims to efficiently control the narrative. (Rid: 2020; Pomerantsev: 2019; Zhao: 2007). Ukraine, on the other hand, utilizes social media to rapidly share frontline updates and rally international support, emphasizing transparency to build trust. (Vaccari & Chadwick: 2020)

Ethical Dilemmas: While Ukraine prioritizes truthful reporting to gain legitimacy, the fast pace of conflict sometimes leads to unverified or emotional messaging, risking misinformation. Russia's approach favors message control and disinformation, sacrificing ethics for short-term efficiency, but

risking international backlash and credibility loss.

Outcome: The conflict illustrates that sacrificing ethics can undermine communication efficiency over time by eroding trust and mobilizing counter-narratives from international actors.

3.4.2. COVID-19 Geopolitical Messaging

The COVID-19 pandemic highlighted the critical role of communication ethics and efficiency on a global scale: (Kreps & Kriner: 2020; WHO: 2020).

Government transparency was supported in countries like New Zealand that emphasized transparent, consistent messaging to efficiently inform and engage their citizens, building public trust and compliance with health measures. (Simons, 2008; Bratic & Schirch: 2007)

Misinformation spread widely in countries whose governments delayed disclosures or downplayed risks in order to avoid economic panic or political fallout, prioritizing efficiency in controlling the narrative, but undermining ethical responsibility. This delay led to confusion, skepticism, and inefficient public health responses globally.

The World Health Organization stressed transparent and ethical communication to manage the pandemic collectively, but competing national interests sometimes led to fragmented and contradictory messaging, illustrating the tension between ethical communication and efficiency in a geopolitical context.

3.5. Strategies for Achieving Balance

Balancing communication ethics and efficiency requires:

Strategic transparency: Disclosing what can be ethically shared promptly, while protecting sensitive security information. (Habermas: 1984; Simons: 2008)

Verification before dissemination: Ensuring messages are accurate and credible to maintain long-term trust.

Ethical use of technology: Leveraging digital tools to enhance communication reach without enabling misinformation or privacy violations. (Wardle & Derakhshan: 2017; Zhao., 2007)

Audience-centered messaging: Respecting cultural and contextual differences while maintaining factual integrity.

Institutional frameworks: International bodies should promote guidelines and accountability standards to harmonize ethics and

efficiency. (Bratic & Schirch: 2007; Pamment: 2013)

CONCLUSION

In today's complex geopolitical environment, communication ethics and efficiency are deeply intertwined, yet often in tension. While rapid, efficient communication is vital for influence-building, crisis response, and the projection of soft power, the abandonment of ethical standards risks misinformation, loss of credibility and unintended escalation of conflicts (Nye: 2004; Simons: 2008; Rid: 2020). The integration of advanced technologies — including real-time social media dissemination, algorithmic amplification, and AI-generated content — has further intensified these challenges, creating an environment where speed and virality often take precedence over accuracy and accountability.

The drive for efficiency may push state and non-state actors to adopt sensational or emotionally charged messaging strategies designed to achieve immediate impact. However, such approaches can undermine long-term strategic interests by eroding public trust and delegitimizing future communication efforts. Indeed, as global audiences become more discerning and information-literate, credibility emerges as a critical strategic asset; once lost, it is exceedingly difficult to recover

(Nye: 2008; Bjola & Holmes: 2015).

Furthermore, the ethical dimension of geopolitical communication extends beyond truthfulness to include respect for audience autonomy and the avoidance of manipulative tactics. For instance, the deliberate use of disinformation campaigns, deepfake technologies, or astroturfing to simulate grassroots support may yield short-term tactical gains but carry significant reputational and diplomatic costs (Bennett & Livingston: 2018; Bradshaw & Howard: 2019). Over time, reliance on ethically dubious methods can provoke domestic backlash, foster international condemnation, and compromise a state's normative soft power.

A balanced approach that integrates ethical considerations into communication strategy is thus imperative. Upholding principles such as transparency, accountability, and factual accuracy not only mitigates the risk of strategic blowback but also reinforces legitimacy and enhances the perceived integrity of the actor on the international stage. Ultimately, sustainable geopolitical influence depends on cultivating trust-based relationships with both domestic and foreign publics — a goal that can only be achieved when ethical standards are treated not as constraints but as integral components of effective statecraft. By harmonizing ethics and

efficiency, states can secure a durable foundation for communication efforts that advance national interests while contributing to global stability and cooperative international order (Nye: 2004; Simons: 2008; Rid: 2020).

REFERENCES

- [1] Tuchman, G., *Making News: A Study in the Construction of Reality*, New York: Free Press, 1978.
- [2] Habermas, J., *The Theory of Communicative Action, Volume 1: Reason and the Rationalization of Society*, Boston: Beacon Press, 1984.
- [3] Simons, G., *Ethics and International Communication*, Journal of International Communication, 14(1), 2008, pp. 1–20.
- [4] Zhao, Y., *Communication in China: Political Economy, Power, and Conflict*, Rowman & Littlefield Publishers, 2007.
- [5] Bjola, C., & Holmes, M., *Digital diplomacy: Theory and practice*, Routledge, 2015.
- [6] Cull, N. J., *Public diplomacy: Lessons from the past. CPD Perspectives on Public Diplomacy*, Figueroa Press, 2009.
- [7] Gilboa, E., *Searching for a theory of public diplomacy*, The Annals of the American Academy of Political and Social Science, 616(1), 2008, 55–77. <https://doi.org/10.1177/0002716207312142>
- [8] Manor, I., *The digitalization of public diplomacy*, Palgrave Macmillan, 2019.
- [9] Nye, J. S., *Public diplomacy and soft power*, The Annals of the American Academy of Political and Social Science, 616(1), 2008, 94–109, <https://doi.org/10.1177/0002716207311699>
- [10] Seib, P., *Real-time diplomacy: Politics and power in the social media era*, Palgrave Macmillan, 2012.
- [11] Bratic, V., & Schirch, L., *Why and When to Use Media for Conflict Prevention and Peacebuilding*, Global Media Journal, 6(11), 2007, 1–17.
- [12] Entman, R. M., *Theorizing mediated public diplomacy: The U.S. case*, The International Journal of Press/Politics, 13(2), 2008, pp. 87–102.
- [13] Hopf, T., *The promise of constructivism in international relations theory*, International Security, 23(1), 1998, 171–200.
- [14] Miskimmon, A., O’Loughlin, B., & Roselle, L., *Strategic narratives: Communication power and the new world order*, Routledge, 2013.
- [15] Nye, J. S., *Soft power: The means to success in world politics*, Public Affairs, 2004.
- [16] Nye, J. S., *Public diplomacy and soft power*, The Annals of the American Academy of Political and Social Science, 616(1), (2008), 94–109.
- [17] Wendt, A., *Social theory of international politics*, Cambridge University Press., 1999.
- [18] Kreps, G. L., & Kriner, R. E., *Crisis Communication and Public Health Emergencies: A Strategic*

- Approach*, Routledge., (2020).
- [19] Pamment, J., *New Public Diplomacy in the 21st Century: A Comparative Study of Policy and Practice*, Routledge, (2013).
- [20] Nye, J. S., *Soft Power: The Means to Success in World Politics*, Public Affairs., 2004.
- [21] Rid, T., *Active Measures: The Secret History of Disinformation and Political Warfare*, Farrar, Straus and Giroux., 2020.
- [22] Waisbord, S., *Truth is What Happens to News: On Journalism, Fake News, and Post-Truth*, *Journalism Studies*, 19(13), 2018, 1866-1878.
- [23] Hall, S., *Encoding/Decoding*, in *Culture, Media, Language*, Routledge, 1980, pp. 128-138.
- [24] Wardle, C., & Derakhshan, H., *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe Report, 2017.
- [25] Pomerantsev, P., *This is Not Propaganda: Adventures in the War Against Reality*, Public Affairs, 2019.
- [26] Vaccari, C., & Chadwick, A., *Echo Chambers and Political Polarization on Social Media: The Moderating Role of News Use and Political Interest*, *Journal of Communication*, 70(5), 778-800, 2020.
- [27] WHO, *Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation*, World Health Organization Report, 2020.

EXAMINING THE UNITED STATES AIR FORCE FIGHTER AIRCRAFT SUPPLY CHAIN: HOW NATIONAL SECURITY, BUDGETING, AND MANPOWER CHALLENGES IMPACT MISSION CAPABILITY

Ciara C. WETZLER, Robert O. WALTON

*Embry-Riddle Aeronautical University, Daytona Beach, Florida, USA

This study examines how the COVID-19 pandemic severely disrupted the United States Air Force (USAF) supply chain, particularly concerning fighter aircraft, leading to further reductions in mission capability (MC) rates. Global delays and shortages in critical components and materials directly impair the Air Force's ability to respond to national security threats and maintain strategic deterrence. This disruption also strained the Department of Defense's (DoD) sustainment budget and manpower requirements. This research examines solutions the Air Force is exploring to combat supply chain disruptions, such as Conditions-Based Maintenance (CBM+) and Quality Function Deployment (QFD), to increase mission capability rates and relieve long-standing issues regarding manpower and budgeting constraints. These challenges highlight the urgent need to modernize supply chain systems, adopt long-term, flexible budgeting, and strengthen industry partnerships to improve readiness and ensure the timely delivery of critical fighter aircraft components during disruptions.

Key words: *supply chain, national security, budget, mission capability, manpower, fighter aircraft, and pandemic*

1. INTRODUCTION

The United States Air Force (USAF) is known around the globe for its air superiority due to the evolution of aircraft weapon systems (Brown: 2020). United States (U.S.) fighter aircraft are among the many airframes advancing through the

skies, but remain the only weapons that dominate it, at least for now. Unfortunately, the fighter fleet struggles to stay *mission-ready*, as proven by low mission capability (MC) rates (Leone: 2021). Evidence following the COVID-19 Pandemic indicates that the military was already

facing further exacerbated challenges in maintaining MC rate standards (Leone: 2021). The Department of Defense (DoD) anticipated pandemic impacts to depot maintenance and supply chain operations; therefore, appropriated \$475 million through the Coronavirus Aid, Relief, and Economic Security Act (CARES) Act to the U.S. Air Force in March 2020, see Figure 1 (GAO: 2021).

form of rate surcharges (GAO: 2021). This strain on the USAF supply chain creates a concern for national security, sustainment budgeting, and fulfilling manpower requirements, highlighting the need to prioritize future logistics and maintenance operations (Mattis: 2018). This situation has profound implications for operational readiness and the Air Force’s ability to respond to

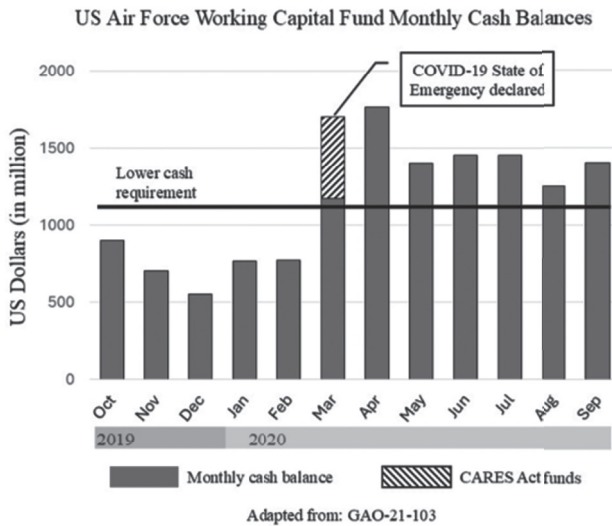


Fig.1 US Air Force working capital fund monthly cash balances

Despite this increase to the Air Force’s Working Capital Fund (WCF), the depots were still unable to support MC rates, flying hour programs, and produce anticipated revenues. The Air Force reported during fiscal year (FY) 2020 approximately \$355 million in maintenance and supply chain losses, which its customers covered in the

international conflict. Central to these challenges are the aging fleets of fighter aircraft (Losey: 2019). As aircraft age, complex and costly maintenance requirements increase, further straining financial budgets, part availability, and manpower skills. In recent years, the Air Force has overhauled its deployment operations to focus on the near-peer

war with countries such as China, North Korea, and Russia, which has placed pressure on the advancement of aircraft and training (Mattis: 2018). This research analyzes the Air Force's supply chain management system and its current strategies and efforts to mitigate these problems among fighter fleets, including modernization initiatives and process improvements to enhance mission capability and reinforce national security.

To set the stage on the scale of the problem, the F-22 *Raptor* is one of the newest Air Force fighter aircraft and entered service in 2005. From 2011 through 2019, the aircraft did not meet its annual availability or MC rate goals, with both availability and MC rates decreasing over this period (GAO:2020). The Operating and Support (O&S) costs for the F-22 were \$13.27 million per aircraft in 2018. With maintenance costs account for \$8.75 million (54 percent) of the total costs.

2. AIRCRAFT AGE AND UNSUSTAINABLE MAINTENANCE BURDEN

Today's fighter aircraft fleets reflect decades of technological innovation and aircraft evolution, dating back to World War I and II with icons such as the P-51 Mustang, to current modern stealth fighters like the F-22 Raptor and F-35 Lightning II

(Linden: 2004, Shklarsky & Shamir: 2023) However, as the fleets begin to age without timely replacements, these advancements struggle to remain sustainable. Mission Capability rates have perpetually experienced rate drops, partly due to part shortages, but mostly impacted by budgeting constraints and aircraft age. The DoD is concerned with affordability surrounding sustainment costs, new aircraft procurement, and modernization, which is currently totaling approximately \$23 million yearly (GAO: 2023).

According to the Government Accountability Office, most Air Force and Navy aircraft failed to meet MC rates between the years FY 2011- FY 2021, with the primary causes being maintenance delays and part availability. Out of the six Air Force fighters reviewed, none of them met MC rate goals in 2020 or 2021 (GAO: 2022). The COVID-19 pandemic further exacerbated existing supply chain and sustainment issues by disrupting supplier operations, delaying transportation of critical components, and limiting depot throughput due to manpower restrictions (GAO: 2021). As the Air Force continues to operate fourth-generation fighters beyond their intended service life, these issues will further create operational risk and threaten long-term fleet readiness.

2.1. Mission capability rates and flying hour programs

Mission capability rates established by the U.S. Air Combat Command (ACC) serve as key metric indicators for assessing the readiness of combat aircraft fleets within the U.S. Air Force (Leone: 2021). Maintenance squadrons utilize these metrics to monitor and report aircraft status, categorizing them as mission-capable or non-mission-capable based on maintenance needs (Leone: 2021). Through this data, maintainers can identify trends, prioritize repairs, and allocate resources effectively, ensuring that aircraft are maintained to the highest standards and ready to respond to operational demands. Unfortunately, this data cannot solve the current issue of a rapidly aging fleet and a bureaucratic supply chain system, especially regarding fourth and fifth-generation fighter jets such as the F-15, F-16, F-22, and F-35.

Reported MC rates over the last 12 years have proven that aircraft readiness is steadily decreasing each year (Cohen & Losey: 2022). From 2012 to 2018, there was a 7.93% decrease in MC rates across the Department of the Air Forces' 5,413 aircraft (Losey: 2019). The ACC MC rate standard is typically 75% or higher, and in 2020, most of the fighter aircraft fleets reported MC rates between 60-70%, remaining starkly below the standard (Leone:

2021). These rates raise national security and operational readiness concerns and impact the day-to-day operations supporting the bases' flying hour program (FHP) (Losey: 2019). Major Commands (MAJCOMs) create the requirements for FHPs based on the Air Force Flying Hour Model (AFFHM), which is outlined in the Air Force Instruction (AFI) 11-102, *Flying Hour Program Management*. These flight hours are critical for pilots to ensure they meet core tasks in their assigned airframe and are approved for downrange missions (Mills et al.: 2018). The Air Force's top priority is supporting the downrange mission; therefore, all mission-capable fighter aircraft are allocated for deployment operations. Most non-mission capable aircraft remain to meet home station needs, creating a difficult challenge for aircraft maintenance personnel directly responsible for fixing the jets and supporting the FHP (Losey: 2019). This unfortunate cycle has long been remedied through the experience of seasoned aircraft maintainers creating workarounds to keep generating aircraft sorties, which is not a sustainable solution (Losey: 2019). As the aging fleet continues to pose challenges for improving mission capability rates, the supply chain management system that supports it is equally outdated.

2.2. Challenges with supply chain, maintenance depots, and aging aircraft

The USAF's supply chain management system is at the core of keeping fighter aircraft operationally ready for down-range and home station requirements. Like many others, the military supply chain system comprises multiple nodes that work together to ensure non-mission-capable aircraft are swiftly repaired and returned to service. In addition to controlling aircraft parts, the Air Force's supply chain system manages many other vital parts, equipment, and weapons needed for base, deployment, transportation, and support operations.

The first step in the supply chain begins at the base level when aircraft maintenance personnel identify a broken part, initiating the repair process by documenting the issue and requesting a replacement through the Materiel Management flight. The Materiel Management flight, commonly called *supply*, is primarily responsible for assessing and managing most of the supply chain (Redfern: 2021). The Materiel Management flight consists of multiple sections mainly responsible for supporting maintenance operations, managing assets, and providing customer service (172nd Airlift Wing: 2024). If the part is available, aircraft maintenance will turn the damaged part into the Aircraft

Part Store (APS) section, where a one-for-one swap is accomplished. This repair level is called *base* or *intermediate maintenance* (Keating: 2019). If the part is unavailable at the base level, an order is submitted with a designated level of importance, which signals to the item manager at the maintenance depot how urgent the part is for mission capability. If an aircraft is unable to fly or is deemed non-mission capable, a Mission Impaired Currently Awaiting Part (MICAP) alert is placed on the part to increase resupply priority. The maintenance depots are larger warehouses that maintain extensive inventories for complex repairs and provide scheduled aircraft maintenance to ensure the aircraft remains safe for flight (Keating: 2018). Unfortunately, due to their backlog, depots are the primary hurdle for most supply chain challenges.

The aging of many aircraft, particularly fourth-generation fighters like the F-15, has directly correlated to an increase in unscheduled depot-level repairs or a high demand for MICAP parts that depots cannot fulfill (Keating: 2018). The fleets in service were not intended to operate for such extended periods, so spare parts demand was not projected. The introduction of newer fighter jets, such as the F-35, was created to replace some of the fourth-generation fighters;

however, with spare part shortages and insufficient supply chains to support repair demands, the F-35 will not be able to completely replace fourth-generation fighters anytime soon (Husseini: 2019). Despite the introduction of the first F-35 models in the early 2000s, replacing older combat aircraft like the A-10 and F-15 has seen minimal progress. This stagnation is primarily attributed to an unsustainable supply chain, along with significant challenges related to budgeting and manpower shortages. These factors have compounded the Air Force's difficulties in maintaining operational readiness and fulfilling its strategic objectives.

2.3. Enduring budgeting issues

The Air Force's budget deficits are longstanding concerns that have been acknowledged

for some time. Sustainment budget concerns can be traced back to the establishment of the Air Force as an independent branch on September 18, 1947, just after World War II (Linden: 2004). As personnel were disbanded, many aircraft were designated *out of service* due to inadequate maintenance and reduced funding. This led to fewer aircraft being delivered to replace aging or non-functional units (Linden: 2004). This cycle of downsizing non-mission-capable aircraft has repeated itself multiple times since 1947.

Most recently, the Air Force's

available fleet has dropped below 5,000 aircraft, which poses a concern for national security compared to its highest point of 26,104 active aircraft in 1956 (Losey: 2024). While the fleet's age has been used as an excuse for decommissioning aircraft over the years, so has the sustainment budget to keep these older fleets in MC status. Combat aircraft such as the F-15 and the A-10 cost more to sustain or replace than current funding levels allow due to the high cost of obtaining parts. Most recently, to combat the cost of supporting an aging fleet, Congress approved the purchase of the Boeing F-15EX model to retire the legacy F-15C/D models. This jet is an updated model of the current F-15C/D airframes while maintaining approximately 70% of the parts from the original design. This should help to reduce the overall supply chain cost to support the new model. However, the F-15EX costs more to produce per aircraft than to continue modifying the legacy models or purchasing more fifth-generation aircraft (Venable: 2021). Without harnessing the capability of flying in combat, the expected cost of a new F-15EX is estimated to be \$87.7 million (Venable: 2021). Once the necessary equipment is added to prepare the airframe for combat, the total cost for each aircraft reaches approximately \$102 million, making it, on average, 30% more expensive

than each F-35A, which costs \$77.9 million per unit (Venable: 2021). Following the passage of the Financial Responsibility Act in 2023 (U.S. Chamber Staff: 2023), Air Force leaders faced difficult decisions: either maintain the aging aircraft over 50 years old or retire them and prioritize new fifth-generation models (Losey: 2024). By fiscal year 2025, the Air Force plans to retire 250 aircraft, including the older F-15 models and the A-10 (Losey: 2024). With this spending cap, the Air Force removed five F-15EX's and five F-35A's from its budget for fiscal year 2025 in efforts to reallocate funding towards the development of future airframes, specifically the Next Generation Air Dominance program, which will focus on the integration of artificial intelligence and advancing capabilities in future combat aircraft (Losey: 2024). The Financial Responsibility Act will compel the Air Force to prioritize investments in aircraft programs that will prepare the DoD for its focus on future conflicts.

The Air Force has evolved in many ways since its creation. Not only have the aircraft requirements changed and advanced, but so has the training of the personnel, specifically, the maintenance and logistics personnel who directly support and repair the fighter fleets across the globe. Following the publication of the 2018 National Defense Strategy

(NDS), the Air Force's mission shifted to near-peer adversaries such as China and Russia; this shift established a renewed militant mindset for the Joint Force, which targets the importance of logistics and sustainment (Mattis: 2018).

2.4. Manpower and skillset concerns

Retired General Jim Mattis, who served as the United States Secretary of Defense from 2017 to 2019, stated in the NDS that the “backlog of deferred readiness, procurement, and modernization readiness” needed to be addressed and described key capabilities the Joint Force would improve upon over the coming years (Mattis: 2018, p. 6). This is where the idea of *adaptive basing* blossomed, currently known as Agile Combat Employment (ACE) (Cochran, et al.: 2023). To overcome adversaries in future conflicts, the Joint Force has restructured its deployment framework to support a more agile model capable of dispersing and rapidly regenerating forces across all domains, even under attack (Mattis: 2018). The ACE initiative and the directive to *accelerate change or lose*, by the previous Chief of Staff of the Air Force, General Charles Q. Brown Jr. (Brown: 2020, p. 3), prompted the Air Force to create a new concept termed *multi-capable Airmen* (MCA) (Cochran, et al.: 2023). Essentially, Airmen are not

only expected to be fully trained in their specific career field but also skilled in other vital tasks such as logistics, refueling, air and ground transportation, and agile combat tactics in contested environments (Cochran, et al.: 2023). Although implementing MCA intends to refine expeditionary combat skills, it poses an overarching concern for overextending maintenance and logistics Airmen (Cochran, et al.: 2023).

Aircraft maintenance is a specialized field that requires years of training to master “the launch, recovery, maintenance, and sustainment of aircraft supporting aircrew training operations while also operating and sustaining other essential aircraft support equipment” (Douglas, et al.: 2024, p. 5). The Air Force is already battling a shortage of skilled and experienced maintainers to tackle the growing issues of improving mission capability rates (Losey: 2019). These Airmen must manage the pressure of learning new skills beyond their expertise while continuing their regular duties. Implementing the MCA construct will provide numerous benefits to the force; however, it also entails a compromise for both the organization and the individuals involved, mainly regarding proficiency, development, and experience (Cochran, et al.: 2023). Without refocusing on retention and technical training, particularly in the

aircraft maintenance career field, the MC rates will continue to suffer and plummet below the standard level, thus contributing to a further decline in national security.

2.5. COVID-19 effects on supply chain operations

While enhancing mission capability rates remains a systemic challenge for the USAF, the COVID-19 pandemic exacerbated these difficulties within the supply chain (Boatman: 2023). This disruption resulted in substantial delays in delivering essential parts and materials, hampering maintenance efforts and leaving many aircraft grounded (Pecho: 2023). The U.S. Senate was informed through a supply chain risk report that the unpredicted impact of COVID-19 on supply chains weakened national security (Korkmaz: 2024). Reliance on outside countries, including the U.S. adversary China, for essential materials, raised concerns about the Department of Defense's ability to advance competitively and strategically (Korkmaz: 2024). For example, research following the origins of one million spare parts in 2011 uncovered that 70% of these parts were being manufactured in China (Korkmaz: 2024). Outsourcing materials has shown that numerous subcontractors are producing low-quality products that fail to meet the minimum design standards for

aircraft, particularly the F-35A (Korkmaz: 2024). This forces the defense industry to rely on one or two companies to source approved materials, imposing significant manufacturing limitations (Korkmaz: 2024).

The Aerospace Industries Association reported that COVID-19 led to the loss of 55,700 positions within the defense supply chain, compounding the workforce issues at maintenance depots, primarily staffed by government civilians, which faced severe manpower shortages due to health restrictions and illness. These shortages slowed down repair processes, making it increasingly difficult for depots and contractors to maintain production rates and fulfill contract obligations. For example, Lockheed Martin, the contractor for the F-35A, responded to COVID-19 by cutting production and adjusting work schedules to prioritize the health and safety of its employees (Tadjdeh: 2020). Lockheed Martin funded approximately \$750 million following the shutdowns to small businesses in their network in hopes of stabilizing the supply chain through this reduction in manufacturing (Tadjdeh: 2020).

Moreover, flying hour programs experienced a decline in training opportunities as access to operational aircraft was restricted, directly impacting pilots' readiness and proficiency (Losey: 2021).

This combination of material scarcity and manpower challenges undermined the effectiveness of defense projects and highlighted critical vulnerabilities in the supply chain that threaten national security (Douglas et al.: 2024). In response, military leaders are evaluating these significant shortcomings and exploring innovative projects and new processes to reduce costs, improve repair timelines, address parts shortages, and ultimately enhance Airmen's quality of life.

2.6. Modernization and advancement initiatives

The U.S. Air Force is actively pursuing innovative initiatives to combat their aging fleet through decreasing maintenance repair times and associated costs, improving supply chains, and strengthening national security, all while prioritizing the quality of life for Airmen. Among these initiatives are concepts such as Conditions-Based Maintenance (CBM+), Quality Function Deployment (QFD), and the establishment of the Tesseract office. Condition-Based Maintenance Plus (CBM+) leverages data analytics and advanced technologies to monitor the real-time health of aircraft systems (Mirnenko et al.: 2020). By using sensors and tracking data, the Air Force can predict maintenance needs before failures occur, allowing for timely interventions that

minimize downtime (Hardin: 2023). This proactive approach improves mission capability by ensuring aircraft are ready for deployment and reduces costs associated with unnecessary repairs and parts replacements.

In addition to CBM+, the Air Force is implementing QFD to better align maintenance strategies with the needs of operational units. Quality Function Deployment focuses on understanding customer requirements and translating them into actionable maintenance and logistics solutions (Tsarouhas & Makrygianni: 2017). By prioritizing user input, the Air Force can develop more effective processes through a mathematical approach that enhances the efficiency of supply chains and reduces lead times for critical parts (Tsarouhas & Makrygianni: 2017). Furthermore, establishing the Tesseract office signifies a commitment to innovative problem-solving and agile responses to current challenges. Tesseract was established to foster rapid experimentation and development, focusing on identifying and implementing cutting-edge technologies and methodologies, particularly in maintenance, logistics, and supply chain management (Duvall: 2022). By leveraging advanced data analytics, artificial intelligence, and modern engineering practices, the Tesseract Office aims to streamline processes, reduce

repair times, and ultimately improve mission capability. This initiative is part of the Air Force's broader effort to overcome emerging challenges by consulting lower-level Airmen and harnessing their innovative ideas (Duvall: 2022).

These initiatives collectively aim to combat the challenges posed by the pandemic, such as supply chain disruptions and staffing shortages, by fostering a culture of continuous improvement and agility within the Air Force. By streamlining maintenance processes and enhancing the quality of life for Airmen, these programs ensure that the Air Force remains well-equipped to meet current and future national security demands. The combination of predictive maintenance, user-centered design, and innovative organizational structures positions the Air Force to enhance its MC rates and resilience.

3. DISCUSSION

To effectively address the ongoing supply chain challenges facing the U.S. Air Force, it is essential to implement a comprehensive approach that targets both immediate and long-term resilience. The first critical step is to support the modernization of the USAF supply chain systems. This can be achieved by advocating for accelerating investments in advanced, resilient, and adaptive technologies, such as artificial intelligence (AI),

machine learning, and predictive analytics. These technologies can help the Air Force predict and manage supply chain disruptions before they escalate, enhancing the ability to respond quickly to unforeseen delays and shortages. Additionally, integrating real-time tracking systems and blockchain for transparency and accountability can ensure critical components are delivered on time and with minimal errors. The USAF must collaborate with technologists, logistics experts, and defense contractors to prioritize the development of such systems, ensuring the Air Force remains agile and capable of maintaining operational readiness in the face of global disruptions like the COVID-19 pandemic. By investing in these technologies, the USAF will be better prepared to face future crises without compromising mission capability.

Simultaneously, the Department of Defense (DoD) must adopt long-term budget flexibility and sustainability to better absorb the financial strain caused by supply chain disruptions. Traditional budgeting models have proven insufficient in addressing the unpredictable nature of global crises, as seen during the pandemic. To ensure that the USAF can maintain readiness despite external challenges, the DoD should explore implementing flexible, adaptive budgeting mechanisms that allow for rapid reallocation

of resources when unexpected supply chain issues arise. This could involve creating contingency funds or adjusting allocations based on real-time data that reflects the impact of supply chain disruptions. Moreover, the DoD should ensure that its budgeting approach accounts for the costs of maintaining aging aircraft and expanding the life cycles of critical components so that these factors do not diminish mission capability in times of need. Through more dynamic budgeting, the USAF could remain operational even during supply chain instability, supporting both short-term needs and long-term sustainability.

Another key initiative is to enhance collaboration with industry partners to address vulnerabilities in the USAF's supply chain. The pandemic underscored the importance of private-sector collaboration in mitigating supply shortages and delays. The USAF must work closely with defense contractors, manufacturers, and other stakeholders to co-develop innovative solutions that improve supply chain resilience. For example, partnerships with private companies specializing in materials science or logistics can help the USAF access cutting-edge solutions that streamline procurement processes, reduce lead times, and ensure the availability of critical components. By fostering a more collaborative

environment, the USAF can leverage the expertise and capabilities of the private sector, ensuring that components are delivered more efficiently and at scale, even during global disruptions. Additionally, joint ventures and information-sharing initiatives between military and industry partners can improve communication, forecasting, and responsiveness, allowing for a more agile and proactive supply chain system.

Together, these actions form a comprehensive strategy for enhancing the USAF's operational effectiveness in the face of future challenges. By modernizing the supply chain with advanced technologies, adopting flexible budgeting practices, and fostering stronger industry collaborations, the USAF can maintain its mission capability rates and ensure it is well-prepared to respond to national security threats. These initiatives will not only help mitigate the effects of past disruptions but also create a more resilient, sustainable defense infrastructure that can endure future global crises with minimal impact on readiness.

4. CONCLUSION

Examining the U.S. Air Force supply chain reveals critical implications that mission capability has on national security, budgetary constraints, and manpower

deficiencies. The primary challenges are an aging fleet and an unreliable supply chain system. Furthermore, the COVID-19 pandemic highlighted these vulnerabilities, resulting in significant delays in spare parts deliveries, loss of crucial positions, and heightened operational readiness concerns. If the Air Force fails to establish an effective supply chain, national security concerns will be profound, even with prioritizing aircraft modernization efforts. The evolution of modern-day warfare requires an agile and responsive supply chain capable of adapting to new threats and challenges.

Addressing these interconnected issues will require a comprehensive advancement that includes investing in new technologies, streamlining supply chain processes, and enhancing the training and retention of skilled personnel. Initiatives like *Agile Combat Employment* and the development of *multi-capable Airmen* reflect the Air Force's commitment to adapt to future conflicts. However, it is crucial to balance these innovative strategies with the need for specialized training and support for maintenance and logistics personnel. Initiatives such as CBM+, QFD, and Tesseract are expected to assist the Air Force in overcoming these obstacles. Without a renewed focus, the USAF risks further declining mission capability rates, compromising its

expeditionary response, national budget, and manpower capabilities during complex global conflicts.

For future research, these findings should be substantiated using primary data obtained from stakeholders, such as depot commanders, industry partners, and maintenance personnel.

Conflict of Interest Statement:

The authors declare no conflict of interest.

Data Access Statement: No data were generated or analyzed in this study.

Funding Statement: This research received no external funding.

REFERENCES

- [1] 172nd Airlift Wing. (2024). *Logistics Readiness Squadron*. 172nd Airlift Wing. <https://www.172aw.ang.af.mil/About-Us/Fact-Sheets/Display/Article/449309/#:~:text=MATERIEL%20MANAGEMENT%20FLIGHT%20%28LGRM%29%20The%20Materiel%20Management%20Flight>
- [2] Boatman, M., Mapp, J., Olsen, N., & Szatkowski, M. (2023, November 3). *Supply Chain Complexities: A Military Intelligence Approach*. Air University (AU). <https://www.airuniversity.af.edu/Aether-ASOR/Perspectives/Article-Display/article/3579465/#:~:text=Using%20multiple%20sources%20of%20information%20and%20analytical%20methods%20will%20help>
- [3] Brown Jr., C. Q. (2020). *Accelerate Change or Lose* (pp. 1–8). Department of the United States Air Force. <https://apps.dtic.mil/sti/pdfs/AD1109857.pdf>
- [4] Cochran, S., Abler, A. M., Keller, K. M., Lytell, M. C., Stallworth, R. L., Thulin, R. C., Toukan, M., Walsh, M., & Winston, I. (2023). *The Forces We Need: Building Multi-Capable Airmen to Enable Agile Combat Employment*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1746-1.html
- [5] Cohen, R., & Losey, S. (2022, February 14). *US Air Force fleet's mission-capable rates are stagnating. Here's the plan to change that*. Air Force Times; Air Force Times. <https://www.airforcetimes.com/news/your-air-force/2022/02/14/us-air-force-fleets-mission-capable-rates-are-stagnating-heres-the-plan-to-change-that/#:~:text=Ninety%20percent%20of%20the%20remotely%20piloted%20Reaper%20attack%20drones%20were>
- [6] Douglas, M., Roberts, M., & Ford, J. (2024). *People First, Mission Always: A Tension-Centered Approach to Conducting Safe, Effective Logistics*. *Journal of Business Logistics*, 45(4). <https://doi.org/10.1111/jbl.12393>
- [7] Duvall, J. (2022, March 17). *Tesseract spotlights major wins, encourages participation in accelerating change - Logistics*

- Officer Association. Logistics Officer Association. <https://atloa.org/tesseract-spotlights-major-wins-encourages-participation-in-accelerating-change/#:~:text=The%20Tesseract%20team%20has%20become%20the%20epicenter%20of>
- [8] Hardin, D. (2023, May 6). *Rapid Sustainment Office's CBM+ artificial intelligence toolkit earns Air Force System of*. Air Force. <https://www.af.mil/News/Article-Display/Article/3382513/>
- [9] Husseini, T. (2019, May 2). *F-35 progress: three challenges to the F-35 supply chain*. Airforce Technology. <https://www.airforce-technology.com/features/f-35-progress-supply-chain/?cf-view>
- [10] Keating, E. G. (2018). *The depot-level maintenance of DoD's combat aircraft: insights for the F-35*. Congress of the United States, Congressional Budget Office. <https://wayback.archive-it.org/6820/20210212081727/https://www.cbo.gov/system/files/115th-congress-2017-2018/reports/53543-depotmaintenancef35.pdf>
- [11] Keating, E. G. (2019). *Approaches to F-35 Depot-Level Maintenance: Insights from Other Systems*. Defense Acquisition Research Journal: 26(1), 2–17. <https://doi.org/10.22594/dau.18-804.26.01>
- [12] Korkmaz, G. (2024). *Supply Chain Risks and Management Strategies in the Defense Industry*. Journal of Defense Resources Management. 15(1). <https://doaj.org/article/d85ce77746014c23853a88844c5f487c>
- [13] Leone, D. (2021, November 23). *Mission capable rates dropped in 2021 for every USAF fighter type except the A-10 - The Aviation Geek Club*. The Aviation Geek Club. <https://theaviationgeekclub.com/mission-capable-rates-dropped-in-2021-for-every-usaf-fighter-type-except-the-a-10/>
- [14] Linden, J. R. (2004). *Bigger, better, faster, more: Jet fighter development and grand strategy in the United States Air Force, 1947–1953* (Order No. 1417608). Available from ProQuest One Academic. (305176598). <https://www.proquest.com/dissertations-theses/bigger-better-faster-more-jet-fighter-development/docview/305176598/se-2>
- [15] Losey, S. (2019, August 1). *Aircraft mission-capable rates hit new low in Air Force, despite efforts to improve*. Air Force Times. <https://www.airforcetimes.com/news/your-air-force/2019/07/26/aircraft-mission-capable-rates-hit-new-low-in-air-force-despite-efforts-to-improve/>
- [16] Losey, S. (2021, November 23). *“No company is immune”: Supply chain woes weigh on defense firms*. Defense News. <https://www.defensenews.com/air/2021/11/23/no-company-is-immune-supply-chain-woes-weigh-on-defense-firms/#:~:text=From%20massive%20deliveries%20of%20steel%20and%20aluminum%20needed%20to%20build>
- [17] Losey, S. (2024, April 23). *As the*

- US Air Force fleet keeps shrinking, can it still win wars?* Defense News. <https://www.defensenews.com/air/2024/04/23/as-the-us-air-force-fleet-keeps-shrinking-can-it-still-win-wars/#:~:text=The%20Air%20Force%20in%20fiscal>
- [18] Mattis, J. (2018). *Summary of the 2018 National Defense Strategy of the United States of America*. Department of Defense. <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>
- [19] Mills, P., Nowak, S., Buryk, P., Drew, J. G., Guo, C., & Vardavas, R. (2018). *Increasing cost-effective readiness for the U.S. Air Force by reducing supply chain variance: technical analysis of flying hour program variance*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2118.html.
- [20] Mirnenko, V., Pustovyi, S., Radko, O., & Yablonskyi, P. (2020). *Mathematical Model of Military Equipment Products Maintenance for the Condition-Based Operation Strategy Taking Into Account Type I Errors*. *Journal of KONBiN*, 50(1), 269–281. <https://doi.org/10.2478/jok-2020-0016>
- [21] Pecho, P., Višnai, K., Trško, L., & Dianovský, R. (2023). *The Effect of Long-Term Aircraft Parking on Propulsion Units During the Covid-19 Pandemic*. *Transportation Research Procedia (Online)*, 75, 229–239. <https://doi.org/10.1016/j.trpro.2023.12.026>
- [22] Redfern, L. R. (2021, February 12). *Materiel Management Flight: Supplying the Mission*. Defense Logistics Agency; Department of Defense. <https://www.dla.mil/About-DLA/News/News-Article-View/Article/2502352/#:~:text=The%2035th%20LRS%20Materiel%20Management%20Flight>
- [23] Shklarsky, I., & Shamir, E. (2023). *Driving innovation in air power: the cold war's four generations of fighter jets*. *Defense & Security Analysis*, 39(2), 146–170. <https://doi.org/10.1080/14751798.2023.2178071>
- [24] Tadjeh, Y. (2020). *Defense Industrial Base Rebounding From COVID-19*. *National Defense*, 105(800), 20–21. <https://www.jstor.org/stable/27023051>
- [25] Tsarouhas, P., & Makrygianni, M. (2017). *A framework for maintenance and combat readiness management of a jet fighter aircraft*. *International Journal of System Assurance Engineering and Management*, 8(Suppl 2), 1895–1909. <https://doi.org/10.1007/s13198-016-0481-8>
- [26] U.S. Chamber Staff. (2023, June 2). *U.S. Chamber Commends Passage of the Fiscal Responsibility Act to Avoid U.S. Default*. U.S. Chamber of Commerce. <https://www.uschamber.com/economy/u-s-chamber-commends-passage-of-the-fiscal-responsibility-act-to-avoid-u-s-default>
- [27] U.S. Government Accountability Office (GAO). (2020). *Weapon System Sustainment: Aircraft*

Mission Capable Rates Generally Did Not Meet Goals and Cost of Sustaining Selected Weapon Systems Varied Widely. <https://www.gao.gov/assets/gao-21-101sp.pdf>

[28] U.S. Government Accountability Office (GAO). (2021). *Depot Maintenance: DOD Should Improve Pandemic Plans and Publish Working Capital Fund Policy.* Gao.gov. <https://www.gao.gov/products/gao-21-103>

[29] U.S. Government Accountability Office (GAO). (2022). *Weapon System Sustainment Aircraft Mission Capable Goals Were Generally Not Met and Sustainment Costs Varied*

by Aircraft Report to Congressional Committees. <https://www.gao.gov/assets/gao-23-106217.pdf>

[30] U.S. Government Accountability Office (GAO). (2023). *Tactical Aircraft: Technical, Delivery, and Affordability Challenges Complicate DOD's Ability to Upgrade Its Aging Fleet.* Gao.gov. <https://www.gao.gov/products/gao-23-106694>

[31] Venable, J. (2021, Mar 22). *Why the F-35 Rules: Study History, Study Costs, Study Threats.* CE Think Tank; Newswire <https://www.proquest.com/wire-feeds/why-f-35-rules-study-history-costs-threats/docview/2504276268/se-2>

THE ENCOURAGEMENT OF ARMS EXPORT IN DEVELOPING COUNTRIES: CAUSALITY ANALYSIS BETWEEN DEFENSE EXPORT, GDP AND DEFENSE EXPENDITURE IN TURKIYE

Meliha ENER*, **Nazan YELKIKALAN****, **Selen SAVAŞKAN*****

*Department of Economics, Biga Faculty of Economics and Administrative Sciences, Onsekiz Mart University of Çanakkale, Çanakkale, Turkiye

**Department of Business Administration, Biga Faculty of Economics and Administrative Sciences, Onsekiz Mart University of Çanakkale, Çanakkale, Turkiye

***Biga Faculty of Economics and Administrative Sciences, Onsekiz Mart University of Çanakkale, Çanakkale, Turkiye

The aim of this study to investigate the the role of defense export in developing countries and also its effects on military expenditure and gross domestic product (GDP) in Turkiye during the period 2001-2024. In addition to theoretical approach, an empirical study was also used in the causality analysis between variables. A Toda Yamamoto granger causality test was performed between defence export, GDP and military expenditure. We demonstrated that increased GDP can facilitate defense export and defense expenditure may have positive effects on economic development in long run. Turkish military production and development activities have accomplished self reliance to proceed the higher amount of defence export. The greater demand for Turkish higher technology military products should enable Turkiye to increase defence export rapidly in near future. Conclusively, developing countries should reinforce their defense industries to decrease technology dependence and develop longstanding sustainable defense export to lower financial burden of military expenditure.

Key words: *defense export, arms trade, defence industry, defense expenditure, time series analysis, economic growth, Toda Yamamoto Test*

1. INTRODUCTION

It is well understood that the connection between defense expenditure and economic growth is controversial. Economic growth has a predilection to elevate defense expenditure as would be seen in major defense exporter countries, such as USA and Russia. As mentioned before, relationship between defence expenses and economic growth seems to be positive or noncausability between the two variables (Abdel-Halek et al, 2020). Thereby, defense export lowers financial difficulties from military production and import. Defense industry manufactures sophisticated products which have higher added values and improved quality for export by the means of skilled and experienced technical labour force. It can also create alternative partnerships in civilian sector and bidirectional shifts of skilled human resource occurs between military sector and civilian one. By the means of research and development activities, military industry encourages defense export and can stimulate economic growth in the long term. Elucidative determination of demand for military expenses appears to be difficult in theoretic and empiric studies (Sezgin and Yıldırım, 2002). We intend to investigate the long run relationship between defense expenditure, economic growth and defense export in Türkiye.

2. REVIEW OF LITERATURE

Following the world war II, there have been remarkable progresses in defense industry and international arms trade which motivated countries to involve in export market with the aids of military organizations of capitalist and socialist systems, respectively NATO and Warsaw Pact between 1945 and 1991 (Krause, 1992). During Cold War, strategic and politic considerations were ruling on ultimate decision making, for this reason, governments had imposed regulatory measures on arms exporters (Kinsella, 2011). The USA and The USSR were dominant arms producer and exporter countries, since they had hegemonic positions in military industry and marketing capacity. The other prominent arms exporters were France, the UK and FRG (Federal Republic Germany) in western or capitalist bloc (Beraud-Sudreau, 2019). Moreover, Czechoslovakia and Poland had increased significantly their defense export in eastern or socialist bloc until the late 1970s. Subsequent to that, Brazil, Canada, Sweden, Netherlands and Israel has also appeared as new arms exporters. Arms race with the USSR and the desire for enhancing the indigenous arms production capability in Western Europe have made an increase in arms export among capitalist countries between 1980 and 1991, with the maximum year of 1982. After the collapse

of the USSR, there was a decline in international arms trade due to impressively diminished demand for arms around the World from 1992 to 2002, with the minimum year of 2002. Especially European countries decreased defense budgets due to termination of cold war which resulted in lowered number of companies and remarkable workforce loss in defense industry. (Buttler C et al, 2000). Companies carried out export with strategic alliances in globalized arms market for survival of defense sector at a competitive advantage. Despite, existence of intermittent regression or stagnation intervals especially from 2003, There have been also a persistent increase in the demand for military expenditure and arms trade due to new threats from regional conflicts, civil wars, and international terrorism during post Cold War duration (Barros and Sandler, 2003).

Uncertainty and threats determined by national governments, as a rule, design defence industry to impede regional conflict and lessening the its costs (Hartley, 2012). In confrontational or unstable regions, economic and political infrastructures of these nations tend to be more desirable to manufacture weaponry for minimizing the delay in national security. It is generally accepted that the influence of government ideology on arms export decisions has been subjected to different considerations (Camola, 2012). Right wing and coalition

governments wish to export more defense products to countries with market liberalization and property rights protection. While, on the contrary, left wing governments seem to prefer for exporting arms to selected countries which have human rights protection and are not involved in conflict (Brender, 2018).

The impact of defense expenditure on economic growth has been found nonsignificant or negative. (Dunne et al, 2006). It has a non-linear effect on growth due to reciprocal interaction between the productivity ascend and tax mutilation in rise of defense expenses. In order to lower impairment in economic growth, net defence export must be elevated greatly (Yakovlev, 2007).

Military spendings heighten economic growth and reinforce the arms investments in developed countries which have improved domestic defense industry and arms export (Masoud and Zaleha, 2015). Debt burden due to military expenditures in nations without efficient defence industry for providing the domestic needs results in production incapability and balance of payments deficit (Kollias et al, 2004), and also enhances the unemployment (Korkmaz, 2015 and Karagöl, 2005). Fullfilling the persistence of security is obligatory to keep sustainable growth and development (Dudzevicivte, 2021). Thence, an effort to produce for revenue generating arms export will relieve the debt burden of defence

spendings and can also be useful to provide the civil commodities which have been restricted due to shortage of foreign exchange stock in developing countries. Whereas, governments in developed nations reinforced the arms export to sustain their leading production competence and for establishing the country-wide safety as well as foreign policy implications with military aid across the world. Besides, they usually act as ultimate decision maker for determining the foreign military sales and export country. The desire for establishing a strong military industry and shrinking the domestic market have led to develop an effective and sustainable arms export policy, as would be seen in Germany where defense industry serves the export market, while the defense corporations in the USA mainly subject to security and strategic implications (Blum, 2019).

Defense expenditure also play a significant role for maintaining the arms export and for promoting the foreign investors. Since, heavy burden of defense budget due to inefficient domestic industry for securing the costly military equipments, governments have restructured defense industries into more proficient to create and export arms as a partial solution to alleviate financial problems and higher unemployment. On the other hand, the need for protection of domestic establishments from foreign competition also leads to support of private sector which produces more

efficiently to increase revenue and highpriced export. In order to enter international market, developing countries have to manufacture under the great difficult conditions for more sophisticated arms subjected to restrictions on export to other nations by the USA and Western Europe firms which have been taken a part in co-operation and realized advanced technology transfer for industry. Thus, the expectation to cover the cost of production and development through export is seen as unfeasible after the completion of domestic military demand.

Governments will require new strategies to rise their arms export with a limited dependence on public finance and replace coproduction and licencing agreements with more captivating systems for buyers (Amara, 2008). Inadequacy of public funds obligates the supporting the capital influx to the defense industry from private sector and foreign companies. Customer requirements also constitute the priorities in production of arms for implementing the successful arms export. It is well known that small and medium sized establishments which tend to be both innovative and to concentrate on licensing with the larger firms to manufacture final products and supplying materials in defense industry.

3. THE PUSH FOR MILITARY EXPORT

The decision to export military equipments is of particular

importance and diplomacy plays a significant role rather than commerce governed decision making. Recently, political and economic considerations have been taken into account to reorganize indigenous arms capability for promoting to export weapons in developing nations. Generally, supply side factors rather than that of demand side have been found more successful contributor for export growth. On the other hand, increased levels of GDP and industrialization have also positive effects on sustainable export in developing nations, as is well known, due to results from econometric studies (Majeed and Ahmad, 2006). Export promotion can allow countries to produce defense goods competitively at lower prices. Eventually, industry provides revenue and employment in a changing degrees depend on level of export.

Financial competence or GDP is a key element to cover the military expenditure which is allocated to maintain the military services for establishing the defense capability of a nation (Kumar G, 2017). Besides GDP, improvements in balance of payment position of government's budget also provide additional funds for military expenses. Despite military expenditure is usually used as the indicator of military capability, it does not reflect many important situations which play significant role in military power such as defense industry, military infrastructure and organization. Alterations in real

exchange rate have no effect on defence export with sophisticated technology as in the manner for export of high technology products.

Foreign direct investment (FDI) inflows was found to have a negative effect on defense export as would be in export of higher technology. FDI activities in developing countries generally act on tertiary sector and retail trade and business operations. Consequently, a marked shifting of human capital which is required for defense industry may be observed (Zhang, 2007).

In developing countries, motivation of arms export has been shaped by economic conditions rather than political affairs. Many governments allocate so much resources to secure military items, as a result, lesser fundings is available for welfare projects including education and health care programs. The rise of GDP may promote governments to increase arms trade and the ratio of military expenditures to GDP augments over time. In the presence of military production which is above the domestic demand, arms export could begin in a varying degree and competes in arms race.

Annual spending for defense research and development activities which have a long-run upward trend could reflect enhancements in arms export capability. Apart from this, nations could also be improve defence programs by purchasing military equipments through international competitive market and military

outsourcing (Hartley, 2007). As usually, private companies in defence industry perform improvements due to changing requirements in armed forces by using newer technology at lower cost in the manners of competition. In addition to economic and political conditions for encouraging the fair competition, it is needed to create an environment for a greater participation of private industry which is capital intensive and has risks on investment.

The growing world-wide demand for sophisticated military equipments and higher national production capability contribute to elevate defense exports which reduce the dependence on foreign suppliers and cover the debts from increased defense imports. Apart from intensive competition in export market, US Government restrictions on transfer of military productions incorporating US technology will also serve to limit foreign sales. Since establishing and maintaining domestic defense industry has drained a significant portion of public resources, governments may be able to raise military exports by at least enough to afford defence imports and to lower financial burden of military production.

The significant increase in economic growth allows countries to contribute defense capabilities via distributing the more capital to the defence industry (Abdel-Halek et al., 2020.). It was found that GDP. was remarkable positive effects on military

expenditure which have negative impact on economic development (Rasyid, 2024). Governments in countries with higher GDP carry out substantial investments in defence industry and promote companies to procure military and nonmilitary equipments and services for armed forces. Increased GDP encourages governments to prioritize defence expenditure over the infrastructure investments (Ageli and Zaidan, 2012).

4. THE CASE OF TURKIYE

Turkish defense industry was mainly rearranged to provide long-standing sufficiency for covering national military needs and developing higher technology capability in 1980s. Defense Industry Agency conducts public policy related to domestic military establishments which incorporates private sector companies in a great scale. Turkiye also desires to develop ties between more increasingly among developing countries via arms trade in order to improve political solutions for regional conflicts and encourages private sector to perform export-driven production and co-operation with foreign partners to acquire skills, higher technology and investment without imposing external restrictions.

Co-production of F-16 aircraft (TAI and General Dynamics) and its engines (TEI and General Electric) have been driving force for creation

of Turkish aircraft manufacturing assembly in 1987 and have contributed higher technological capability and skilled human resource to support aerospace industry. Despite, the end of the cold war, Türkiye had difficulty to procure increased defence requirements due separatist internal threats and prolonged traction with Greece in the Aegean Sea during 1990s. USA and other Western allies refused to transfer military equipments, therefore, Türkiye has restructured defense sector to supply the needs of armed forces. It was also expected that investments in the defense industry would accelerate economic growth in line with export-driven military production. Initial public defense companies such as ASELSAN (Military Electronic Industry), TAI (Aviation and Space Industry), MKE (Infantry Guns, Artillery Weapons and, Ammunition Industry), TEI (Aviation Engines Industry), ROKETSAN (Rocket and Missile Industry), and ASFAT (Naval Shipyards) have been centre of the industry and realized successful platform-level productions such as F16 aircraft, T129 attack helicopter, Altay main battle tank, and Milgem battle ship. Until 2000s, Türkiye could not realized indigenization of defence industry owing to political and economic problems. Improved version of existing defence products has been developed and manufactured using domestic industry from the onset of 21th century. Measures have been taken to increase qualified

workforce in the industry and to provide export and coordination among the defense companies. Export revenues of Türkiye have increased over the years and expanded product range in military sector. Impressive progression in defense industry has been occurred with emphasize on raising capability of domestic production. Especially, drone technology has been advanced and TB2 (Bayraktar) used effectively in conflict areas of Northern Iraq, Syria, Libya, Karabakh of Azerbaijan and Ukraine. Significant share of defense export has been carried out to NATO countries including the United States, Czechia, Romania, Poland, Slovakia and Bulgaria. Recently, sales of unmanned combat aircrafts, aeroplanes, helicopters, armed land vehicles, and naval platforms have increased in a large degree. Due to impressive progression in military production and export, Türkiye has been evaluated as an “emerging supplier” in the global arms trade by SIPRI (Stockholm International Peace Research Institute) in 2020. (Sudreau et al, 2020).

Türkiye has maintained a long-standing policy related national defense manufacturing sector after 2001 in order to become one of the self confident countries. It has established a military industry which succeeded self sufficiency in a marked degree for domestic military requirements and realized a notable military export which might contribute to economic growth.

Aside from direct effect of defense export on economic development, Turkish defense industry reinforces the civilian sectors by raising the capacity of small scale industrial companies for manufacturing the military equipments and developing the new defense systems. Private companies in defense industry usually perform improvements due to changing requirements in armed forces by using newer technology at lower cost in the manner of competition. Türkiye also has linkages with foreign defence companies for co-operation in higher technology military production, especially in aeronautics and naval industries. Recently, industrial collaborations have been carried out such as TAI (Turkish Aerospace Industry) with Embraer (Brazilian Aerospace Industry) and Baykar (Turkish Drone Industry) with Leonardo (Italian Aerospace Industry) to establish joint production for civil and military aviation platforms. Military industry also enriches the country by generating highly skilled jobs and encouraging investments and courses to expel Turkish innovation into the international defence market. In the last two decades, Türkiye took place significant restructuring in the defense industry and encouraged the defense export activities in many arms platforms including unmanned combat aerial vehicles (TB2, Anka), attack helicopters (T129), general purpose helicopter (T625, T925), fighting aircrafts (Hürjet, Kaan),

main battle tanks (Altay, Tulpar), wheeled armoured personnel carriers (Kirpi, Vuran, Pars and Otokar), artillery systems (T55 Fırtına), infantry rifles (MPT76, KNT 76), frigates (İstif), corvettes (Milgem), attack submarines (Preveze), antiship rockets (Atmaca), submarine torpedoes (Akya), amphibic drone ships (Anadolu), engines for tank and armoured land platforms (Batu, Utku and Tuna), engines for drones (PD170, TF6000, TF10000), engines for helicopters (TS1400), aviation electronics (AESAs radar, Aselfir remote vision systems). Especially, US permission on sales of defense products merged from US technology has facilitated export in foreign markets as would be seen in export of T129 attack helicopter to Phillipines.

Defense export is needed to decrease the financial burden of Turkish defense industry. Türkiye has also been exporting their defence products abroad to cover the cost of imported arms and military equipments. Achievements in defense export also help subsidise defense import. Revenues from international arms trade has increased from 134 million US dollars in 2001 to 5500 million US dollars in 2023. Türkiye has a capability to provide equipment for national arms forces using domestic industrial facilities in situations of conflict with interrupted supply roads, potential restrictions from foreign arms suppliers and high priority requirements for weapons.

In 2024, Turkish defense industry has acquired a goal of 80% self reliance which was only 20% in 2001 by the means of government's defence export. Approximately, one-third of Turkiye's total defense export sales in 2023 were realized by Baykar, unmanned aerial vehicle manufacturer as \$ 1700 million. The heavy public involvement in the major defense investments such as Aselsan, TAI, Roketsan, MKE and ASFAT facilities the expansion of industry without financial difficulty. Attempts by domestic private companies to procure defence products have decreased government's budget to allocate for foreign purchases, particularly Baykar for combat drones, BMC and FNNS for armoured land platforms. Workers in Turkish defence industry has risen from 33000 in 2012 to an estimated 91000 in 2023 (SASAD,2023). Labour force comprise highly competent and specialized personnel who have difficulty to acquire jobs in the civilian industry.

In the last decade, defence industry indigenisation with export potential has been established to meet long-term military requirements, especially for high technology products which heavily depend on import from USA and Germany. The capability to equip Turkish armed forces with the means of domestic industry will play significant role in conflict situations where external supply lines for key components of sophisticated arms

systems may unpredictably may be disrupted. In this context, USA has restricted the sale of engine for the attack helicopter (T129) to Pakistan. Similarly Germany has blocked to transfer engine systems for the battle tank platform (Altay).

Turkiye has diversified the portfolio of defense export including armoured vehicles, unmanned combat drones, patrol vessels, warships, missiles and ammunition. Defense export have raised gradually from 19th largest exporter in 2010 with 634 million US\$ to 11th in 2023 with 5500 million US\$ (SIPRI,2023) as shown in Table 1.

5. DATASET AND METHODOLOGY

This study includes annual time series data of Turkiye between 2001 and 2023 (23 years).

AE: Annual arms export in million US dollar which is based on SIPRI data.

ME: Annual military expenditure in million US dollar which is based on SIPRI data.

GDP: Annual growth rate of gross domestic product in US dollar which is based on SIPRI data.

The economic model specification was expressed such that AE is a product of GDP. In the model, military expenditure was factored in as a control variable because it had nexus between arms export and GDP. Hence, the economic model is expressed thus;

$$AE_{t=\alpha+\beta}GDP + \delta_iME + \eta_t$$

In this study, natural logarithms of AE, GDP and ME can be used and can be derived as;

$$\ln AE_t = \alpha + \beta \ln GDP + \delta \ln ME + \eta_t$$

where μ is the random error term, α is the constant term; β and δ are the coefficients.

Firstly, stationary is examined using the Augmented Dickey Fuller (ADF) test and Phillips Perron (PP) test for all the time series variables. Then, the LM test and Heteroscedasticity tests are used for testing residual diagnostic properties

of the VAR (Vector Autoregression) model. We apply CUSUM (Cumulative Square Sum) test and CUSUM of square test to investigate the stability of the VAR model. Toda and Yamamoto procedure of Granger causality test is utilized to acquire the causality and direction of causality among the variables difference of coefficients from zero or not and the direction of causality. When k is the optimum lag length, d_{max} is the maximum integration order, and η is the White noise term. VAR model for estimation of AE, ME, and GDP variables for Toda and Yamamoto procedure can be written as follows

$$\ln AE_t = \alpha_1 + \sum_{i=1}^{k+d_{max}} \beta_{1i} \ln AE_{t-i} + \sum_{i=1}^{k+d_{max}} Y_{1i} \ln GDP_{t-i} + \sum_{i=1}^{k+d_{max}} \delta_{1i} \ln ME_{t-i} + \mu_{1t} \quad (1)$$

$$\ln GDP_t = \alpha_2 + \sum_{i=1}^{k+d_{max}} \beta_{2i} \ln AE_{t-i} + \sum_{i=1}^{k+d_{max}} Y_{2i} \ln GDP_{t-i} + \sum_{i=1}^{k+d_{max}} \delta_{2i} \ln ME_{t-i} + \mu_{2t} \quad (2)$$

$$\ln ME_t = \alpha_3 + \sum_{i=1}^{k+d_{max}} \beta_{3i} \ln AE_{t-i} + \sum_{i=1}^{k+d_{max}} Y_{3i} \ln GDP_{t-i} + \sum_{i=1}^{k+d_{max}} \delta_{3i} \ln ME_{t-i} + \mu_{3t} \quad (3)$$

Ho: $\beta_{1i} = 0$ (The null hypothesis is demonstrated that Arms export does not Granger cause neither GDP or ME). $H_1 = \beta_{1i} \neq 0$ (The alternative hypothesis means that AE Granger cause both GDP and ME. Hypotheses were examined by the Wald test using chi-square distribution with k degrees of freedom. Causal relationships among the other variables were studied in the same manner.

6. EMPIRICAL RESULTS AND DISCUSSION

The numbers in parenthesis show the P values which delineate rejection of null hypothesis and the series are stationary. Lag length for ADF test at the 1% is selected by Schwarz Information Criteria (SIC). Bandwidth for PP test is determined using the Newey-West method.

Concerning the results from PP Unit test presented on Table 2, LAE and LME are stationary in their first differences for equations with constant and trend at 1% significance level. Due to different results for stationary of LGDP, the maximum integration order is $d_{max} = 2$. Hence, 2 additional lag will be added to the VAR model. Optimum lag length is obtained $k=1$ for the VAR model to be calculated using various information criteria including AIC (Akaike Information Criterion), SC (Schwarz Information Criterion), and HQ (Hannon – Quin Information Criterion). Evaluated VAR model is stable and serially uncorrelated due to results from

LM (Lagrangde Multiplier) test. The probability value is 0.6006 and greater than 0.05 in VAR residual Heteroskedasticity test. Therefore, the calculated VAR model is free from Heteroskedasticity. CUSUM (Cumulative Sum) and CUSUMSQ (Cumulative Square Sum) statistics outline the significance level for the calculated coefficients of the VAR model as a 5%. Hence, estimated coefficients are accepted to be stable.

In Toda Yamamoto causality analysis, unidirectional relationship between the GDP and defense export was found (Table 3). Nevertheless, similar causal link between military expenditure and GDP was observed. The empirical results depict that annual growth rate positively affects the arms export in Turkiye over long-run. Military expenditures have positive effects on GDP. These results are consistent with the theoretical data in literature.

Most of the developing countries have to militarize for stabilizing the internal conflicts and external threats despite negative fiscal consequences in long-run. Significant increases in defense expenditure with excessive import cause external debt burden and worsen national economies with more borrowing (Azam and Feng, 2017). National security systems greatly depend on technological capability and production of domestic defense companies which are mostly supported by governments' funds. State embracement usually seems to exist in major defence firms which manufacture main weapon

systems in order to survive and remain competitive unlike the civil industries. Governments both foster the growth of domestic companies and survive the dominant role in the sector as the major purchaser of military products. Several countries without self-reliant indigenous defense industry prefer mainly production under license or through offset-led programmes.

A well-constructed and competent defense industry not only contributes national security but also facilitates the development of higher technology in civil industry. In the last decade, a remarkable amount of funds has been allocated for investment in development and procurement of new original high-tech defense products. For this reason, the Turkish defense industry has enlarged markedly and realized revenues to a great degree. Especially, small national defense firms which produce subsystems perform advantageous operations out of the country with global defense firms and continue to be profitable.

Ideas differ on the appropriate level of defense expenditure in a stated nation and on what encourages countries to military export. Desire for military expenditure and export might be shaped mainly by financial considerations. Military expenses in developed countries have a stable course in their GDP, while on the contrary, developing countries spend a significant portion of GDP on the defense expenditure (Hewitt, 1991).

International cooperation in the defense sector facilitates foreign direct investment, joint venture, arms export and transfer of military technology in the defense industry. Today, many countries have encouraged the defense industries to work in a more transnational manner for accessing foreign markets and facilitating inward investments. Thus, globalized defense supplier firms lose over the flow of major technologies and their dominant role in policy of the defense industry (Hayward, 2000). As a characteristic feature, companies in the defense sector are subject to limitations on the nature of arms production and their technology transfer by governments in contrast to other industries based on free markets. Environment for the defense industry appears to be unforeseeable with descending national defense expenditure. The defense sector must perform intensively to export abroad in order to constrain problems such as increased financial burden of arms import, reduction in domestic military budgets, and raised international competition. Since establishing and maintaining domestic defense industry has drained a significant portion of public resources, governments may be able to raise military exports by at least enough to afford. Increased indigenous production with well-supported research and development establishments and promoting export strategy will achieve desired targets in the economic base of the defense industry. A healthy defense sector

with a strong domestic production capability provides positive effects on economic growth through elevating the demand and employment in the long run (Mohanty, 2020). Increased investments due to raised demand instigates new job access and augments purchasing power and development (DeGrasse, 1983)

We observed that the rise in GDP has pushed the arms export due to well established defence industry in Turkiye. Military expenditures have also increased GDP in a stable course between 2000 and 2023 under the light of results from Toda Yamamoto Granger causality test. The long-term needs for national security in future will encourage ensuring the strong defence industry with export potential. It is assumed desirous defense industry that holds mainly the manufacturing fighter aircrafts, upgraded main battle tanks, antiwarship programs, unmanned combat air vehicles, armoured land platforms, ammunition and electronic military devices which have comprised the great part of defense export.

Turkiye is one of the emerging defense supplier countries including Israel, South Korea, Saudi Arabia, UAE, Brazil and have 5 firms among Top 100 World's largest defense supplier firms for 2025 in accordance with Spade Defense Index and the International Institute for Strategic Studies. As a result of our study, we suggest that creative defense expenditure may have positive effects on military export in the presence of integrated military industry with innovative technologies, skilled labour force and economic growth. Turkiye which provides weaponry platforms at low cost in a short time period can enhance defense export in competitive international market due to its self reliant defense industry.

Conclusively, future research directions should focus on the role of higher technology for development of sophisticated arms used in aerospace, land and naval platforms such as engine for fighter jet, long range antiballistic missile and military electronics.

Table 1 shows arms export, military expenditure and GDP in Turkiye between 2001-2023 (SIPRI)

YEARS	Arms Export (Current million US Dollars)	Military Expenditure (Current million US Dollars)	GDP (Current million US Dollars)
2001	134	7216,1	201.753123806
2002	248	9050,4	240.249071871
2003	331	10277,9	314.595572145

YEARS	Arms Export (Current million US Dollars)	Military Expenditure (Current million US Dollars)	GDP (Current million US Dollars)
2004	196	10920,8	408.865430220
2005	337	12081,2	506.314717661
2006	352	13036,5	557.076157773
2007	420	14987,8	681.321124295
2008	576	16809,6	770.449132861
2009	670	16047,5	649.289324627
2010	634	17650,5	776.967266305
2011	817	17006,5	838.785289694
2012	1200	17694,3	880.555885492
2013	1390	18427,6	957.799120008
2014	1647	17576,5	938.934609296
2015	1655	15668,8	864.314810469
2016	1678	17827,7	869.683881593
2017	1739	17822,7	858.988849285
2018	2035	19648,7	778.972199727
2019	2741	20436,9	761.005946788
2020	2279	17478,4	720.338498174
2021	3325	15567,4	819.865253669
2022	4396	10779,9	907.118435952
2023	5500	15827,9	1108.022373259

Table 2 Results of Unit root test

Variables	At levels		At 1st Difference	
	ADF	PP	ADF	PP
InAE	0.0144	0.144	0.0002	0.0000
	(-4.2645)	(-4.2645)	(-6.3474)	(-8.2870)
InME	0.3842	0.3981	0.0019	0.0022

	(-2.3680)	(-2.3490)	(-5.2771)	(-5.2228)
InGDP	0.2276	0.2276	0.2047	0.2186
	(-2.7519)	(-2.7519)	(-2.8239)	(-2.7804)

Table 3 Toda Yamamoto Causality (Block Exogeneity Wald) test results

Null Hypothesis	Chi-sq	Prob	Direction of Causality
GDP does not cause AE	47.966	0.0285	GDP → AE
ME does not cause AE	0.4903	0.4838	No Causality
AE does not cause GDP	0.0181	0.8229	No Causality
ME does not cause GDP	45.270	0.0334	ME → GDP
AE does not cause ME	0.6105	0.4346	No Causality
GDP does not cause ME	0.1403	0.7079	No Causality

REFERENCES

- [1] Abdel-Khalek G, Mazloum MG, El Zeiny MRM (2020). Military expenditure and economic growth: The Case of India. *Review of Economics and Political Sciences*. 5(2), 116-135.
- [2] Ageli MM, Zaidan SM. (2012). *Consequential effects of defence expenditure on economic growth of Saudi Arabia*. 1970-2012, 5(2), 155-163.
- [3] Amara J. (2008). Military industrialization and economic development. Jordan's defense industry. *Review of Financial Economics*. 17, 130-145.
- [4] Azam M, Feng YI (2017). Does military expenditure increase external debt? Evidence from Asia. *Defence and Peace Economics*. 28, 5, 550-567. <https://doi.org/10.1080/10242694.2015.1072371>.
- [5] Barros CP, and Sandler T, (eds) (2003). Internal and external threats: Defence economic analysis. *Defence and Peace Economics*. Special Issue, 146(6), 385-474.
- [6] Beraud – Sudreau, Lucie. (2019). Building Franco-German Consensus on Arms Export. *Survival*, 61(4), 79-98.
- [7] Blum J. (2019). Arms production, national defense spending and arms trade: Examining supply and demand. *European Journal of Political Economy*. 60 (12), 1-6.
- [8] Butler C, Kenny B, Anchor J (2000). Strategic alliances in the European defence industry. *European Business Review*. 12(6), 308-321.
- [9] Brender A. (2018). Government Ideology and Arms Exports. *ILE Working Paper Series*, 21
- [10] University of Hamburg, Institute of Law and Economics (ILE), Hamburg.
- [11] Camola M. (2012). Democracies, Politics and Arms Supply. *Review of the International Economics*. 20(1), 150-163, doi: 10.1111/j.1467-9396.2011.01014.x.
- [12] DeGrasse RW. (1983). Military expansion, economic decline: The impact of military spending on US economic performance. New York, USA: Routledge.
- [13] Dudzeviciute V, Cesnvyte D, Prakapienė D. (2021) Defence expenditure - government debt nexus in. The context of sustainability

- in selected small European Union countries. *Sustainability*. 13(12).
- [14] Dunne JP, Smith RP, Willenbockel D. (2006). Models of military expenditure and growth : A Critical Review. *Defence and Peace Economics*. 16(5), 449-46.
- [15] Hartley K. (2012). Conflict and Defence Output : An Economic Perspective, *Revue D'economie Politique*. 122(2), 171-195.
- [16] Hartley K. (2007). Defence economics: Achievements and challenges. *The Economics of Peace and Security Journal*. 2 (1); 45-60..doi : 10.15355/2.1.45.
- [17] Hayward K. (2000) The Globalisation of Defense Industries *Survival*, 42(2), 1-13.
- [18] Hewitt DP. (1991). What Determines Military Expenditures? *Finance & Development*, December 22-25.
- [19] Karagol E. (2005). Defence expenditures and external debt in Turkey. *Def Peace Econ*. 16 (2), 117-125.
- [20] Kinsella David. (2011). The Arms Trade, *The Handbook of Political Economy of War*, edited by Christopher J, Coyne and Rachel L, Mothers, Cheltenham, UK: Edward Elgar.
- [21] Kollias C, Manolas G, Paleologour SM. (2004). Military expenditure and government debt in Greece: Some preliminary empirical finding. *Def. Peace Econ*. 15 (2), 189-197.
- [22] Korkmaz S. (2015) The effect of military spending on economic growth and unemployment in Mediterranean countries. *Int J Econ Financ Issues*. 5(1), 273-280.
- [23] Krause Keith. (1992). Arms and the State: The Patterns of Military Production and Trade. New York: Cambridge University Press.
- [24] Kumar G. (2017). Countries Military Expenditures: Definitions and Determinants. *Economic Affairs*. 62(4), 647-654. <https://doi.org/10.5958/0976-4666.2017.00078.X>
- [25] Majeed MT, Ahmad E. (2006). Determinants of export in developing countries. *The Pakistan Development Review*. 45(4) ; 1265-1276.
- [26] Masoud AK, Zaleha MN. (2015). Military expenditure and economic growth in developing countries. Evidence from system GMM estimates. *J Emerg Trends Econ Manag Sci*. 6(1), 31-3.
- [27] Some preliminary empirical findings. *Def. Peace Econ*. 15(2), 189-197.
- [28] Mohanty RK, Panda S, Bhuyan B (2020). Does defence spending and its composition affect economic growth in India. *The Journal of Applied Economic Research*. 14(1). 62-85.
- [29] Rasyid MG. (2024). The nexus between GDP and military expenditure in Indonesia: Evidence from Time series Analysis. *Jurnal Pertahanan*. 10(1), 1-15.
- [30] SASAD (Turkish Defence and Aviation Industry Association) *Annual Activity Report*. 2023. <https://www.sasad.org.tr/etiket/savunma-sanayi-raporu>.
- [31] Sezgin S, Yıldırım J. (2002). The demand for Turkish military expenditure. *Defence and Peace Economics*. 13(2), 121-128.
- [32] SIPRI (2023). [https:// sipri.org/databases/milex](https://sipri.org/databases/milex)
- [33] Sudreau LB, Da Silva DP, Kuimova A, Wezeman PD (2020). Emerging suppliers in the global arms Trade. SIPRI, *Insights on Peace and Security no. 2020(13)*, December.
- [34] Yakovlev P. (2007). Arms trade, military spending, and economic growth. *Defence and Peace Economics*. 18(4), 317-338.
- [35] Zhang KH. (2007). International production networks and export performance in developing countries. Evidence from China. *The Chinese Economy*, 40:83-96. doi: 10.2753/CES1097-1475400605.

SOLUTION OF TASK OPTIMAL PLANNING OF AIR DEFENSE MEANS AGAINST LOW-ALTITUDE AIR TARGETS

Arzuman G. GASANOV

Military Research Institute of National Defense University,
Baku, Azerbaijan

The article examines the methods of their destruction by air defense systems, taking into account the low-altitude operation of various types of air attack weapons fighter airplane, helicopter, cruise missile, reconnaissance unmanned aerial vehicles and armed unmanned aerial vehicles. For this purpose, taking into account the tactical and technical characteristics of low-altitude air attack weapons, efficiency coefficients were determined using methods of destruction by specially selected anti-aircraft missile systems. To solve the problem S-125 2TM, BUK-MB, BARAK-8, S-300 PMU2, TOR-M2KM, PATRIOT MIM-104, PANSIR S-1, NASAMS-III against low-altitude air attack weapons such as fighter airplane, helicopter, cruise missile, reconnaissance unmanned aerial vehicles and armed unmanned aerial vehicles by applying the method Gomori modified variant of the Simplex method is solved. As a result, it was possible to determine the maximum and minimum number of destroyed low-altitude air targets. Maximum 86 % and minimum 78 % of air targets operating at low altitude of this conventional enemy. These results can be used in optimal planning of the use of air defense systems against air attack systems operating at low altitude during combat operations.

Key words: *Unmanned aerial vehicle, air attack weapons, air defense system, radar station, anti-aircraft missile system, mathematical modeling, optimal control.*

1. INTRODUCTION

Low altitude activity on air targets showing air defense optimal planning of resources a little on the topic an important factor to consider

is to buy. This is planning in progress both technical, both too much operation to the next in its aspects special attention necessary:

Radar placement; weapon

choice; C3 systems (command, control and communications); education and tactical analysis; an enemy tactics analysis.

Create an optimal air defense system and at low altitude activity on air targets showing more effective against events key to see directions.

Low altitude activity on air targets showing against optimal planning of anti-aircraft missiles numerous factors demand attention does military strategy and taking into account technological developments being taken anti-aircraft missile systems effective use at low altitude activity on air targets showing against protection strengthens. At present, the current issue is the optimal planning of detection and destruction of air attack weapons operating at low altitudes by air defense systems.

1.1. Potentials of the low-altitude air attack vehicles

Low altitude activity demonstration of air attack vehicles the potential is vast and many similar platforms military in operations can be effective. These tools different types of technologies, speed and maneuver capabilities with special used to carry out missions. Below are the types potential opportunities and advantages of air attack:

Hide from the radar and less visibility; high maneuver ability;

high act stupidity; fast raid attacks; don't be an enemy protection positions penetration depth; small size targets and your enemy target systems confusion; small tools; deception measures; in mixed weather conditions operation skill; modular weapons options; precision attack capabilities; intelligence and joint strike capabilities usage; drones and unmanned aerial vehicles; cruise missiles; hypersonic missiles; stealth technology with equipped aircraft; with ammunition equipped artificial satellites.

These satellites attack ground and air targets from space will know they have the ability. technological developments are artificial. satellites high from above different type targets increases the possibility of accurate shooting. These systems modern in wars big advantages provided does and air attack vehicles increase effective attack capabilities.

1.2. Potentials of the air defense protection

The potential capabilities of air defense in modern warfare are also enormous and have been developed to provide effective protection against various threats. Some examples of such capabilities are as follows:

Mobile and flexible defense systems; radar and detection technologies; defense against

hypersonic targets; drone defense; laser technologies; electronic warfare system; anti-missile defense systems; anti-aircraft missile defense; enhanced drone control.

These vehicles have high potential capabilities in the field of air defense and are designed to provide effective protection against modern air threats.

In modern warfare, the use of low-altitude air defense is crucial due to the dynamic and multifaceted nature of conflicts. The effectiveness of these tools depends on many factors in strategic and tactical aspects. Modern air defense systems use advanced radar technology to detect low-altitude targets. These radars benefit from phased array radars designed to track and evaluate multiple targets. Artificial intelligence and machine learning algorithms to speed up target analysis and is used to refine the target selection. It is the more efficient of the systems. work provided does.

Modern Air defense in wars systems usually with each other integrated. These are systems together work and to goals provide broader protection against makes low altitude air defense systems, various integration at levels (strategy, tactics). complementing each other. High, medium and low height protection measures, a wide range of air defense

systems creates a network.

Real time information exchange, various weather protection synchronization between components and coordination provided makes Various means of protection from bad weather systems together operation, effective air attacks by the enemy on the way allows you to avoid.

Mobile air defense systems, quickly in the combat zone positions change ability comes to the fore with This is a more flexible response to enemy air attacks. give opportunity knows.

The main difference between air attack targets and other types of targets is that their detection is a complex task. In modern warfare, low-altitude air defense systems are constantly being improved to become more effective in the complex conditions of air warfare. The development of these systems helps maintain air superiority in modern warfare and improve the safety of allied forces[1-6].

2. METHODOLOGY OF THEORETICAL STUDING

Let us assume that according to statistics from previous years, N a certain number of low-altitude attack aircraft were used during combat operations over a certain period. According to certain characteristics

of these air attack targets, m_1 numbers type of the H_1 , m_2 numbers the of type H_2 , etc. m_n numbers type of the H_n to separate is possible. Then according to the condition

$$m_1 + m_2 + \dots + m_n = N \quad (1)$$

the probability or proportion of a particular type of air attack among low-altitude air attacks .

$$P_j = \frac{m_j}{N}, \quad j = 1, 2, \dots, n \quad (2)$$

can be calculated using the formula.

Let us assume that there are m species ME_1, ME_2, \dots, ME_m the matrix elements characterizing the use of a_{ij} air defense against a j -type

air attack target are given (table 1). H_j it is necessary to provide recommendations that ensure an optimal solution during combat operations when determining air attack targets and planning the destruction of the maximum number[7-9].

Therefore, it is necessary to study in advance the possibilities of using air defense against air attack targets operating at low altitude. It is important to provide recommendations on the effective selection of air defense means that ensure the optimal solution to the combat task of detecting, neutralizing and destroying air attack targets operating at low altitude.

Table 1 Effectiveness coefficients of weapons by targets

№	Air defense equipment	Type of targets					
		H_1	H_2	...	H_j	...	H_n
1	ME_1	a_{11}	a_{12}	...	a_{1j}	a_{1n}
2	ME_2	a_{21}	a_{22}	...	a_{2j}	a_{2n}
...
i	ME_i	a_{i1}	a_{i2}	...	a_{ij}	a_{in}
...
m	ME_m	a_{m1}	a_{m2}	...	a_{mj}	a_{mn}

Let us assume that mM different air defense systems can be used in combat operations against N low-altitude air attack targets. n to solve the problem of hitting the target, we introduce the following quantities:

x_{ij} - the number of uses of weapons i of the type ME_i against low-altitude air targets j of the type H_j

p_{ij} - coefficients of the effectiveness i -th type of ME_i air defense against air targets operating at low altitude j -th type of H_j .

$p_{ij} x_{ij}$ - average number of destroyed targets that can be by using air defense i -th type of ME_i the against low-altitude air targets the j -th type of H_j .

If all M different means of destruction $ME_i, i=1,2,\dots,m$ are used during combat operations against N number of low-altitude air attack vehicles $H_j, j=1,2,\dots,n$, then the average number of air targets that can be destroyed

$$MH(x) = \sum_{i=1}^m \sum_{j=1}^n p_{ij} x_{ij} \quad (5)$$

here x - a matrix of m rows and n columns, composed of $x_{ij}, i=1,2,\dots,m$ and $j=1,2,\dots,n$ values, the function $MH(x)$ - the average number of air targets that can be destroyed during combat operations using m this type of air defense n against air attack targets operating at low altitude.

This is the objective function of the solution to the problem. Then it is necessary to find such an optimal option that destroys the maximum number of targets. In addition, it would be interesting to destroy the minimum number of targets in the most unfavorable situation. The mathematical model of the problem within the given combat capabilities looks like this:

The objective function

$$MH(x) = \sum_{i=1}^m \sum_{j=1}^n p_{ij} x_{ij} \rightarrow \max(\min) \quad (6)$$

Conditions of limitation

$$\sum_{j=1}^n x_{ij} = a_i, \quad i = 1, 2, \dots, m \quad (7)$$

$$\sum_{i=1}^m x_{ij} = b_j, \quad j = 1, 2, \dots, n \quad (8)$$

$$x_{ij} \geq 0 \quad (9)$$

here a_i - the number of means of destruction of the i -type, (7) - use of conventional weapons ME_i of destruction of the i -type against all low-altitude air attack targets, b_j - the number of targets of the j -th type, -(8) conditional- application of all air defense means to the air target j type.

Let's assume that

$$p_{ij}, \quad i = 1, 2, \dots, m; \quad j = 1, 2, \dots, n$$

the values of their quantity, a_i - the number of air defense systems and b_j targets is indicated. Based on these data, problems (6) - (9) can be solved using the Gomori method [10, 11]

which is a modified version of the Simplex method. with the "Minimize" and "Maximize" functions of the Mathcad program[12]

$$x_{ij}, i = 1, 2, \dots, m; j = 1, 2, \dots, n$$

we will find the values of their quantities and $MH(X)$ functions. That is, the smallest and largest values of the number of destroyed targets are known.

3. APPLICATION

Let's assume that low-altitude fighter airplanes, helicopters, cruise missiles, reconnaissance unmanned aerial vehicles and armed unmanned aerial vehicles, and air strikes against them S-125 2TM, BUK-MB, Barak-8, S-300 PMU2, TOR M2KM, PATRIOT, PANSIR S-1 and NASAMS-III [2-6] the efficiency coefficients of the means of destruction are given in table 2.

Table 2 The coefficients of effectiveness of specially selected air defense against low-altitude air attack targets are given conditionally

№	Air attack Protection means	Low altitude targets				
		Fighter airplane	Helicopter	Winged rocket	Reconnaissance unmanned aerial vehicle	Armed unmanned aerial vehicle
1	S-125 2TM	0.652	0.853	0.454	0.801	0.791
2	BUK-MB	0.711	0.891	0.651	0.871	0.852
3	BARAK-8	0.971	0.981	0.956	0.972	0.981
4	S-300 PMU2	0.892	0.952	0.882	0.982	0.973
5	TOR M2KM	0.731	0.752	0.721	0.861	0.853
6	PATRIOT MIM-104	0.724	0.854	0.681	0.843	0.834
7	PANSIRA S-1	0.704	0.784	0.684	0.754	0.734
8	NASAMS-III	0.784	0.879	0.769	0.849	0.839

According to generally accepted data, the enemy currently has fighter airplanes, helicopters, cruise missiles, reconnaissance unmanned aerial vehicles, armed unmanned aerial vehicles available. Enemy conventional fighter airplanes, helicopters, cruise missiles, reconnaissance in modern operations in the case of the use of reconnaissance unmanned aerial vehicles, armed unmanned aerial vehicles, it is necessary to plan the combat operations of air defense systems in advance.

Let's assume that the conventional enemy's fighter airplanes, helicopter, cruise missile, reconnaissance unmanned aerial vehicles and armed unmanned aerial vehicles against air targets S-125 2TM, BUK-MB, BARAK-8, S-300 PMU2, TOR-M2KM, PATRIOT MIM-104, PANSIR S-1, NASAMS-III have anti-aircraft defenses such as anti-aircraft missile systems.

Using the data in table 2 and the conventional enemy the number of fighter airplanes - 87, helicopters - 46, cruise missiles - 95, reconnaissance unmanned aerial vehicles - 76, armed unmanned aerial vehicles - 88.

We will calculate the probabilities or shares of an air attack by a fighter airplane, helicopter, cruise missile, reconnaissance unmanned aerial

vehicles and armed unmanned aerial vehicles using formulas (1) and (2):

The probability or proportion of the fighter airplane appearing $p_{qt} = \frac{87}{392} = 0.222$, the probability or proportion of the helicopter appearance $p_v = \frac{46}{392} = 0.117$, the probability or proportion of the cruise missile appearing, $p_{qr} = \frac{95}{392} = 0.242$ the probability or proportion of the reconnaissance unmanned aerial vehicles appearance $p_{kpua} = \frac{76}{392} = 0.194$ the probability or proportion of the an armed unmanned aerial vehicles appearing $p_{spua} = \frac{88}{392} = 0.224$.

Thus, according to the calculated values, it can be said that air attack targets of cruise missiles and armed drones are more expected targets. Air defense against low-altitude air attack targets can be defined as follows:

S-125 2TM $4*3*4=$ with 48 missiles against 24 targets; BUK-MB $5*6*4=$ with 120 missiles against 80 targets; Barak-8 $2*4*8=$ with 64 missiles against 64 targets; S 300 PMU2 $3*4*4=$ with 48 missiles against 48 targets; TOR M2KM $4*4=$ with 16 missiles against 64 targets; PATRIOT MIM-104 $4*4*4=$ with 64 missiles against 64 targets; PANSIR S-1 $7*12=$ with 84 missiles against 42 targets; NASAMS-III armed with $3*3*6=54$ missiles against 54 targets, the means of destruction thus applied and the

total number of missiles is 498, the number of targets is 392.

Then for the solution combat use the air defense systems (498) against the air attack targets (392) apply the Gomori method [10, 11], which is a modified version of the Simplex method, for a conventional combat kit the task (6) - (9) for dates in table 3 can be solved. For this purpose, we use the Maximize() and Minimize() functions in the Mathcad program, we will get the following results [12]:

$$x_{1,2} = 24, x_{2,2} = 22, x_{2,4} = 58, x_{3,3} = 64, x_{4,3} = 22, x_{4,4} = 18, \\ x_{4,5} = 8, x_{5,5} = 16, x_{6,5} = 64, x_{7,1} = 42, x_{8,1} = 45$$

the number of deployed air defense systems for the maximum number of air attack targets.

That is, S-125 2TM with 48 missiles against helicopters; BUK-MB with 34 missiles against helicopters, 86 missiles against reconnaissance drones; 64 Barak-8 missiles against cruise missiles; S-300 PMU2 with 22 missiles against cruise missiles, with 18 missiles reconnaissance unmanned aerial vehicles and armed with 8 missiles unmanned aerial vehicles; TOR M2KM with 16 missiles against armed unmanned aerial vehicles; PATRIOT with missiles 64 against armed unmanned aerial vehicles; PANSIR S-1 with 84 missiles against fighter airplanes; NASAMS-III with 45 missiles against fighter airplane the means of destruction thus applied and the maximum number of air attack targets destroyed. $MH(x) \approx 335$. This is probably 86% of the technical potential of low-altitude air targets. A minimum number of low-altitude airstrikes are used to hit targets

$$x_{1,3} = 24, x_{2,1} = 9, x_{2,3} = 71, x_{3,4} = 64, x_{4,1} = 14, x_{4,2} = 30, \\ x_{4,4} = 4, x_{5,2} = 16, x_{6,1} = 64, x_{7,5} = 42, x_{8,4} = 8, x_{8,5} = 46$$

the number of weapons used.

That is, S-125 2TM 48 with missiles against cruise missiles; BUK-MB with 14 missiles against fighter airplanes and with 106 missiles against cruise missiles; BARAK-8 with 64 missiles for reconnaissance unmanned aerial vehicles; S-300 PMU2 with missiles against fighter airplanes, with 30 missile against helicopters and with 4 missile reconnaissance unmanned aerial vehicles; TOR-M2KM with 16 missiles against helicopters; PATRIOT MIM -104 with 64 missiles against fighter airplanes; PANSIR S-1 with 84

missiles against armed unmanned aerial vehicles; NASAMS-III with 8 missiles against reconnaissance unmanned aerial vehicles and with 46 missiles against armed unmanned aerial vehicles against is the number of the means applied. As well as a minimum number of destroyed air targets $MH(x) \approx 305$. This is probably 78% of the technical potential of low-altitude air targets.

4. SUMMARY

In large-scale operations during combat operations, an air strike against a simulated enemy at low altitudes is carried out by means of fighter airplane aircraft, helicopters, cruise missiles, and reconnaissance. The probabilities of drones, armed drones, unmanned aerial vehicles, and kamikaze aerial targets participating in a combat zone are 0.222, 0.117, 0.242, 0.194, 0.224 respectively.

S-125 2TM, BUK-MB, BARAK-8, S-300 PMU2, TOR-M2KM, PATRIOT MIM-104, PANSIR S-1 and NASAMS-III the maximum number of low-altitude air targets destroyed when using anti-aircraft missile systems against low-altitude air attack systems can be 325, the minimum 305. This is a maximum of 86% and a minimum of 78% of the technical potential of air targets operating at low altitude.

REFERENCES

- [1] Su-25 attack aircraft in the Second Karabakh War. (January 08, 2021).: [Electronic resource] / *anna-news. information*. URL: HYPERLINK "https://anna-news.info/shturmoviki-su-25-na-vtoroj-karabahskoj-vojne/" https://anna-news.info/shturmoviki-su-25-na-vtoroj-karabahskoj-vojne/
- [2] "Shahed Heads 129 Iranian Armed UAV Force". *Aviation & Space Week*. Accessed. (July 26, 2022) .: [Electronic resource] https://aviationweek.com/defense/shahed-129-heads-irans-armed-uav-force .
- [3] Makarenko S.I. (2020). Opposition drone devices / *Saint Petersburg: Science-intensive technologies*, - 204 p.
- [4] "Osa": history of creation, description and technical characteristics. (April 29, 2019). : // *MilitaryArms.ru* [Electronic resource]. URL: https://militaryarms.ru/voennaya-technika/boevye-mashiny/zrk-osa/
- [5] Tuchkov V. (06 October 2020). Yerevan has already lost the air phase of the battle for Karabakh.: // *Free press* [Electronic resource]. URL: https://svpressa.ru/war21/article/277832/
- [6] Parsch, andreas. Raytheon MIM-104 Patriot. *U.S. Military Rockets and Rockets catalog*. (September 27, 2014).: [Electronic resource] https://web.archive.org/web/20150411014329/ http: // www.oboznachenie-systems.net/

- dusrm/m-104.html
- [7] Arzuman Gasanov, Yashar Kerimov. (2023). Study of the possibilities of using drones at the operational-tactical level. *Scientific-practical Journal of National Security and Military Sciences*, –Baku, No. 3 (9), pp. 40-46.
- [8] Samarsky, A.A. (2005). Mathematical modeling. Ideas. Methods. Examples. - 2nd edition., former. / A. A. Samarsky, A. P. Mikhailov, Moscow: Fizmatlit, - 320 p.
- [9] Arzuman Gardashkhan oglu Gasanov, Yashar Shukur oglu Karimov. (2024). Methodology for effective planning of means of destruction located in the cover and in the stern for various types of targets. *Voenen Zhurnal, Sofia, Bulgari.*, Volume 131, Issue 2, pp. 207-213.
- [10] Arzuman Gardashkhan oglu Gasanov, Yashar Shukur oglu Karimov. (2023). Optimal management of the application of a group of unmanned aerial vehicles (UAVs) of the same type to different targets. *Journal of Defense Resources Management*, Brasov – Romania, vol. 14, issue 2 (27), pp.125-130.
- [11] Arzuman G. Gasanov. (2018). Solving problems of mathematical modeling of military systems. *Study guides. - Baku: Military Publishing House*, -120 p.
- [12] Mathcad. (2025).: [Electronic resource] / Wikipedia - the free encyclopedia / URL: <https://en.wikipedia.org/wiki/Mathcad>.

BLUE ECONOMY, MARITIME RESILIENCE, AND A SYMBOL OF SOVEREIGNTY: AN INTEGRATIVE STUDY OF BERHALA ISLAND AS A STRATEGIC DEFENCE POINT

SUSILAWATI, SUTANTO, Adnan MADJID,

Totok Imam SANTOSO*

Republic of Indonesia Defense University, Jakarta, Indonesia

This study explores the strategic, economic, and symbolic significance of Berhala Island, a small Indonesian island located near the maritime boundary with Malaysia. Through a qualitative, document-based approach, the research investigates how outer islands like Berhala can serve as dual-purpose assets, functioning as both forward defence outposts and nodes of blue economy development. Drawing from secondary data sources including government policy documents, marine spatial plans, and scholarly literature, the study analyses Berhala's role in maritime surveillance, its potential to support coastal livelihoods, and its representation as a symbol of national sovereignty. Findings reveal that Berhala Island embodies an integrative model where defence, economic development, and symbolic presence intersect. The study concludes with policy recommendations, including the development of dual-use infrastructure, the integration of blue economy principles into national defence doctrine, and the positioning of Berhala Island as a governance model for managing Indonesia's outermost islands sustainably and strategically.

Key words: Blue economy, maritime security, strategic islands, sovereignty, intersectoral governance

1. INTRODUCTION

In recent years, the strategic relevance of small islands has grown significantly within the broader framework of maritime defence

and territorial resilience. Situated at the edges of national jurisdictions, small islands often serve not only as geospatial anchors for maritime sovereignty but also as forward defence outposts, economic nodes,

and cultural symbols of state presence (Marcão et al., 2025). In the case of Indonesia, a vast archipelagic state with over 17,000 islands, the role of outermost islands has become increasingly critical amid rising geopolitical tensions in the Indo-Pacific.

As global defence paradigms shift from traditional, military-centric approaches to more multidimensional strategies, concepts like the *blue economy* have emerged as integrative solutions. This paradigm envisions sustainable economic development based on ocean resources, coupled with ecological protection and regional security (Voyer et al., 2021). The blue economy is no longer just a matter of economic policy; it is rapidly becoming a key component of national resilience and defence planning (Patil et al., 2016).

Maritime zones that once were viewed purely as defence perimeters are now being reframed as opportunities for socio-economic integration and strategic diplomacy.

Berhala Island, located near the maritime boundary between Indonesia and Malaysia, exemplifies such a dual-role territory. With its proximity to major maritime routes and its contested history, the island holds both strategic and symbolic significance. It functions not only

as a potential military watchpoint but also as a sheltering area for local fishermen, revealing its multifaceted value across defence, livelihood, and diplomacy dimensions.

This research seeks to answer the following guiding questions:

1. How can Berhala Island contribute to Indonesia's national defence through blue economy strategies?
2. In what ways does territorial symbolism strengthen state sovereignty in the context of outer islands?
3. How can intersectoral and integrated policy frameworks be designed to manage such strategic maritime zones effectively?

Through a qualitative, document-based approach, this study aims to offer insights into how Indonesia can align economic development, sovereignty assertion, and maritime defence in managing its small, strategic islands.

2. THEORETICAL AND CONCEPTUAL FRAMEWORK

The multifaceted nature of maritime defence in the 21st century necessitates a paradigm shift from conventional military doctrines toward more integrated, interdisciplinary frameworks. This

study draws upon five interrelated theoretical pillars to understand the strategic relevance of Berhala Island within the context of national defence, economic policy, and symbolic sovereignty.

First, the concept of the *blue economy* offers an expanded understanding of ocean-based development beyond resource extraction. It incorporates sustainability, security, and equitable growth as core principles (Voyer et al., 2021). Institutions such as the FAO, UNCTAD, and the World Bank have emphasized the role of the blue economy in enhancing resilience for coastal and island communities, particularly in developing nations. Within a defence context, the blue economy creates dual-use frameworks, supporting both economic productivity and strategic presence in remote maritime zones (Patil et al., 2016).

Second, *maritime resilience* is emerging as a non-conventional defence strategy that integrates civilian infrastructure, environmental stewardship, and localized economic systems into broader national security doctrines. Resilience emphasizes the capacity of maritime communities and institutions to absorb, adapt to, and recover from disruptions, be they ecological, economic, or geopolitical

(Pomeroy et al., 2019). This aligns with Indonesia's need to strengthen its outermost islands not only through military installations but also through community-based initiatives and sustainable development.

Third, the study incorporates *territoriality and identity theory* to understand how geography becomes a symbol of sovereignty. Territoriality is not merely about control of space, but also about its representation in national consciousness (Miller, 2018). The visibility of a state in remote zones, such as the deployment of flags, military posts, or civilian settlements, functions as a performative act of sovereignty, reinforcing territorial claims in international discourse.

Fourth, the *geopolitical theory of strategic islands*, historically informed by thinkers like Alfred Mahan and Halford Mackinder, remains relevant in contemporary regional security settings. Mahan's maritime dominance theory argues that control over key islands enables projection of naval power and influence across sea lanes (Furse, 2023). Mackinder's land-sea interaction framework similarly recognizes the value of island territories as pivot points in the balance of global power. In the Indo-Pacific context, small islands

like Berhala Island become critical elements in a state's ability to assert influence and deter external threats.

Lastly, this study adopts an *interdisciplinary framework* that integrates defence strategy, economic planning, and socio-political identity. Such integration allows for the development of hybrid policies where strategic infrastructure, sustainable fisheries, local governance, and cultural identity are interwoven. As nations face increasingly complex maritime challenges, from transnational crime to climate change, no single discipline can sufficiently address these problems in isolation.

By weaving together these theories, this study positions Berhala Island not just as a military asset, but as a symbolic, economic, and strategic space that embodies Indonesia's commitment to sovereignty, development, and regional stability.

To better illustrate the convergence of key conceptual domains informing this study, namely defence theory, blue economy, territorial symbolism, and strategic island geopolitics, the following diagram presents an integrated theoretical framework.

This model emphasizes how Berhala Island's multifaceted value is not singularly militaristic but embedded in a broader interdisciplinary context.

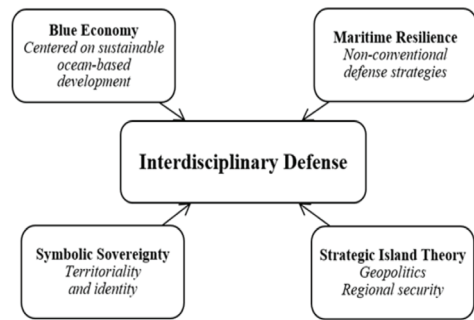


Fig. 1 Interdisciplinary framework for maritime defence of strategic islands

Source: Author's conceptual synthesis based on geopolitical theory, blue economy literature, and identity-territoriality frameworks (Miller, 2018; Voyer et al., 2021).

As visualized in Figure 1, this study operates within a multidimensional framework that connects maritime resilience, economic empowerment, and national symbolism. Theoretical inputs from geopolitics (Mahan, Mackinder), territoriality, and sustainable development coalesce to inform a defence paradigm rooted not only in military preparedness but also in socioeconomic integration and symbolic presence. This framework underpins the subsequent analysis of Berhala Island's practical strategic roles.

3. METHODOLOGY

This study adopts a qualitative descriptive research design to explore

the strategic and symbolic role of Berhala Island within Indonesia's maritime defence and blue economy framework. Qualitative research enables a holistic understanding of social, political, and economic phenomena, especially in the context of complex policy intersections and spatial sovereignty (Flick, 2015).

3.1. Data Sources

This research utilizes both secondary and primary data sources. The secondary data include:

- Government policy documents and defence white papers issued by the Ministry of Defense (*Kementerian Pertahanan*), Maritime Security Agency (*Bakamla*), and the Ministry of Marine Affairs and Fisheries (*KKP*).
- Peer-reviewed journal articles addressing maritime strategy, blue economy, and sovereignty.
- Marine spatial planning documents, maritime zone maps, and regional development blueprints.
- Verified news reports and public communications from state institutions such as *Kemenko Marves* and the Indonesian Navy (*TNI AL*).

In addition to secondary data,

this study also incorporates primary fieldwork through:

- *Interviews* with local fishermen, government officials, and military personnel to gather firsthand insights on the lived realities and operational challenges in Berhala Island's maritime zone.
- *On-site observation* to explore local interpretations of sovereignty, economic utilization, and symbolic significance.

This combination of documentary analysis and field-based empirical evidence enhances the contextual validity and practical relevance of the study's findings.

3.2. Analytical Techniques

Two qualitative techniques were employed in data analysis:

- *Content analysis*, used to identify recurring themes, narratives, and policy patterns within textual documents (Bell et al., 2022).
- *Contextual analysis*, applied to position Berhala Island within broader national frameworks of maritime defence, territorial governance, and blue economy integration (Schreier, 2012).

To ensure transparency and analytical rigor, the content analysis followed a structured process:

- *Text Selection*: Materials were chosen based on relevance, authority, and publication recency (post-2015).
- *Coding Process*: Codes were initially derived from the theoretical framework and refined based on emerging patterns during reading.
- *Thematic Synthesis*: The data were clustered into thematic domains such as strategic symbolism, defence-economy synergy, and institutional coordination.
- *Triangulation*: Key insights were validated by cross-checking among academic references, government documents, and media sources to ensure credibility and consistency (Carter et al., 2014).

This methodological structure provides a robust basis for understanding the strategic, economic, and symbolic dimensions of Berhala Island.

4. FINDINGS AND DISCUSSION

4.1. Strategic Value of Berhala Island

Berhala Island, a small island strategically located in the Malacca

Strait near the maritime border between Indonesia and Malaysia, has long held significance in geopolitical discourse, especially concerning maritime surveillance and territorial control. Historically, the island was subject to a *territorial dispute* between Indonesia and Malaysia that culminated in a resolution by the International Court of Justice in 2002, which confirmed Berhala Island's sovereignty under the Republic of Indonesia. This resolution did not merely settle a bilateral disagreement; it re-emphasized the island's geopolitical value as a *sovereign foothold* in a contested maritime corridor.

The island's location near one of the busiest shipping lanes in the world, *the Strait of Malacca*, enhances its value for maritime oversight. It lies close to Indonesia's *Exclusive Economic Zone (EEZ)* boundary, giving it strategic leverage in monitoring transnational maritime activities, including illegal fishing, smuggling, and foreign naval movement (Dao et al., 2024). From a defence perspective, Berhala Island serves as a forward surveillance post, offering tactical visibility into the Indo-Pacific maritime traffic.

The need for *persistent maritime domain awareness (MDA)* has driven several countries in the region to invest in small island fortifications and radar-

based defence installations (Kamran Dastjerdi & Hosseini Nasrabady, 2020). Indonesia’s own strategy under the Global Maritime Fulcrum doctrine emphasizes the strengthening of maritime surveillance through radar installations and naval posts on outer islands (Simatupang, 2023). Berhala Island thus represents a vital node within this broader security architecture, enabling real-time data collection and coordination among naval and coast guard units.

The Indonesian Navy (TNI AL), in cooperation with Bakamla and the Marine Security Agency, has periodically deployed assets near Berhala as part of regional patrol coordination (Rosyidin, 2021). While not a full-fledged naval base, its symbolic and operational function as a maritime watchtower underscores the island’s relevance in Indonesia’s layered maritime defence.

Moreover, Indonesia’s obligations under the *United Nations Convention on the Law of the Sea (UNCLOS)*, especially regarding EEZ control, require not only legal recognition but also physical presence and routine activity on its outermost islands (Bueger et al., 2019). Berhala Island, therefore, is more than a point on the map, it is an active instrument of sovereign presence in a geopolitically sensitive zone.

Berhala Island’s geopolitical significance is underscored by its role in maritime surveillance and EEZ management. The following table summarizes key strategic functions and their implications for Indonesia’s defence posture:

Table 1 Strategic functions of Berhala Island in maritime defense

Function	Description	Defense/Policy Implication
EEZ Monitoring	Proximity to Indonesia’s EEZ boundary enables control over resource exploitation and foreign vessel movements.	Ensures compliance with UNCLOS; deters illegal fishing and smuggling (Dao et al., 2024).
Maritime Surveillance	Acts as a forward radar/sensor node for the Malacca Strait.	Enhances Maritime Domain Awareness (MDA) under Global Maritime Fulcrum doctrine (Simatupang, 2023).
Naval Coordination	Periodic patrols by TNI AL and Bakamla.	Strengthens layered defence strategy and regional deterrence (Rosyidin, 2021).

Source: Synthesized from Kamran Dastjerdi & Hosseini Nasrabady (2020); and Bueger et al. (2019).

As shown in Table 1, Berhala Island's multifunctional role aligns with Indonesia's need to integrate territorial control with proactive surveillance. This synergy underscores the island's irreplaceability in regional security architectures.

4.2. Blue Economy Potential for Maritime Communities

While Berhala Island has traditionally been viewed through the lens of territorial sovereignty and surveillance, its latent economic value within the framework of the blue economy remains largely underdeveloped. This island, located near artisanal fishing routes and within sheltered anchorage zones, presents opportunities for sustainable maritime livelihoods.

The blue economy model, as promoted by UNCTAD and adopted by Southeast Asian states, seeks to integrate ocean-based economic development with ecological stewardship and community resilience (Voyer et al., 2021).

In its current use, Berhala Island serves as an informal rest stop for traditional fishers, particularly those from Sumatra's eastern coast. However, this informal use lacks supporting infrastructure and regulation. The potential

development of small-scale facilities, such as cold storage units, docks, and navigation aids, would not only improve fisher safety and efficiency but also reinforce sovereign presence in remote maritime spaces.

4.2.1. Cost-Benefit Considerations

A preliminary cost-benefit analysis suggests that modest investments in dual-use infrastructure could yield significant social and strategic returns:

- *Costs:* Construction of multi-use docks, solar-powered cold storage, and communication beacons may require an initial investment of approximately IDR 5–7 billion, based on comparative infrastructure projects in outer islands (Leal Filho et al., 2022).
- *Benefits:* These facilities could serve over 500 small-scale fishers, enhance Indonesia's maritime domain awareness, reduce fuel and operational costs by up to 30%, and stimulate local fishery productivity and safety.
- *Strategic Return:* The physical development also reinforces sovereign visibility and operational readiness in a high-traffic maritime corridor. Hence, although initial

infrastructure costs are non-trivial, the long-term benefits to both economic empowerment and national defence posture justify the proposed interventions.

The blue economy potential of Berhala Island hinges on targeted infrastructure and policy support. Table 2 outlines actionable opportunities and their projected impacts on local communities:

Table 2 Blue economy opportunities and community benefits

Initiative	Description	Expected Impact
Fisheries Shelter Hub	Construction of docks, ice storage, and navigation aids.	Improves safety and productivity for 500+ artisanal fishers (Leal Filho et al., 2022).
Eco-Tourism Zone	Designated area for low-impact tourism (e.g., birdwatching, coral trails).	Diversifies livelihoods; attracts regional tourism revenue (Mycoo et al., 2022).
Marine Logistics Point	Fuel and emergency supplies for vessels.	Reduces response time during maritime crises by 40% (Pomeroy et al., 2019).

Source: Derived from Voyer et al. (2021); and Wen et al. (2022).

Table 2 demonstrates how blue economy investments could transform Berhala Island into a nexus of resilience. Such initiatives would concurrently bolster sovereignty by embedding state presence in daily economic activities.

4.2.2. Environmental and Ecological Considerations

Sustainable development of Berhala Island must also address environmental risks and ecological constraints:

- *Marine biodiversity:* The island lies near coral-rich waters, which may be sensitive to increased vessel traffic, anchoring, and pollution. Environmental impact assessments (EIA) are necessary prior to major construction.
- *Carrying capacity:* Given the island's small size and limited freshwater sources, infrastructure must be designed for minimal ecological footprint using renewable energy and waste management systems.
- *Regulatory integration:* All development must align with Indonesia's National Marine Spatial Planning (RZWP3K) framework to prevent zoning

conflicts and ensure protection of critical habitats (Wen et al., 2022).

Balancing economic activity with environmental safeguards is essential to uphold the integrity of the blue economy model. By integrating ecological resilience into infrastructure planning, Berhala Island can serve as a prototype for sustainable, low-impact development in strategic maritime zones.

4.3. Berhala Island as a Symbol of Sovereignty

Territorial sovereignty is not merely an issue of legal boundaries or cartographic representations; it is also profoundly symbolic. In the case of Berhala Island, the assertion of Indonesian sovereignty is expressed through physical presence, symbolic markers, and institutional visibility. This island, while small in size, embodies a larger national narrative of asserting identity at the periphery, where geography intersects with political will.

Drawing on territoriality and identity theory, scholars emphasize that sovereignty is enacted not only through legal instruments but through daily practices and spatial representations (Miller, 2018). The presence of a military outpost, the hoisting of a national flag, or the

construction of civilian infrastructure on a remote island like Berhala Island serves as a performative expression of Indonesia's rightful claim. These symbolic gestures are especially vital in zones close to international boundaries, where ambiguity can invite competing claims or encroachment (Bueger et al., 2019).

Indonesia's defence and maritime strategy recognizes the semiotic power of presence. The TNI AL's surveillance post on Berhala Island, while minimal in scale, is emblematic of Indonesia's broader doctrine of territorial consolidation, where infrastructure serves both strategic and symbolic functions. The establishment of posts and outposts in borderland islands not only aids in surveillance but also sends a clear message of spatial ownership to international observers.

The role of local narratives and cultural representation also plays a crucial part. Berhala Island has long been embedded in the collective memory of coastal communities in Jambi and Riau as a marker of national boundary. Oral histories and media representations often portray the island as a "guardian" of the sea border, enhancing its symbolic relevance. These narratives are essential in reinforcing the social legitimacy of state presence,

especially in regions historically marginalized by central policy (Yulianto & Effendi, 2020).

Moreover, the symbolic role of Berhala Island gains importance within regional geopolitics. The *Association of Southeast Asian Nations (ASEAN)* has often highlighted the need for peaceful resolution of maritime disputes, but at the same time, member states continue to assert their claims through “acts of occupation”, including infrastructure development and civilian deployment (Ali et al., 2024). Indonesia, by embedding sovereignty through developmental and symbolic means, aligns with this broader regional trend.

Sovereignty, in this context, is not static. It is a dynamic process of making space visible, inhabitable, and politically legible. Berhala Island’s current status, though modest in physical development, represents a layered sovereignty, one that merges defence strategy, community engagement, and national symbolism into a coherent narrative of belonging and control.

4.4. Intersectoral Integration for Defense Strategy

Effective defence of maritime spaces, especially small, outermost islands like Berhala Island requires

more than the deployment of naval units or installation of surveillance equipment. It demands intersectoral coordination, where institutions across defence, maritime affairs, environment, and regional governance work in harmony to achieve both national security and local resilience. In the Indonesian context, this approach aligns with the principles of *total defence (pertahanan semesta)*, in which every component of society contributes to safeguarding the state (Fathun, 2019).

Berhala Island falls under the jurisdiction of several national and local actors. The *Indonesian Navy (TNI AL)* is responsible for military surveillance and coastal patrols; the *Ministry of Marine Affairs and Fisheries (KKP)* oversees the sustainable use of fisheries and marine zones; the *Ministry of Environment and Forestry (KLHK)* governs conservation regulations if designated as a protected area; and local governments (*Pemda*) handle administrative and infrastructure development. The overlapping mandates can often lead to coordination gaps, inefficient resource use, or contradictory policy outcomes (Thomas et al., 2021).

A successful model for intersectoral coordination lies in

the creation of a joint maritime task force or inter-agency platform, where policy alignment and operational synchrony are institutionalized. Drawing lessons from the Sulu–Sulawesi Sea trilateral patrols between Indonesia, Malaysia, and the Philippines, integrated command structures supported by real-time communication systems can significantly enhance both security and operational efficiency (Cheng, 2019).

Berhala Island could serve as a pilot site for intersectoral cooperation, especially through integrated activities like:

- Establishing a dual-use maritime facility for both defence and fishing logistics.
- Deploying *community-based surveillance (CBS)* models where local fishermen serve as informal maritime sentinels, reporting suspicious activity to authorities (Distincta et al., 2025).
- Incorporating the island into the *Marine Spatial Planning (RZWP3K)* framework, clearly designating zones for defence, conservation, and livelihoods, thus reducing jurisdictional conflict.

Another recommendation is the formation of a *Local Maritime Coordination Council (LMCC)*

involving TNI AL, Bakamla, KKP, KLHK, and local representatives. Such councils can function as adaptive governance units, responding dynamically to changing security threats, ecological risks, or economic developments.

Crucially, intersectoral defence strategy is not merely bureaucratic, it is transformative. It redefines security as a shared national project, combining the presence of naval institutions with the voices and interests of coastal communities. This reflects the modern security doctrine that connects hard power with soft governance, ensuring that even the smallest islands, like Berhala Island, become active centres of national cohesion and integrated development.

Effective management of Berhala Island requires harmonizing diverse stakeholders. Table 3 maps key actors and their roles in an integrated governance model:

Table 3 Stakeholder roles in Berhala Island’s intersectoral governance

Stakeholder	Primary Responsibility	Proposed Coordination Mechanism
TNI AL	Maritime patrols, surveillance, and sovereignty enforcement.	Joint task force with real-time data sharing (Cheng, 2019).

Stakeholder	Primary Responsibility	Proposed Coordination Mechanism
KKP	Fisheries management and sustainable resource use.	Marine Spatial Planning (RZWP3K) integration (Thomas et al., 2021).
Local Government	Infra-structure development and community engagement.	Local Maritime Coordination Council (LMCC) for adaptive governance.

Source: Adapted from Fathun (2019); and Thomas et al. (2021).

Table 3 highlights the need for institutionalized collaboration to avoid fragmentation. A unified framework, as proposed, would optimize Berhala Island’s dual defence-development mandate.

To move from theory to implementation, Berhala Island must be governed through a practical, multi-stakeholder model. The following diagram visualizes a governance framework that integrates military, civilian, and ecological functions in a coordinated and adaptive structure.

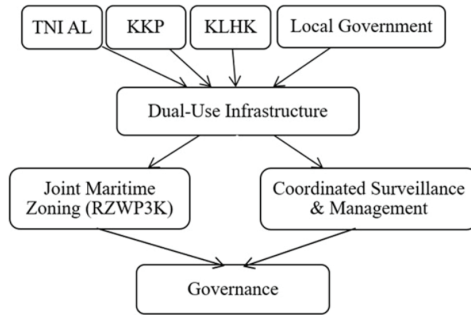


Fig. 2 Integrated Governance Framework for Strategic Maritime Island Management

Source: Author’s design based on inter-agency coordination models from Indonesian maritime policy (Kemenhan, KKP, KLHK, Bakamla).

This model places Berhala Island at the centre of shared institutional responsibilities. Rather than treating defence, ecology, and economy as siloed mandates, the framework encourages cooperative zoning, joint monitoring, and synchronized operations. It proposes the formation of a *Local Maritime Coordination Council (LMCC)*, enabling cross-sectoral dialogue and implementation. The island thus evolves from a marginal outpost into a prototype of integrated sovereignty, secure, sustainable, and socially responsive.

5. CONCLUSION AND POLICY RECOMMENDATIONS

Berhala Island stands as a remarkable example of how small, remote islands can embody complex and layered roles in a nation's maritime architecture. Strategically located near international sea lanes and within Indonesia's Exclusive Economic Zone, it offers far more than a point of military surveillance, it is a living symbol of national sovereignty, a latent economic node, and a bridge between defence and development.

From an *economic standpoint*, Berhala Island holds untapped potential to support small-scale fisheries, act as a shelter hub for maritime communities, and promote sustainable ocean-based livelihoods. From a *security perspective*, its position enhances Indonesia's ability to monitor strategic maritime corridors, strengthening maritime domain awareness. *Symbolically*, the island represents a performative act of territorial identity, a marker of presence in a contested maritime region.

To optimize its strategic value, the following policy recommendations are proposed:

- *Develop Dual-Use Infrastructure:* Construct facilities that simultaneously

support defence operations and community needs, such as multi-purpose docks, communication towers, and emergency shelters that serve both military and fisher populations.

- *Integrate Blue Economy into Defense Doctrine:* Incorporate marine economic development into national defence planning to reinforce sovereignty not just through force, but through sustainable presence and prosperity.
- *Establish Berhala Island as a Governance Model:* Designate the island as a pilot site for intersectoral governance, integrating defence, fisheries, conservation, and local development into a unified island management strategy.

In doing so, Indonesia not only safeguards its borders but transforms its outermost islands into beacons of sovereignty, sustainability, and security.

REFERENCES

- [1] Ali, I., Tarsat, M. & Taong, D.N. (2024) Revaluation and Reconstruction of the Maritime Historiography in Southeast Asia Archipelago. *International Journal of Business and Social Science Research*, 5(5), pp. 1–9. Available at: <https://www.>

- www.jstor.org/stable/48557419
- [16] Patil, P. et al. (2016) Toward A Blue Economy: A Promise for Sustainable Growth in the Caribbean; An Overview. *The World Bank*. Available at: https://www.researchgate.net/publication/308714082_2016_Toward_A_Blue_Economy_A_Promise_for_Sustainable_Growth_in_the_Caribbean_An_Overview_The_World_Bank_Washington_DC
- [17] Pomeroy, R.S. et al. (2019) The role of scale within an Ecosystem Approach to fisheries management: Policy and practice in Southeast Asian seas. *Marine Policy*, 106, 103531. <https://doi.org/10.1016/j.marpol.2019.103531>
- [18] Rosyidin, M. (2021) The cult of glory: national myth and the idea of Global Maritime Fulcrum in Indonesia's foreign policy, 2014–2019. *South East Asia Research*, 29(3), pp. 297–314.
- [19] Schreier, M. (2012) *Qualitative Content Analysis in Practice*. London: SAGE Publications.
- [20] Simatupang, H.Y. (2023) Progress and Prospects: President Jokowi's Maritime Diplomacy and Global Maritime Fulcrum. *Dinamika Global: Jurnal Ilmu Hubungan Internasional*, 8(2), pp. 174–191.
- [21] Thomas, A. et al. (2021) Why they must be counted: Significant contributions of Fijian women fishers to food security and livelihoods. *Ocean & Coastal Management*, 205, 105571. <https://doi.org/10.1016/j.ocecoaman.2021.105571>
- [22] Voyer, M. et al. (2021) Launching a Blue Economy: crucial first steps in designing a contextually sensitive and coherent approach. *Journal of Environmental Policy & Planning*, 23(3), pp. 345–362. <https://doi.org/10.1080/1523908X.2020.1856054>
- [23] Wen, W. et al. (2022) Towards Marine Spatial Planning Implementation in Indonesia: Progress and Hindering Factors. *Coastal Management*, 50(6), pp. 469–489. <https://doi.org/10.1080/08920753.2022.2126262>