JOURNAL OF DEFENSE RESOURCES MANAGEMENT

Vol. 16, Issue 1 (30)/ 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
- 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

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, 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 and Sherpa Romeo.***

INTERNATIONAL ADVISORY BOARD

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

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; ISSN-L: 2247-6466

EDITING GUIDELINES

Page setup: top – 28mm, bottom – 28mm, inside – 21mm, outside – 24mm, header – 12,5mm, footer – 12,5mm, mirror margines activated;

- paper format B5 176X250;
- font: Times New Roman;
- style: normal.

Paper title: upper case, font size 14pt, bold, centered;

Author (s) name:

- first name, surname, font size 12pt, bold, centered;
- two free spaces below the title of the paper.

Author's affiliation, city, country:

- one free space (12pt) below author's name, font 12pt, centered.

Abstract:

- one free space (12pt) below author's workplace name;
- up to 150 words;
- font size 11pt, Italic, justified, left-right alignment.

Key words:

- maximum 8;
- one free space (12pt) below the abstract;
- 11pt, italic, lef alignment, separated by comma.

Paper body:

- even number of pages (maximum 6; research papers may have more depending on topic comprehensiveness);
- no free space between lines;
- two free spaces below the key words (24 pt);
- two columns, width: 60mm, spacing: 5mm;
- font size 12pt, justify;
- paper main parts: introduced by titles numbered with Arabic figures, upper case, font size 12pt, bold, centered. One free space (12pt) above the text and one free space (12pt) below it;
- paragraph indentation: 6mm;
- quotations of more than two lines should be indented in a separate paragraph;
- authors should organize the article into sections and also include sub-headings where appropriate.

Drawings, diagrams and charts:

- one free space (12pt) below the text;
- width similar to that of the column they belong to. Should this be impossible to achieve, then they will be printed across the whole breadth of the page either at the top or the bottom of the page;
- numbered in Arabic figures;
- accompanied by captions, one free space (12pt) below the drawings, centered, font size 12pt;
- font size 12pt, justify;mathematical formulae: 6mm left alignment; ordinal numbers: in round brackets, right alignment; Times New Roman;
- Full – 12pt.; Subscript / Superscript – 9pt.; Sub-Subscript / Superscript – 7pt.; Symbol – 16pt.; Sub-Symbol – 12pt;
- Long mathematical formulae: not wider than the column or displayed on the whole width of the page either at the top or bottom of the page.

Names of organizations: printed in Upper case, straight.

Names of military technology products: in Upper case, Italic.

Essential notes:

- indicated by superscript numbers in the text;
- presented at the end of the text but before the references.

Reference citations in the text: in round brackets;

- author: year (e.g. Smith:1995) OR if quote provided: author: year, page no. (e.g. Smith:1995, p.45);
- “et al.” mentioned when citing a work by more than two authors. For example: Brown et al. (1981) or (Brown et al., 1981).
- use letters (e.g. a, b, c, etc.) to distinguish citations of different works by the same author in the same year. For example: Brown (1975a, b).

References:

- listed in alphabetical order, at the end of the article;
- numbered in Arabic figures;
- the titles of the reference books will be printed in Italic.

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

Journal website: https://jodrm.eu

PRINTED AT THE MILITARY TECHNICAL PUBLISHING CENTER

CONTENTS

THE BEST OF TWO WORLDS? GATHERING VALIDITY EVIDENCE FOR AN INTEGRATED INSTRUCTIONAL DESIGN MODEL FOR SKILLS TRAINING AND ACADEMIC EDUCATION AT A MILITARY ACADEMY

Steven HORNSTRA*, Jaap HOOGENBOEZEM, Steven DURNING***, 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,
** Royal Netherlands Army, Armed forces of the Netherlands, The Netherlands; Department of political science, Maastricht University, 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, **** 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

During military operations, officers must often integrate military skills and academic education (i.e. strategic thinking), which are typically taught separately at a military academy. To address this, an innovative integrated instructional design framework, the TrEd ID model, was developed to combine these learning tracks. A focus group study with academic educators from the Dutch military academy provided validity evidence for the TrEd ID model, showing it effectively meets the demands of both military skills training and academic education. The study also offered insights for potential implementation. Future research could focus on further validating the TrEd ID model among other stakeholders and exploring practical guidelines for its implementation at military academies.

Key words: *officer education, military training, academic education, instructional design.*

1. INTRODUCTION

Military officers must be able to perform under demanding (e.g. volatile, uncertain, complex and/or ambiguous) conditions. Consequently, comprehensive training and education of military officers is of prime importance (Victor Tillberg: 2020). Skills training and academic education have always been important aspects of their professional development. The training of military skills is typically provided by military instructors in non-commissioned officer (NCO) ranks (i.e. military trainers). Military skills training traditionally focuses on a specific performance or action (Hornstra et al., 2023), such as map-reading and selected leadership skills (Jansen et al., 2019).

On the other hand, academic education is provided by fellow military officers and/or civilian academicians (i.e. academic educators). Academic education focuses on strategic thinking (i.e. analytic thinking in military or associated domains in order to cope with new experienced situations that not had been previously experienced), such as reinstalling the rule of law under the specific circumstances of a mission area. Due to the intensified role of civil-military interaction and the rise in hybrid warfare ever more emphasis has been placed on academic education as part of officer education (Hornstra et al., 2023). For instance, at the NETHERLANDS DEFENCE ACADEMY (NLDA), academic education is fostered by courses such as “methods and techniques of research”, or “evolution of armed forces and warfare” (NLDA: 2021a). The name of some academic courses, such as “weapon systems and technology” (NLDA: 2021b), may suggest that these courses can be halfway between skills training and academic education. Nevertheless, some topics that skills training focuses on, can also be considered specifically from the perspective of strategic thinking.

At a military academy, skills training and academic education are often separated learning tracks, lacking a common language and common methods. However, in frequently complex and dynamic operational settings, officers typically need to apply military skills and academic education (i.e. strategic thinking) simultaneously. As a result, it is paramount that officer cadets thus learn to integrate military skills and strategic thinking in a relevant way, without assuming that this integration occurs spontaneously over time. It is thus important to link skills training and academic education at a military academy in meaningful ways (Hornstra et al., 2023).

To contribute to this meaningful connection, Hornstra et al. (2024) developed an innovative integrated instructional design (ID) model, referred to as the TrEd ID model (See Appendix A). This model incorporates elements from both skills training and academic education ID models. By doing so, it intends to address the needs of both domains. A goal of the TrEd ID model is to promote and support the development of mutual awareness and collaborative initiatives among military trainers and academic educators at a military academy, and ultimately to better prepare officer cadets for their future responsibilities.

Previously, Hornstra et al. (submitted, 2024) collected evidence for the TrEd ID model among officer cadets of a Gendarmerie Corps. Based on the experiences and insights of these officer cadets, they refined the possible use of the TrEd ID model and made recommendations about its implementation at a military academy. Although acknowledging the perspective of the students (e.g. officer cadets) on the TrEd ID model, other stakeholder viewpoints are likewise of importance. The purpose of the current study is therefore to gather additional validity evidence for the TrEd ID model in the military academy context from the academic educators' perspectives in order to (a) further refine the possible utilization of the TrEd ID model and (b) further explore how to implement it at a military academy. The findings of this study can supplement the existing literature about closing the gap between skills training and academic education in a military setting.

2. METHODS

We conducted two focus group interviews (N=4, N=5) via an online platform. The decision to utilize a location-independent, online format was necessitated by the logistical challenges of convening a group of academic educators simultaneously, particularly given that many hold concurrent positions at civilian universities. Given the geographical dispersion of participants, such an online method was recommended by Halliday et al. (2021). Subsequently, we thematically analyzed the data to gather validity evidence for the TrEd ID model at a military academy. We selected focus groups over other qualitative research methods, because focus groups enable us to let participants generate new ideas and react to each other's insights in order to obtain a deeper understanding of the phenomenon studied (Krueger: 1994; Morgan: 1996; Bowling:

2002). Furthermore, focus groups are suited to explore ill-defined and poorly studied topics (Britten et al., 1995; Kitzinger: 1995). For example, Stalmeijer et al. (2009) used focus groups to gather validity evidence for teaching methods in a clinical context. As a benchmark for rigor of our focus group research, we used the AMEE Guide No. 91 on using focus groups in medical education research (Stalmeijer et al., 2014). We followed a questioning route based on Krueger and Casey (2009), and applied in Stalmeijer et al. (2014) (See Appendix B).

To conduct online focus group interviews, we employed the software application Microsoft Teams, as endorsed by Keemink et al. (2022). To facilitate smooth interpersonal interactions during these sessions, we organized the focus group interviews into small groups of approximately four to five participants, following the recommendations of Keemink et al. (2022) and Bolin et al. (2023).

Each focus group session lasted a maximum of 60 minutes, using a semi-structured interview guide. The semi-structured interview guide was developed on the basis of the teaching and learning activities prescribed by the TrEd ID model (See Appendix C). To provoke spontaneous discussion, we did not a priori share this ID model with the participants. Further, we used the elements of the TrEd ID model that were not yet covered by the focus group discussion as prompts to elicit additional discussion on those remaining elements.

The viewpoint of the participants originated from their specific lived experiences, whereas the researchers abstracted and generalized the information. Because of these different viewpoints, and the potential disagreements that could arise from them, we conducted verbal member checking both throughout and at the conclusion of the focus group sessions. This process entailed summarizing and verifying the information with the participants, which did not yield any additional insights or recommendations for revision. In this way, member checking served as an additional quality control measure to ensure the credibility of our study findings (Mays & Pope: 2000).

2.1. Participants

We used a purposive sampling strategy: the participants were subject-matter experts on the professional development of officer cadets. These subject-matter experts are academic educators, meaning military officers and civilian academicians who provide academic education at a military academy. We expected that heterogeneous focus groups, i.e. both (former) military officers and civilian academicians, could enhance the group interaction and facilitate contrasting military academic and civilian academic points of view.

2.2. Theoretical framework and methodology

The study was based on the constructivist paradigm, meaning that the data and analysis are actively and socially constructed by both participants and researchers (Boeije: 2010). This epistemological viewpoint implied the application of a research method that allows for an active and social construction of knowledge by both participants and researchers. For this reason, we chose the combination of focus groups and phenomenological approach.

Our focus group research was set within a phenomenological approach. The roots of phenomenology as a research methodology are in the school of philosophy named alike, in which it is assumed that all understanding of reality comes from the lived experiences of individuals (Creswell et al., 2007). Within phenomenological research, researchers rather describe than analyze or explain the common elements in the self-described experiences of the participants with a phenomenon (Creswell et al., 2007). Consequently, phenomenological research helps to explore and understand the experiential meaning of people regarding the phenomenon studied (Creswell: 2012). In this study, we intended to explore and understand the experiences, ideas and opinions of academic educators with regard to the TrEd ID model in the context of a military academy.

As Cook et al. (2015) stated, validation is rather a process of gathering evidence to support specific decisions and actions than a final result. We applied Kane’s (2013) framework, originally meant to gather validity evidence for test scores, to direct the process of gathering and interpreting validity evidence for the TrEd ID model. In this framework, Kane (2013) stressed the importance of determining the use of the validation process in advance. Here, we employed the qualitative data produced by subject-matter experts to improve the use of the TrEd ID model and to formulate associated implementation guidelines.

Furthermore, Kane (2013) described a chain of four inferences in the validity argument: scoring, generalization, extrapolation and implications. In this study, the scoring inference is in translating the group interaction within the focus groups into qualitative data; generalization in generalizing the data from the focus groups to the research setting; extrapolation in extrapolating the data from the research setting to the context of officer education; and implications in interpreting the data to propose actions regarding the use of the TrEd ID model within officer education.

2.3. Setting and procedure

The study was conducted at the NLDA, an institution dedicated to preparing officer cadets to meet the dynamic demands of operational military environments (DUTCH DEPARTMENT OF DEFENCE: 2021). The FACULTY OF MILITARY SCIENCES (FMW) of the NLDA is responsible for delivering the academic education component of the Dutch officer cadets education, specifically through a bachelor's degree program (Van Schilt: 2011). During the initial phase of officer education, which spans approximately the first five months of a four-year program, cadets undergo intensive military skills training (Jansen et al., 2019). This training is periodically reinforced throughout the entire duration of their officer education (e.g. seven times over the course of one week during both the second, third, and fourth year of the officer education program). Following this initial period, cadets transfer to academic coursework provided by the FMW (Van Schilt: 2011).

The department heads within the FMW extended invitations to their team members during departmental meetings to participate in the focus group sessions centered on instructional design at military academies. Participation in such a session was voluntary. The scheduling and location of the two one-hour sessions were determined based on the availability and preferences of the participants, with online sessions conducted on 3 and 12 June, 2024.

During the focus groups sessions, one researcher (JH) served as moderator, while another acted as observer (SH). The researchers introduced themselves as colleagues within the Dutch MINISTRY OF DEFENCE, so the participants would consider the researchers as insiders from the start, to create a safe social environment for the participants to share their experiences, ideas and opinions. The researchers explicitly confirmed in advance the role of the academic educators as experts on the subject at hand, whereas the researchers did not express viewpoints themselves in the focus group discussion. Before starting each focus group, the participants were reminded about the study's objectives and the research protocol. To ensure confidentiality, the participants were assured that all the data would be stored securely (i.e. only accessible to the research team), and processed and reported anonymously. Furthermore, we provided the opportunity for participants to contact us afterwards in the event of any additions or concerns, although none of the participants utilized this option. All focus group discussions were audio recorded and subsequently transcribed verbatim.

2.4. Data analysis

We strived for data sufficiency through analytic saturation, meaning that we continued conducting focus groups until no new themes about our research topic emerged anymore (Stalmeijer et al., 2014). The time of saturation was determined by reaching consensus in the research team, based on the ongoing thematic analysis. However, the sample size was set at a minimum of two focus groups in advance.

We applied a deductive approach of the six-step procedure of the AMEE Guide No. 131 on thematic analysis of qualitative data (Kiger et al., 2020). These six steps are (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. The thematic analysis was conducted by two of the researchers (SH and JH). These two researchers resolved inconsistencies on codes and themes by consensus. If necessary, discrepancies were resolved by discussion with the entire research team (SH, JH, SD, WvM). We used ATLAS.ti (Version 24) to organize the thematic analysis. Additionally, we applied the COREQ guidelines for qualitative research (Tong et al., 2007) as a quality assurance check contributing to scientific rigor.

2.5. Reflexivity

The researchers actively engaged in the social process of constructing knowledge and so they influenced the outcomes of this study. Therefore we share the following information. Three researchers (SH, JH and SD) are experienced as (former) military officers. Two researchers (SD, WvM) are experienced as medical specialists. Four researchers (SH, SD, JH, WvM) possess professional qualifications in the field of education. During this entire study, we kept an audit trail to provide insight into and reflect on the influence of the researchers on the process of constructing knowledge.

3. RESULTS

In this section, we present the qualitative findings from the focus group interviews. Across the two focus group sessions, we identified four themes that described participants' perceptions of the quality of officer education: (1) Active learning approach, (2) Authenticity, (3) Rigorous learning approach, and (4) Institutional alignment. Table 1 presents the four identified themes, accompanied by their respective definitions and representative quotations.

Table 1. Definitions of themes

Theme	Description	Example quotes
Active learning approach	Teaching strategies with the aim of officer cadets' engagement and participation in learning activities	"Let them prepare, do group assignments, let them present, work with a video, work with a forum. In short, try to create as much interaction as possible."
Authenticity	Connection between educational setting and professional domain	"Last week, I went with the class to Ypres to feel, look, taste, and smell on that battlefield and to let them experience it there."
Rigorous learning approach	Connection between different learning tracks at military academy	"...there is a contrast in that respect between the approach of teaching people to think - what the principle of the bachelor's program is - and, on the other hand, expecting people to perform a certain task"
Institutional alignment	Conformity of ID with institution's educational framework	"We have a lot of freedom ... of course within the framework of our accredited education program"

3.1. Theme 1 – Active learning approach

The theme "Active learning approach" describes the teaching strategies with the aim of officer cadets' engagement and participation in learning activities. Participants expressed that the fundamental nature of active learning is

> *…to maximize interaction with the class as much as possible…*

(Participant 2, Session 1). They reported that they valued these active learning approaches as practiced by "…a variety of working methods" (Participant 3, Session 2), including innovative and creative approaches such as "…creating a podcast" (Participant 4, Session 2) to demonstrate the newly acquired knowledge and skills, and "interviewing colleagues... in the different branches" (Participant 2, Session 2) to develop research skills. Participants indicated a preference for such working methods, provided that the overall structure remains clear and that attention is given to the guidance offered, as expressed in the observation

> *…it is essential to ensure that there is a coherent framework in your teaching and in the approach to the program. They [i.e. officer cadets] do not want to be thrown into the deep end entirely. They require a certain level of stability.*

(Participant 3, Session 2). For example, as discussed by participants, this structure and guidance can be provided by offering such innovative working methods "…in conjunction with a form of classroom instruction" (Participant 4, Session 2).

Nonetheless, participants also still appreciated a traditional approach in which a gifted teacher delivers

> *...just a good story, told well, and trying to engage people in that way.*

(Participant 2, Session 1).

3.2. Theme 2 – Authenticity

The theme "Authenticity" represents the connection between the educational setting and the professional domain. Regarding the acquisition of new knowledge and skills, participants expressed appreciation for providing officer cadets with a rationale for understanding "…why that is part of being an officer" (Participant 2, Session 1). They valued linking academic principles to real-world applicability, reflected in the remark

> *What we talk about concerns real people who have faced genuine problems and have struggled with them, sometimes managing well and sometimes not at all. All the dimensions that one might encounter in real life as an officer suddenly become very tangible.*

(Participant 1, Session 1). However, participants underscored the complex relationship between theoretical insights and practical application:

> *Look, there is the principle that the world is more complex than the theory. So if you want to apply the theory, you need to think about how to do that.*

(Participant 5, Session 1). Additionally, based on responses from the officer cadets such as

> *The bachelor's degree, so what? I'm here to learn the military profession.*

(Participant 2, Session 2), participants regretted that, according to them, officer cadets do not always perceive a clear link between academic education at a military academy and the real world of the professional domain.

3.3. Theme 3 – Rigorous learning approach

The theme "Rigorous learning approach" represents the connection between the different learning tracks during the professional development of officer cadets transitioning to officers. Participants summarized the officer cadets' overall learning experience at the military academy as

> *Cadet corps, military life [i.e. military skills training] and study [i.e. academic education].*

(Participant 2, Session 1). They experienced the learning tracks of military skills training and academic education as strictly separated from each other, as reflected in the observation

> *...we also set very clear boundaries in between; now you are in your bachelor's period [i.e. academic education], and at that moment, a new green period [i.e. military skills training] begins, and then you have to focus entirely on your studies [i.e. academic education] again*

(Participant 3, Session 1). Participants noted that, in the current context, these learning tracks differ fundamentally in their nature:

> *...there is a contrast in that respect between the approach of teaching people to think - what the principle of the bachelor's program [i.e. academic education] is - and, on the other hand [i.e. military skills training], expecting people to perform a certain task.*

(Participant 1, Session 1). Moreover, from a practical perspective, participants are concerned

> *...that all those parties [i.e. military skills trainers and academic educators] are busy completely blocking the agenda of cadets, because they are afraid that if they do not do so, another party will take over their time.*

(Participant 5, Session 1).

The current organization of these separate learning tracks not only leads to "an incredibly full program" (Participant 4, Session 2) for officer cadets, but also to uncertainty about the desired ultimate learning outcome, as remarked by the commentary

> *... the real proof of the pudding is, of course, [in its eating, that is], how they bring it all together in their own performance [i.e. as an officer]*.

(Participant 2, Session 2). Therefore, participants concluded that

> *...it would be great if we could develop something integral, yes design it, where there are no separate elements [i.e. military skills training and academic education]. Instead, we create a win-win situation [by linking military skills training and academic education], a synergy. And not - what often happens, perhaps unconsciously or in the perception of the receiver [i.e. officer cadets] - that we [i.e. military skills trainers and academic educators] sometimes contradict or undermine each other.*

(Participant 2, Session 2).

3.4. Theme 4 – Institutional alignment

The theme "Institutional alignment" put forward the conformity of ID with the institution's educational framework. Participants indicated that officer education is shaped based on institution-wide established policies and principles. They expressed that learning activities, in their perception, must fit within the policy of "Professional Military Education" (Participant 3, Session 1), essentially meaning the conglomeration of skills training and academic education activities with the aim of optimally preparing officers for their future responsibilities as officers. Furthermore, participants pointed out that "…the applied sciences principle…" requires that officer education contributes to the development of cadets into officers who can both think critically and perform tasks adequately, as aptly summarized in the concepts "…reflective practitioner..." and "…thinking soldier…" (Participant 3, Session 1). Usually, as worded by participants, these learning activities are based "…on the principle of problem-based learning…" (Participant 1, Session 1). Moreover, participants stated that all learning activities must fit within

> *...the framework of formal quality assurance as arranged for accreditation.*

(Participant 5, Session 1), but it must also be aligned with "…the needs of the future workplace" (Participant 2, Session 1). Nevertheless, concerning ID, participants noted that they

> *... have a lot of freedom in that... you can shape the actual implementation in your own way. So there is no prescribed format for that. Sure, there are some basic conditions, but you can create something nice within academic freedom. Therefore, I believe there is a lot of freedom within our institution to design your own instruction.*

(Participant 3, Session 2).

4. DISCUSSION

Our study's findings offered validity evidence supporting the TrEd ID model as an effective ID approach for integrating military skills training with academic education for officer cadets. Additionally, the results highlighted potential strategies for implementing this ID model at a military academy. The following sections provide a detailed discussion of these key points.

4.1. Validity evidence for the utilization of the TrEd ID model

The focus group data revealed that academic educators appreciated the two fundamental principles of the TrEd ID model: Active learning and authenticity. An active learning approach encompasses teaching strategies designed to foster engagement and participation among officer cadets in learning activities. The TrEd ID model mainly actualizes active learning by the activities of its *Practicing* phase: *Providing guidance*, *Practicing skills/trying out solutions* and *Providing feedback*. Additionally, activities in other phases of the TrEd ID model contribute to the active learning approach as well, including *Activating prior knowledge/skills/experiences* and *Complementing skills/ideas by experimenting and studying*.

Furthermore, authenticity signifies the linkage between the educational environment and the professional field. In the TrEd ID model, authenticity is chiefly substantiated by the activities of its *Getting real* phase: *Performing skills/solving problems in authentic environments*, *Assessing performance/problem solving* and *Reflecting on learning process and outcomes in relation to the learning objectives*. Activities of other phases of this ID model insert authenticity in the learning activities as well, such as *Providing authentic problem to be solved* and *Practicing skills/trying out solutions*. In summary, the academic educators' perceptions of the quality of the officer cadets' education program thus aligned with the TrEd ID model's primary tenets.

4.2. Potential strategies for implementing the TrEd ID model

The findings of this study provide potential strategies for the implementation of the TrED ID model at a military academy. These strategies concern a rigorous learning approach and institutional alignment. In the following sections, we elaborate upon this.

4.2.1. Rigorous learning approach

According to the academic educators, the current linkage between military skills training and academic education is thus inadequate, which presents organizational obstacles for officer cadets and unnecessarily increases their workload. Moreover, this prompts academic educators to question whether officer cadets learn to effectively apply military skills and strategic thinking simultaneously if they have learned these in mainly separate learning tracks. Besides, such concerns are not unique to the NLDA, but these are also present at military academies in, for example, Belgium

(Lepinoy et al, 2022) and Sweden (Larsson: 2024). The academic educators therefore aim to achieve an improved connection between military skills training and academic education. To align with this intrinsic need of the academic educators and thereby increase the likelihood of the TrEd ID model's actual use, it may be more effective to introduce the model not merely as a new ID tool in the academic educators' toolbox, but as an instrument that can potentially contribute to establishing the desired connection and thus to a rigorous learning approach.

4.2.2. Institutional alignment

This section consequently delves into the academic educators' suggestion to align the implementation of the TrEd ID model with the institution's educational policies and principles. More specifically, if academic educators were to implement the TrEd ID model in their courses, they must ensure that it contributes to the realization of the institution's educational viewpoint. This is consistent with the recommendation of Schophuizen and Kalz (2020), which states that in the context of innovations in higher education, top-down (e.g. implementation of educational policy) and bottom-up (e.g. implementation of TrEd ID model in class) efforts must be synchronized. However, with an aim towards educational innovation in individual courses, institutional policies are typically perceived as obstacles to innovation (Gilbert et al., 2021). On the other hand, academic freedom, as amply experienced by the academic educators, serves as a crucial enabler for (bottom-up) educational innovation (Laufer et al., 2024). Moreover, if a critical mass of students (e.g. officer cadets) becomes convinced of the benefits of the changes in a course (e.g. an innovative ID), it will provide a positive impetus for the associated implementation (Agrawal et al., 2020). In summary, implementing the TrEd ID model in their courses, academic educators should aim to align their course implementations with institutional educational guidelines, leverage their academic freedom to tailor instruction, and explicitly address the learning needs of officer cadets.

4.3. Strengths and limitations

This study has some strengths. Each focus group included individuals with merely civilian backgrounds as well as those with (former) military backgrounds. This heterogeneous composition of academic educators may have further stimulated the discussion and provided additional insights into ID at a military academy. Furthermore, during the focus group interviews, participants maintained their cameras on to more closely simulate a face-to-face interaction. Despite the virtual environment, this allowed for a fairly natural interaction with and among the participants (Keemink et al., 2022).

However, there are some limitations as well. Online focus group interviews provide fewer non-verbal cues and signals, such as body language, compared to traditional in-person interactions. This could have obfuscated our interpretation of participants' expressions and interactions (Roald et al., 2024). Moreover, academic educators had the option to voluntarily register for the focus group interviews, which may have introduced a degree of self-selection bias. Specifically, participants might have had a pre-existing interest in and/or strong opinions about the research topic of ID. Consequently, the sample of participants may not have been representative of the entire population of academic educators at the NLDA, potentially affecting the findings and their generalizability (Shadish et al., 2002). Lastly, this study is limited to academic educators as experts on the officer cadets' learning process. Nevertheless, the inclusion of military skills trainers in the focus group interviews could have introduced contrasting points of view with academic educators, thereby potentially further enriching the discussion on ID at a military academy and providing additional insights.

4.4. Future research

Future research could focus on gathering further validity evidence for the application and implementation of the TrEd ID model at a military academy among other stake holders in the officer cadets' learning process, including military skills trainers as experts on the development of cadets into officers, and commanders as future employers of the officer cadets. Additionally, further research could investigate the necessary practical guidelines for implementing the TrEd ID model at a military academy.

Finally, the trainees of NCO education and training programs face the same challenge of integrating strategic thinking with military skills (Hornstra et al., 2023). Therefore, future research could also focus on gathering validity evidence for the TrEd ID model within the NCO education and training programs context.

5. CONCLUSIONS & ACKNOWLEDGMENT

This research offers validity evidence for the TrEd ID model as an integrated ID framework that successfully fulfills the criteria of both military skills training and academic education for officer cadets. The tenets of active learning and authenticity inherent in the TrEd ID model correspond with the key themes recognized by academic educators as pivotal to the quality of officer education. Furthermore, concerning the implementation of the TrEd ID model at a military academy, a rigorous learning approach, meaning providing military skills training and academic education in a coherent manner, and an institutional alignment with the educational policies deemed essential by the academic educators.

Acknowledgment

We thank the following academicians of the FACULTY OF MILITARY SCIENCES of the NETHERLANDS DEFENCE ACADEMY for their support in organizing this study: prof. dr. Wim Klinkert, prof. dr. Floribert Baudet, prof. dr. Lonneke Peperkamp and prof. dr. Eric-Hans Kramer.

REFERENCES

[1] Agrawal, V.K., Khanna, P., Agrawal, V.K., Hughes, L.W., Change in student perceptions of course and instructor following curriculum change. In: *Decision Sciences Journal of Innovative Education*, Vol. 18, No. 3, 2020. DOI:10.1111/dsji.12214

[2] Boeije, H., (2010). *Analysis in qualitative research*, Sage Publications, London.

[3] Bolin, G., Kalmus, V., Figueiras, R., Conducting online focus group interviews with two generations: Methodological experiences and reflections from the pandemic context. In: *International Journal of Qualitative Methods*, Vol. 22, 2023. DOI:10.1177/16094069231182029

[4] Bowling, A., (2002). *Research methods in health: Investigating health and health services*. Open University Press, Maidenhead.

[5] Britten, N., Jones, R., Murphy, E., Stacey, R., Qualitative research methods in general practice and primary care. In: *Family Practice*, Vol. 12, No. 1, 1995. DOI:10.1093/fampra/12.1.104

[6] Cook, D., Brydges, R., Ginsburg, S., Hatala, R., A contemporary approach to validity arguments: A practical guide to Kane's framework. In: *Medical Education*, Vol. 49, No. 16, 2015. DOI:10.1111/medu.12678

[7] Creswell, J.W., (2012). *Qualitative inquiry and research design: Choosing among five approaches (3rd ed.)*, Sage Publications, London.

[8] Creswell, J.W., Hanson, W.E., Clark Plano, V.L., Morales, A., Qualitative Research Designs: Selection and Implementation. In: *The Counseling*

Psychologist, Vol. 35, No. 2, 2007. DOI:10.1177/0011000006287390

[9] DUTCH DEPARTMENT OF DEFENCE (2021). *Profielschets van de officier van de Nederlandse krijgsmacht (Versie 1.0)* (Profile of the officer of the Dutch armed forces (Version 1.0)) [Report].

[10] Gagné, R.M., Briggs, L.J., Wager, W.W., (1992). *Principles of instructional design (4th ed.)*, Harcourt Brace Jovanovich College Publishers, San Diego.

[11] Gilbert, A., Tait-McCutcheon, S.L., Knewstubb, B., Innovative teaching in higher education: Teachers' perceptions of support and constraint. In: *Innovations in Education & Teaching International*, Vol. 58, No. 2, 2021. DOI:10.1080/14703297.2020.1715816

[12] Halliday, M., Mill, D., Johnson, J., Lee, K., Let's talk virtual! Online focus group facilitation for the modern researcher. In: *Research in Social and Administrative Pharmacy*, Vol. 17, No. 12, 2021. DOI:10.1016/j.sapharm.2021.02.003

[13] 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

[14] 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, 2024. https://uesit.org.ua/index.php/itse/article/view/445

[15] Jansen, M., Brænder, M., Moelker, R., (2019) What sets the officer apart? Dutch and Danish educational reforms leading to the habitus of the thinking soldier. In W. Klinkert, M. Bollen, M. Jansen, H. de Jong, E.H. Kramer, L. Vos (Eds.), *NL ARMS Netherlands annual review of military studies 2019* (337-353), T.M.C. Asser Press, The Hague. DOI:10.1007/978-94-6265-315-3_21

[16] Kane, M.T., Validating the interpretations and uses of test scores. In: *Journal of Educational Measurement*, Vol. 50, No. 1, 2013. DOI:10.1111/jedm.12000

[17] Keemink, J.R., Sharp, R.J., Dargan, A.K., Forder, J.E., Reflections on the use of synchronous online focus groups in social care research. In: *International Journal of Qualitative Methods*, Vol. 21, 2022. DOI:10.1177/16094069221095314

[18] 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

[19] Kitzinger, J.,. Qualitative research: Introducing focus groups. In: *BMJ, 311*(7000), 1995. DOI:10.1136/bmj.311.7000.299

[20] Krueger, R.A., (1994) *Focus groups: A practical guide for applied research (2nd ed.)*, Sage Publications, London.

[21] Krueger, R.A., Casey, M.A., (2009). *Focus groups, a practical guide*

for applied research (4th ed). Sage Publications, London.

[22] Larsson, S., The military academy as a civilizing institution: A historical sociology of the academization of officer education in Sweden. In: *Armed Forces & Society,* 0095327X241256127, 2024.

[23] Laufer, M., Deacon, B., Mende, M.A., Schäfer, L.O., Leading with trust: How university leaders can foster innovation with educational technology through organizational trust. In: *Innovative Higher Education,* 2024. DOI:10.1007/s10755-024-09733-5

[24] 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, 2022.

[25] Mays, N., Pope, C., Assessing quality in qualitative research. In: *BMJ*, 320, 2000. DOI:10.1136/bmj.320.7226.50

[26] Morgan, D.L., Focus groups. In: *Annual Review of Sociology,* Vol. 22, 1996.

[27] NETHERLANDS DEFENCE ACADEMY, (2021a) *Studiegids Krijgswetenschappen. Bachelor Krijgswetenschappen. Studiejaar 2021-2022 (Study guide Military Sciences. Bachelor Military Sciences. Academic year 2021-2022).* Dutch Department of Defence. https://www.defensie.nl/binaries/defensie/documenten/brochures/2021/08/30/studiegids-bachelor-krijgswetenschappen-2021-2022/STUDIEGIDS_BaKW_2021-2022.pdf

[28] NETHERLANDS DEFENCE ACADEMY, (2021b) *Studiegids Opleiding Militaire Systemen en Technologie. Academisch jaar 2021/2022. Studiejaar 2021-2022 (Study guide Military Systems and Technology. Academic year 2021-2022).* Dutch Department of Defence. https://www.defensie.nl/binaries/defensie/documenten/brochures/2021/08/30/studiegids-militaire-systemen-en-technologie-2021-2022/Studiegids+MS%26T+2021-2022.pdf

[29] Roald, G.M., Schruijer, S., Neergård, G.-B, The researcher's facilitating role in stimulating a constructive group climate in online focus-group interviews. In: *Qualitative Inquiry,* 2024. DOI:10.1177/10778004241260656

[30] Schophuizen, M., Kalz, M., Educational innovation projects in Dutch higher education: bottom-up contextual coping to deal with organizational challenges. In: *International Journal of Educational Technology in Higher Education,* Vol. 17, No. 1, 2020. DOI:10.1186/s41239-020-00197-z

[31] Shadish, W.R., Cook, T.D., Campbell, D.T., (2002) *Experimental and quasi-experimental designs for generalized causal inference,* Houghton Mifflin Company, Boston.

[32] Stalmeijer, R.E., Dolmans, D.H., Wolfhagen, I.H., & Scherpbier, A.J., Cognitive apprenticeship in clinical practice: Can it stimulate learning in the opinion of students? In: *Advances in Health Sciences Education,* Vol. 14, No. 4, 2009.

[33] 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

[34] 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

[35] 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* (pp. 183–213), Lawrence Erlbaum Associates, Mahwah.

[36] Tong, A., Sainsbury, P., Craig, J., Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups. In: *International Journal for Quality in Health Care*, Vol. 19, No. 6, 2007. DOI:10.1093/intqhc/mzm042

[37] 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 (The autumn of the military elite feeling. The elite self-image of aspiring officers at the Royal Military Academy in the period 1948 to 2008)*. [Doctoral dissertation]. Tilburg University.

[38] Victor Tillberg, L., The dynamics of military skills: The role of experience-based knowledge in challenging situations. In: *Scandinavian Journal of Military Studies*, Vol. 3, No. 1, 2020. DOI:10.31374/sjms.40

Appendix A

The TrEd ID model as an integrated five-phase ID model for skills training and academic education (Hornstra et al., 2024), based on the Nine events of instruction model (Gagné et al., 1992) and STAR Legacy (Schwartz et al., 1999a, 1999b)

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
3) Presenting	a) Trainer/Educator showing content (e.g. demonstration, presentation) b) Learners comparing content with initial skills/ideas c) Learners complementing skills/ideas by experimenting and studying
4) Practicing	a) Trainer/Educator providing guidance (e.g. discussion, tools, checklists, job aids) b) Learners practicing skills/trying out solutions c) Trainer/Educator/Learners providing feedback
5) Getting real	a) Learners performing skills/solving problems in authentic environments 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 B

Questioning route based on Krueger and Casey (2009), also applied in Stalmeijer et al. (2014)

1) Opening questions: asking for facts instead of opinions to get all the participants engaged in the discussion.

2) Introductory questions: asking open-ended questions to get participants starting to think about the topic of discussion.

3) Transition questions: asking gradually more in-depth questions to guide the discussion to the key questions.

4) Key questions: asking those questions directly related to the purpose of the study.

5) Ending questions: asking questions to get participants reflecting on their contributions and end the discussion.

Appendix C

Semi-structured interview guide

Opening questions (5 minutes)

1) Which officer cadets do you teach?

2) What do you teach the officer cadets?

Introductory questions (10 minutes)

3) What do you think are some important considerations regarding the teaching of officer cadets?

4) What do you think are some important considerations regarding instructional design?

Transition questions (10 minutes)

5) How do you typically design or structure your classes?

6) How do the officer cadets typically respond to your instructional design?

Key questions (30 minutes)

Design of the TrEd ID model

7) How do you get your officer cadets focused?
Prompts: - Getting purposefully the attention.
- Providing explicitly learning objectives.
- Providing authentic problems.

8) How do you prepare your officer cadets to learn?
Prompts: - Activating prior knowledge/skills/experiences.
- Sharing initial skills/ideas.

9) How do you present the content to your officer cadets?
Prompts: - Showing content.
- Comparing content with initial skills/ideas.
- Complementing skills/ideas by experimenting and studying.

10) How do you get your officer cadets to practice?

Prompts: - Providing guidance.
- Practicing skills/trying out solutions.
- Providing feedback.

11) How do you get your officer cadets to make the transfer of the newly learned skills and knowledge from the educational setting to the real world?
Prompts: - Performing skills/solving problems in authentic environments.
- Assessing performance/problem solving.
- Reflecting on learning process and outcomes in relation to the learning objectives.

Implementation of the TrEd ID model
12) If an integrated instructional design model would actually be used by both military trainers and academic educators at your military academy, how should it be implemented?
Prompts: - Who should use it.
- When over the course of the officer education should it be used.
- Where could it be used (e.g. in classroom, outside).
- What help should the users need to get started.
- What are the success factors.
- What are the failure factors.

Ending questions (5 minutes)
13) Is this summary of the discussion complete and correct?

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

WHAT FEEDBACK AND COACHING DO JUNIOR NAVAL OFFICERS NEED?

CDR William D. Hatch II, USN, Ret Dr. Deborah E. Gibbons

*Naval Postgraduate School, Monterey, California

This research identified crucial knowledge and skills that coaches or mentors should help Junior Officers develop in early stages of their careers. The initial phase involved interviews with subject matter experts and experienced officers to determine important attributes for junior officers' success. The research team then held focus group meetings with officers who were at various career milestones. Participants in the focus groups identified important skills that junior officers need to develop, and they shared ideas about making feedback and coaching more effective. Beyond navigation and other technical skills, participants indicated that leadership skills such as motivation, communication, and relation management are qualities of successful officers. Results suggest that better coaching in these areas could improve junior officers' competencies, with implications for the culture and future effectiveness of the services.

Key words: *Junior officers, skill-building, coaching, officer competencies*

1. INTRODUCTION

Training and retention of military officers is crucial for the continuity and success of each military service. The U.S. Navy has identified several important attributes that help modern Junior Officers (JO) succeed. These include leadership competencies, technical expertise, and personal qualities related to character, ethics, and teamwork (Naval Education and Training Command, n.d.). The U.S. Army Center for Junior Officers provides resources for JOs to develop their leadership and decision-making abilities, as well as more specific knowledge about jobs and roles. The Center emphasizes several characteristics that junior officers should develop, including transformational leadership (Plenge, n.d.a) and ability to make sound decisions under conditions of extreme uncertainty (Plenge, n.d.b). Successful Junior Officers have skills to support mission accomplishment, leading people and change, collaborating with people, and stewarding resources (DIVOLD, 2023).

Unfortunately, opportunities for Junior Officer mentoring and development are not consistent across branches of military and within particular communities. For example, the U.S. Navy has low retention of Naval Warfare Officers (officers whose main job is aboard ships). Instead of addressing root problems that led people to go elsewhere, the Navy began commissioning nearly twice as many ensigns as it needed aboard ships to address historically low retention rates of first term contract officers. The excess personnel were then assigned to share positions or find their own place aboard ship, requiring "these newbies to compete for ship driving time or other hands-on experience needed to be a good warfare officer" (Ziezulewicz, 2021). This inconsistent training can contribute to poor performance and ascorbate retention attrition. Only 33 percent of JOs remain in the community after a decade of service, compared to 45 percent of officers in other Navy communities (U.S. GAO, 2021). This situation aboard ships is a particularly egregious problem for effectiveness and retention, but more individualized coaching could be valuable to develop junior officer competencies across the breadth of military services and professions.

This study identifies key areas of learning and skill development that junior officers must achieve to be competent in their roles aboard Navy ships. Results were intended to inform training and coaching efforts by more senior Navy personnel.

1.1.General Expectations of Junior Officers

Following high-profile accidents at sea, military leaders reassessed foundational issues in the Naval Warfare community, identifying weakness in essential areas such as seamanship, watch- standing skills, teamwork, operational safety, evaluations, and professional culture (Adams, 2018). Many leaders recommended interventions to improve the Navy's at-sea competence.

Admirals Mullen and Natter (2018) focused on junior officer competencies, arguing that higher-quality training is necessary to "fix the JO career path." In particular, they emphasized seafaring and warfighting skills that are best learned through on-the-job training that builds practical skills and tacit knowledge, which they term "the sixth sense." About the same time, the Surface Warfare Officer Requirements Document (SWORD) was written to "define the competencies of a Junior Naval Warfare Officer during career progression from first tour Officer to Major Commander" (COMNAVSURFORINST

1412.4A, 2018). The document establishes milestones for Junior Warriors to build technical knowledge, skills, and abilities (KSAs) throughout their careers. It outlines the expectations and core competencies for Junior Warfare Officers (JOs) at five key career milestones: Junior Officer (0-1 to 0-3), Department Head (0-4), Executive Officer (0-5), Commanding Officer (0-5), and Major Commander (0-6). Specific competency areas include "Fight the Ship, Drive the Ship, Manage the Ship, and Command the Ship." It is worth noting that this document heavily emphasizes technical know-how that can be learned aboard a ship, via simulations, or in formal education. Leadership skills are largely outside the scope of the document.

The U.S. Government Accountability Office (2021) provided a comprehensive evaluation and noted that the U.S. Navy JO career paths deviate significantly from those in other navies. For example, the U.S. JOs are expected to become generalists, serving on various ships and in various roles, without developing high levels of proficiency in any particular role or ship. In contrast, many military services develop specialists in particular types of jobs, ships, or both. The report indicated that there is a need for improvements in training and evaluation, with the intent to improve proficiency and increase retention. Strong partnerships with senior enlisted personnel can support Junior Officer success, including frequent communication, mutual respect, willingness to learn, and alignment of goals and expectations (Talbot, 2020). Training during deployment is intended to build these crucial skills, but this often fails to occur.

1.2.A 360° Coaching Program for Junior Officers in The U.S. Navy

The U.S. Navy has a specialized learning initiative that aims to improve the leadership and operational abilities of naval officers in surface warfare positions. This program, conducted by the Surface Warfare Officers School Command (SWOSCOM), offers a comprehensive and structured approach to developing skills and knowledge in various cognitive domains. To support these efforts, instructors, mentors, and coaches need to understand the relative importance of different kinds of know-how for junior officers. The program collects assessments from bosses, peers, self, and subordinates (called 360 assessments) about how each junior officer is performing, and the school uses this feedback as a foundation for coaching. This process can help early-career JOs to understand their strengths and weaknesses because it provides feedback from multiple sources about everyone's skills, competencies, and behaviors (London & Smither, 2002). With this information, the time and resources spent in the development of JOs can be focused and more effective aboard ship and ashore. This project gathered information about what kinds of knowledge and skills the young officers should be developing. Results were intended to inform 360-degree assessment and coaching efforts. Well-trained coaches can then help each person understand the feedback and set personal goals for professional development.

2. METHODS

The work began with qualitative inputs from subject matter experts about attributes that are crucial for a young officer's success. The research team interviewed ten post command officers to obtain a broad perspective on knowledge and behaviors that should be addressed.

Finally, the team held focus group meetings with Navy personnel at various milestones in their careers. Before the meetings, participants were asked to complete a pre-survey rating the importance of a variety of knowledge and skills that are mentioned in the SWORD.

2.1. Interviews with Experts

We began by interviewing people who have extensive experience as Naval officers or trainers. The interviewers invited respondents to share whatever knowledge or skills are most important for Junior Officers.

2.2. Focus Groups

Focus group meetings were held at the Naval Postgraduate School and at the Surface Warfare Officer School. Participants at the Naval Postgraduate School were mid-level officers. Participants at SWOCOM were selected to represent all levels from Ensigns (0-1 to 0-3) receiving their first coaching to experienced coaches working at SWOCOM. The groups were sorted according to rank, and the questions were open enough to allow participants to share their thoughts about the need and process of developing knowledge and skills that are necessary for success as Junior Officers.

In total, the researchers conducted eight focus group meetings about necessary skills and knowledge for Division Officers. Seven were held at SWOSCOM in Newport Rhode

Island and one at the Naval Postgraduate School (NPS). These included a group of JO master's degree students (at NPS), two groups of new Junior Officers, two groups of Department Heads, two Prospective Executive Officer (PXO) groups, and one group of more senior officers.

Before joining the focus group meetings, participants were asked to complete a pre-survey. Prior to the focus group meetings at SWOSCOM, we sent a brief survey to participants, asking them to assess the importance of 18 JO-specific competencies at the Junior Officer level. These competencies were drawn from the SWORD (Naval Education and Training Command, n.d.). This enabled us to capture quantitative measures alongside the qualitative discussions that we held onsite at SWOSCOM.

2.2.1. Pre-survey variables

The pre-survey was conducted using Qualtrics. Variables measured in the pre-survey, including a term followed by the definition, appear below. For each item, respondents were asked how important each type of knowledge is for a junior officer, on a one to five Likert scale, and if the definition provided adequately explained the concept.

- *Drive the Ship*

Navigation: Uses available information to determine the ship's position, plan courses, and track progress and recommend course corrections as appropriate.

Seamanship: Demonstrates a basic understanding of routine ship operations, customs and courtesies, roles and responsibilities, equipment, weather, and maritime terminology.

Ship handling: Knows and anticipates how a ship behaves and what orders should be given to make the ship move correctly.

- *Manage the Ship*

Maintenance & Material Management, Engineering: Understands how to plan, schedule, and execute maintenance requirements to meet ship's standards.

Damage Control: Knows how to maintain and use appropriate equipment and procedures to prevent or minimize damage caused by adverse situations on the ship.

Combat Systems: Understands systems and procedures used to enhance situational awareness, facilitate planning and decision-making; and ensure proper command and control of weapon systems.

Supply Management: Understands how supplies and equipment are ordered, purchased, stored, and distributed on the ship in support of operations.

- *Fight the Ship*

Naval Warfare: Understands how maritime threats to the ship are detected, interdicted, and destroyed.

Ballistic Missile Defense: Understands how radar and ship missile systems are used to intercept external missile threats.

Electronic Warfare: Understands how electromagnetic and directed energy systems are used to identify and defend the ship.

Undersea Warfare: Understands the strategic, operational, and tactical use of undersea systems.

Air Warfare: Understands active and passive actions used to neutralize or destroy enemy air threats in the maritime domain.

Amphibious Warfare: Understands how amphibious ships operate close to shore when launching and supporting land-based operations.

- *Command the Ship*

Knowledge of Navy Regulations: Knows where to find required information in relevant manuals, regulations, and instructions.

Professional Development Training and Scheduling: Ensures people they lead complete necessary training and tracks training status using appropriate systems.

Leadership & Management: Be a good example of virtue, honor, patriotism, and fairness and ensure personnel assigned to you always demonstrate appropriate behavior.

Organization & Command Structure: Uses Ship Organization Regulation Manual guidance to organize and execute duties as assigned.

Planning, Briefing, Executing, Debriefing, Operational Risk Management, Safety: Creates environments in which people they lead are trained and motivated to safely accomplish their jobs.

3. RESULTS

This section of the report presents qualitative information related to important competencies and coaching for Junior Officers. To identify needed competencies, we begin by summarizing findings from a prior study about shipboard mentoring. Then we report the results of interviews with active and retired Navy Captains, as well as Naval Warfare leaders, about qualities that make Junior Officers successful. Finally, we summarize results from focus groups held to identify important competencies to address in 360 reviews and coaching of Junior Officers.

3.1. Concerns about Junior Officer Training and Mentoring

Junior Officers have expressed

concerns about the training culture and practices in their community for several years. With Sailors and officers as busy as they are on ships, many indicate that Naval officer training is rushed and does not ensure that Junior Officers acquire the foundations they need to become future expert mariners and leaders. Junior Officers have highlighted box-checking rather than ensuring thorough training, lack of accountability in understanding qualification requirements, prioritization of work over qualifications, perceived lack of rigor in earning the Naval Warfare Officer designation badge, and difficulties in conducting training due to organizational constraints (Crawford, Bowman & Hatch, 2011). In this study, some senior officers expressed a desire to revive positive aspects of the Navy's culture, emphasizing leadership and motivation. There was good training onboard some ships, but on the majority of the ships visited, personnel were stressed, frustrated, questioning the quality of junior officer training, and—in the minds of some— concerned for the future of the surface Navy.

Many junior officers and their seniors indicated that the junior officers often learn from someone who has only been in the job 6 months longer and may pass down incorrect beliefs. Mentoring by more experienced people could help with this, but very few junior officers reported having high caliber mentors. As one said, “There is no vested interest in our community for mentoring and helping us to advance in our qualifications. It’s not like other communities. We do a disservice to our future COs.” Many thought that the Naval Warfare Badge does not mean much due to the lack of rigor in the training, and they expressed interest in better mentoring that would not become another check-the-box.

3.2. SWOSCOM Leaders

SWOSCOM leaders indicated that the 360 feedback should focus on leadership, relationships, and professionalism. Based on their lengthy experience, JOs varied significantly in their competencies in these areas, and coaching could be valuable to help them improve their skills.

3.2.1. Navy Captains: What Makes a Successful Junior Officer?

During the Spring of 2022, the researchers interviewed four Naval warfare officers who had attained the rank of Navy Captain. Two were still on active duty and the others had retired from the Navy and taken civilian jobs within the Department of Defense. We asked for their frank assessments of requirements for developmental feedback at the Junior Officer level.

Key questions included:

1) Please think of a junior officer who was a top performer and model JO, in your view. What were the most important skills, competencies, or behaviors that made this person so effective as a Junior Naval Warfare officer?

2) Now think of a Junior Naval division officer who was *not* effective. What deficiencies in knowledge, competence, or behavior contributed to the officer's poor performance?

3) What 5–6 competencies or characteristics do you look for prior to deciding if a JO is ready to qualify as a Naval Warfare Officer?

These senior officers identified several important skills, competencies, or behaviors that make a Naval Warfare officer effective. Key areas of expertise included leadership and management, professional knowledge including tactical competency, and character. For example, an active- duty Navy captain recommended that early coaching should address the following: "Is the leader honest, will he or she be forthright? [*Do they demonstrate]* approachability, empathy, emotional intelligence (but not that phrase in the 360). Integrity is a non-negotiable leadership skill. Communication. Do people see them as honest, forthright, approachable, a part of the team, not just out for themselves? Operational effectiveness without leaving human wreckage in their wake, effective without destroying the team."

Asked what are the attributes of good leadership, the active-duty Captain replied:

> "The longer I'm in this business, the more I realize how important people's emotions are… Some people say, 'hey do this thing,' and others who are more effective want to understand why or there may be something else going on that prevents them from doing just that… People have feelings, and those really matter to mission accomplishment but also to their ability to be part of the team...

The SWORD includes 300 pages of spreadsheet items that are universal competencies that are desirable. How do you distill that down into something realistic? For a young JO, the most important thing is the navigation and ship handling, which applies to every ship. The leadership piece, both on the watch team and the divisional level. And the other thing is being really good at what you have been assigned to do.

Another thing, can you collaborate with your peers and make an informal team of people who can help you and you can help? Informal connections and communication. The biggest value of the 360 to the individual is [feedback on non-tangible competencies such as] "you're really good at talking people through problems. Or you need to look out when you say x because it puts people off."

A retired captain, now teaching at a Naval college, emphasized qualities such as diligence and comprehension in carrying out responsibilities. He argued that timeliness, thoroughness, and reliability reflect holistic development, and successful officers understand what people in their divisions do. "When personnel issues arise you get glimpses of the officers who engage well with their senior enlisted leadership, with chiefs and petty officers dealing with junior enlisted personnel. You get an impression of some who do not engage well with their senior enlisted leadership… Leadership is important to develop as a junior officer, but the circumstances are different in different jobs with different troops." This professor also emphasized trustworthiness and taking initiative rather than waiting to be told that something needs attention.

Another active-duty captain argued that a successful officer needs to have quick decision-making skills, which involve rapidly evaluating and assimilating information, along with critical thinking. He said that some people may struggle as leaders due to personal ego issues, but collaboration and teamwork are essential, and conflicts between competent individuals must be managed to ensure smooth operations. He emphasized the importance of treating people with respect and having a good relationship with others. Finally, he explained that understanding ship handling and tactics, knowing the ship, and being trainable in these areas are crucial. Summarizing, he said that "three-quarters of being a Naval Warfare Officer is being a good junior officer: can you lead sailors, can you manage equipment, can you manage maintenance, can you somewhat manage a budget?"

Finally, a retired captain working as a professor of military operations research emphasized knowledge, trust, and judgment, with demonstrable ability to keep the crew and ship safe. He cautioned against expecting too much of people so early in their military careers.

3.3. Focus Groups Conducted at Surface Warfare Officers School Command

- *Focus Group Pre-survey*

Thirty participants completed the pre-survey, assessing the importance of technical skills for Junior Officers using a 1 to 5 Likert scale. Average ratings for all items appear in Table 1.

Most notably, respondents ascribed the greatest importance to competencies in driving the ship and managing the ship, and the least importance to competencies related to fighting the ship.

Table 1. Importance of Junior Naval Warfare Officer-specific Competencies for Junior Officer Success

Average Importance	**Category and Specific Competencies**
	Drive the Ship
4.75	Navigation
4.46	Seamanship
4.86	Ship handling
	Manage the Ship
4.04	Maintenance & Material Management, Engineering
4.00	Damage Control
4.57	Combat Systems
3.54	Supply Management
	Fight the Ship

4.07	Surface Warfare
3.00	Ballistic Missile Defense
3.32	Electronic Warfare
3.33	Undersea Warfare
3.68	Air Warfare
3.03	Amphibious Warfare
	Command the Ship
3.82	Knowledge of Navy Regulations
3.96	Professional Development Training and Scheduling
4.36	Leadership & Management
3.54	Organization & Command Structure
4.00	Planning, Briefing, Executing, Debrief PBED, ORM, Safety

- *Focus Group Discussion Results*

Each focus group lasted from 30 to 60 minutes. Themes from these sessions are summarized below and accompanied by representative comments. Findings are presented regardless of resource implications or other circumstances.

Focus group participants generally agreed that Junior Officers have limited opportunities to engage with undersea warfare or ballistic missiles, but they must understand navigation, ship handling, leadership, and combat systems in general. Frequently mentioned topics for Junior Officer feedback included integrating information from multiple sources, communicating clearly, and applying what they have learned to real situations. Members of all groups recommended feedback about leadership behaviors, ranging from conflict management and emotional self-control to demonstrating integrity and inspiring confidence. Many emphasized the importance of working effectively with senior enlisted personnel and other functional groups aboard ship. More senior participants talked about understanding the big picture aboard ship and developing positive interpersonal skills. The junior participants expressed more confusion about what is really expected, and many seemed disappointed by the lack of learning opportunities they had experienced thus far.

The master's students came from a variety of backgrounds. Some remembered their Junior Officer 360 assessment, and many had since completed 360 reviews for subordinates or peers. Thoughts on the process varied. One person had received detailed coaching about specific areas to work on, while others could not recall receiving any coaching at all. Areas of emphasis for this group included management of people and resources. One person valued "understanding the equipment we have on the bridge and then understanding the roles and capabilities of the people." Another participant explained that Junior Naval Warfare Officers need to develop skills in "teamwork and coordination, because it's basically effectively managing everyone that's on your watch up there with you." This group helped our team fine-tune the wording for questions about technical skills that are outlined in the SWORD.

AJOC groups reported vastly different experiences aboard ship, some positive and excited about continuing their JO careers, others discouraged and intending to leave the Navy as soon as possible. Several lacked information about the purpose of 360 assessments. Some hoped to receive developmental information from their coach, but others anticipated that "they'll just tell us how much we suck." Some of the people had experienced criticism aboard ship without explanations or mentoring about how to improve. For example, one young man said "I didn't trust the command to give me proper feedback. They shuffled me around, saying that I was struggling in my first job, and it was news to me. I went on to a second tour, and I asked, 'was I doing bad', and they said no. None of them gave me feedback about what they wanted. I think it was style over substance that they wanted."

Members of the AJOC groups indicated that they need truthful feedback, "usable and timely." They recommended gathering feedback about leadership competencies and consistency. Several asked for specific guidance about areas to improve, such as "What is the one thing from this JO that is their greatest weakness and what steps could they take to improve?" and "What parts of the JO's job (admin, management, etc.) need improvement and what should they work on?" Others talked about explosive or inattentive commanding officers, and many emphasized the importance of providing feedback about how the person handles stress and treats their sailors. Some emphasized trustworthiness in accomplishing tasks, others emphasized trustworthiness in making good decisions, and still others focused on interpersonal trust.

Department Heads emphasized leadership, management, and professional development of others as key areas to be assessed. Specific themes revolved around leadership qualities, relationship-building, effective management, communication skills, decision-making abilities, and fostering a culture of trust and development within the team. When asked what types of feedback could increase the value of the 360 assessments, some said that useful feedback is actionable, with specific steps for improvement, and it helps people anticipate second and third order effects. Others emphasized professional development with guidance on how to enhance one's skills. Overall, the Department Heads valued people skills and recommended coaching that would enable Junior Officers to identify specific areas for improvement and would provide guidance on how to go about it.

The Prospective Executive Officers talked extensively about providing a good example, being attuned to the well-being of people in their group, and ensure personnel assigned to you always demonstrate appropriate behavior. The PCOs emphasized systems thinking and communication. A successful Junior Officer "knows how the various information systems coordinate and is able to extract the necessary information when needed," and "takes coordination time into account when giving commands." The PCOs recommended providing feedback about how well the junior officers apply knowledge to their jobs. One asked "do they understand the ship and drive the ship tactically in the environment, do they understand what is going on?" Another questioned "can they apply what they know to the real world?". With regard to communication, the PCOs stated that communication, both written and verbal, needs to be discussed. Particular issues included speaking to a group, providing feedback, motivating action, showing empathy, and delivering bad news.

3.4. Summary of Results

The numeric responses on pre-surveys rated ship-driving, understanding of combat systems, and leadership as most important. The discussion groups provided details particularly about crucial navigation, leadership, and combat skills. Necessary areas of feedback included integrating information from multiple sources, clear communication, and applying learned skills to real situations. Leadership behaviors such as conflict management, emotional self-control, integrity, and inspiring confidence were highlighted. Senior participants emphasized understanding the big picture and developing interpersonal skills, while junior participants expressed confusion about expectations and disappointment with learning opportunities.

Participants who had recently completed the coaching process reported varied experiences with 360 assessments and on-the-job training, highlighting the need for truthful, timely feedback and specific guidance for improvement. Department Heads and prospective Executive Officers emphasized leadership, management, communication skills, decision-making, and fostering a culture of trust. They valued actionable feedback and professional development guidance, stressing the importance of understanding and applying knowledge practically.

4. DISCUSSION AND CONCLUSIONS

This study identified crucial knowledge and skills that merit feedback and coaching for junior officers. Senior officers identified key skills and behaviors essential for a Junior Naval Warfare officer’s effectiveness, including leadership, management, professional knowledge, and character. It is important to point out that these are general skills and behaviors, so they also apply to the Air Force and the Army. The research emphasized integrity, communication, empathy, and emotional intelligence. Effective leaders are honest, approachable, and team- oriented, balancing operational effectiveness with team well-being. Officers must be diligent, reliable, and capable of quick decision-making. Building informal peer networks and receiving feedback on non-tangible competencies are vital. Trustworthiness, initiative, and respect for others are crucial for successful leadership and smooth operations. While some JOs have these qualities before they join the military, others need good role models, feedback from commanding officers, peers and subordinates. They all need coaching to improve their weaknesses and build on their strengths.

4.1. Implications for Future Force Development

Participants identified a broad range of characteristics for which junior officers need feedback and coaching. Many of these characteristics pertain to all military organizations, including communication, conflict management and trust-building, leadership and management, decision- making, and technical know-how. Those who had been through the formal coaching process recently highlighted the value of honest, timely feedback and specific improvement guidance. It was clear that existing on-the-job training and coaching have helped some people, but other JOs felt unclear about expectations and disappointed by a lack of learning opportunities. Some of these expressed a desire to leave military service as soon as possible. This disparity in on-the-job training, feedback, and coaching reveals a strong need for systematic intervention. The SWOSCOM program endeavors to provide this support for every JO. Similar programs for JOs in other militaries could likewise benefit from 360-degree feedback and coaching about their know-how and leadership behaviors.

Countries with all-volunteer militaries have the further challenge of recruiting new soldiers, sailors, and air crews, and the reputation of the service affects young people’s decision about joining. In the United States, recruitment rates vary by year and branch of service. but all branches except the Navy met recruiting goals between October, 2023, and September, 2024 (Austin, 2024). The Navy’s recruiting challenges may be partly attributed to perceptions about different quality of life as a member of the various services. One factor in quality of life is the quality of military officers. Systematic coaching, emphasizing actionable feedback and practical guidance for JOs, could strengthen the quality of leadership, morale, and performance. Beyond the obvious benefits in terms of the effectiveness and satisfaction of the service members, better leaders would create a more attractive place to work. This, in turn, could support the recruiting and retention of highly capable individuals.

REFERENCES

[1] Adams, R. (2018). Navy Begins to Implement Surface Fleet Review Recommendations. *ExecutiveGov, January 9, 2018*. Retrieved from https://executivegov.com/2018/01/navy-begins-to-implement-surface-fleet-review- recommendations/

[2] Austin, L.J. (2024). *Statement by Secretary of Defense Lloyd J. Austin III on the Fiscal Year 2024 Recruiting and Retention Report,* U.S. Department of Defense, Oct. 30,

2024.

[3]https://www.defense.gov/News/Releases/Release/Article/3951833/statement-by-secretary- of-defense-lloyd-j-austin-iii-on-the-fiscal-year-2024-re/Crawford, A.M., Bowman, W.R., & Hatch, W.D., (2011). *Training Practices for Surface Warfare Junior Officers*. Monterey, CA: Naval Postgraduate School.

[4] COMNAVSURFORINST 1412.4A, (2018). *Surface Warfare Officer Requirements Document (SWORD).*

[5] Hanisko, J. C., & Mulanax, J. A. (2021). *Surface Warfare Officer School 360-Degree Feedback Program: Evaluation of Division Officer Assessments* (MBA Professional Project). Naval Postgraduate School. Retrieved July 5, 2023, from https://apps.dtic.mil/sti/trecms/pdf/AD1150986.pdf

[6] London, M., & Smither, J. W. (2002). Feedback orientation, feedback culture, and the longitudinal performance management process. *Human Resource Management Review*, 12(1), 81-100.

[7] Mullen, M., & Natter, R. (2018). We can fix the SWO career path. *Proceedings*, 144(4). United States Naval Institute.

[8] Naval Education and Training Command. (n.d.). *Officer Candidate School*. Retrieved July 5, 2023, from https://www.netc.navy.mil/Commands/Naval-Service-Training-Command/OTCN/OCS/

[9] Plenge, C. (n.d.a). Traits of successful leaders: Be the example. *The Center for Junior Officers*. Retrieved from [https://juniorofficer.army.mil/traits-of-successful-leaders-be-the-example

[10] Plenge, C. (n.d.b). Traits of successful leaders: Mission accomplishment. *The Center for Junior Officers*. Retrieved February 12, 2025, from https://juniorofficer.army.mil/traits-of-successful-leaders-mission-accomplishment.

[11] Talbot, A. (2020). Truth #4: The Division Officer and Chief Must Form a Powerful Partnership. *Proceedings Magazine – May 2020* Vol. 146/5/1,407. Retrieved July 5, 2023, from https://www.usni.org/magazines/proceedings/2020/may/truth-4-division-officer-and- chief-must-form-powerful-partnership

[12] U.S. Government Accountability Office. (2021). *Navy readiness: Actions needed to evaluate and improve surface warfare officer career path* (GAO-21-168). https://www.gao.gov/products/gao-21-168

[13] Ziezulewicz, G. (2021). Why can’t the Navy keep its surface warfare officers? *NavyTimes*. Retrieved from https://www.navytimes.com/news/your-navy/2021/07/07/why-cant-the- navy-keep-its-surface-warfare-officers/

STRATEGIC PROFESSIONAL LEADERSHIP IN HUMAN RESOURCE MANAGEMENT TOWARD SUSTAINABLE NAVAL EDUCATIONAL INSTITUTION IN INDONESIA

A.K. SUSILO, M.B. PANDJAITAN, A. FAISOL, E.P. PUDIASTUTI

Command and Staff College, Indonesia Navy
Ciledug Raya Cipulir, Kebayoran Lama, Jakarta, Indonesia

The Indonesian Navy educational institution has the task and responsibility to form reliable and respected human resources for soldiers. However, how is strategic professional leadership in human resource management for sustainable marine educational institutions in Indonesia? This study aims to analyze the factors of strategic professional leadership in human resource management for sustainable marine educational institutions in Indonesia which are supported by the theory of strategic leadership and human resource theory.

This study is supported by a qualitative method approach that examines both documentary studies and in-depth interviews with participants who are administrators and education personnel working in Indonesian Navy educational institutions totaling 20 personnel. The results of the study indicate that twelve factors have a collective role in contributing to effective strategic professional leadership in human resource management. The twelve factors include 1) Visionary Leadership; 2) Strategic Workforce Planning; 3) Talent Acquisition and Retention; 4) Leadership Development Programs; 5) Performance Management Systems; 6) Employee Engagement; 7) Diversity and Inclusion; 8) Change Management; 9) Ethical Leadership Practices; 10) Technology Integration in HRM; 11) Sustainability-Oriented Policies; 12) Continuous Learning Culture.

Key words: *Indonesian Navy Educational Institution, Strategic Professional Leadership, Human Resource Management, Change Management.*

1. INTRODUCTION

Education based on the Basic Policy of Indonesian Navy Development is a conscious and planned effort to create a learning atmosphere and learning process so that students actively develop their potential to have spiritual religious strength, self-control, personality, intelligence, noble morals, and skills needed by themselves and society [1]. Naval educational institutions have an important role in shaping future leaders and skilled personnel of the Indonesian Navy [2].

Through a combination of classroom instruction and hands-on experience, these institutions ensure that naval personnel are not only operationally ready but also equipped with the knowledge necessary to adapt to the ever-evolving challenges in maritime security. As global security dynamics shift, this educational framework is essential to maintaining a competitive edge against adversaries, ensuring that naval forces can effectively deter aggression and respond to crises around the world [3].

For every country, education is undeniably a key mechanism to developing, promoting, and instilling ideas as knowledge to citizens and society as a whole [4]. At the beginning of the 20th century, various maritime educational institutions and other multi-level systems were opened. These institutions provided the basis for the formation of a network of naval educational institutions in Ukraine. This educational network included vocational education (navigation, engineering, artillery, maritime cadet schools) maritime and naval training. In addition, it included maritime higher educational institutions for training officers for special skills required on board ships and for service ashore. In addition, maritime higher educational institutions offered refresher courses and advanced professional training for officers. The academies of this network also provided training for fleet management personnel [5].

Strategic development and management prepare people, create people, innovate, connect access to technology, and change. This requires systematic management that uses education-driven planning to achieve success and can be transformed into practice as a procedure for problem-solving and development, identity change including cultural change that can drive [4] Navy including in Indonesia. Educational management is an important process and ongoing activity. Educational leaders are involved in operations, personnel work together seriously to achieve goals. Educational management is concerned with developing the quality of education [6].

An organization will not be able to achieve its goals without the availability of human resource factors. Especially regarding the quality of human resources, knowledge, skills, behavior, and competence that is the nature of the work, attitudes, and good relationships between personnel with operators and leaders or executives and the existence of job satisfaction [4].

The Indonesian Navy educational institution has the task and responsibility of forming reliable and respected human resources for soldiers [7]. However, how is strategic professional leadership in human resource management for sustainable marine education institutions in Indonesia?

This study aims to analyze the factors of strategic professional leadership in human resource management of sustainable marine education institutions in Indonesia supported by strategic leadership theory and human resource theory. This study is supported by a qualitative method approach that examines both documentary studies and in-depth interviews with participants who are administrators and education personnel working in TNI AL educational institutions totaling 20 personnel.

There are several contributions from this study, including: first, this study shows that integrating SHRM principles into naval educational institutions can result in better recruitment processes, better training programs, and better retention strategies. Second, the study shows that by recognizing these institutional pressures, naval educational institutions can develop HR policies that not only comply with regulations but also promote innovative practices aimed at sustainability. Third, by contributing to inclusive decision-making, by applying stakeholder theory to HR practices, naval educational institutions can ensure that diverse perspectives are considered in decision-making processes related to sustainability initiatives. Fourth, research shows that strategic professional leadership directly impacts organizational performance by aligning HR practices with the institution’s goals. This alignment ensures that the institution not only meets its immediate operational needs but also prepares for future challenges. Fifth, strategic professional leadership informs policy formulation at naval educational institutions by integrating evidence-based practices into the decision-making process. Leaders who leverage research findings can create policies that address current challenges while anticipating future needs.

2. LITERATURE REVIEW

2.1. Strategic Leadership Theory

Strategic leadership is the ability of a leader to influence and guide an organization toward achieving long-term goals while navigating a complex environment [8]. At its core, strategic leadership involves making decisions that are aligned with the organization's vision and mission, ensuring that resources are allocated efficiently to meet organizational goals [9]. This theory emphasizes the importance of foresight, adaptability, and the capacity to inspire others. Leaders who embody strategic leadership are often characterized by their ability to think critically about future trends, assess risks, and capitalize on opportunities in ways that foster sustainable growth [10].

One of the key aspects of strategic leadership is the integration of various organizational functions and processes to create a cohesive strategy [11]. Effective strategic leaders engage in continuous learning and encourage innovation within their teams, recognizing that adaptability is critical in a rapidly changing business landscape [12]. By promoting values such as transparency, accountability, and inclusiveness, strategic leaders can create an environment conducive to high performance and resilience during times of change. Ultimately, strategic leadership theory states that effective leaders are those who not only set a clear direction for their organizations but also empower their teams to contribute meaningfully to achieving shared goals [13].

2.2. Human Resource Theory

Human Resource Theory is a framework that explores human resource management in organizations, emphasizing the strategic role of employees in achieving organizational goals [14]. This theory emerged from the recognition that human capital is a vital asset that can significantly impact overall productivity and performance. The evolution of Human Resource Theory can be traced back to classical management theory, which primarily focused on efficiency and productivity [15]. However, as organizations began to recognize the importance of employee satisfaction, motivation, and engagement, the focus shifted toward understanding how to effectively manage and develop human resources [16].

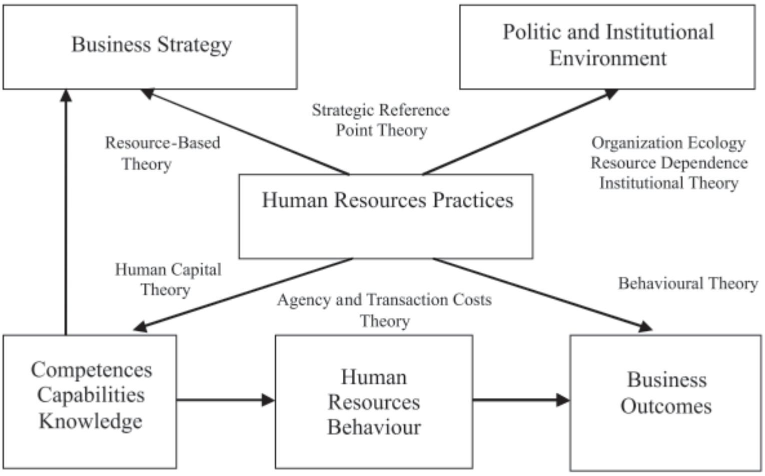

Business Strategy
Politic and Institutional Environment
Strategic Reference Point Theory
Resource-Based Theory
Organization Ecology Resource Dependence Institutional Theory
Human Resources Practices
Human Capital Theory
Agency and Transaction Costs Theory
Behavioural Theory
Competences Capabilities Knowledge
Human Resources Behaviour
Business Outcomes

Fig. 1. Theoretical approaches to Human Resources Management.
Source: McMahan, Virick & Wright [17]

One of the key aspects of Human Resource Theory is its emphasis on strategic alignment between human resource practices and organizational goals [18]. This alignment ensures that HR policies are designed not only to attract and retain talent but also to foster an environment conducive to innovation and growth. Human Resource Theory has evolved with the advancement of technology and globalization, leading to new challenges such as remote work dynamics, diversity management, and ethical considerations in HR practices [19]. The integration of data analytics into HR processes enables organizations to make informed decisions regarding employee recruitment, training, performance evaluation, and retention strategies [20]. As organizations continue to adapt to changing market conditions and workforce expectations, Human Resource Theory remains an important area of study for understanding how to best manage human capital in a manner that aligns with organizational goals and employee aspirations.

3. METHODOLOGY

This study uses a qualitative method approach that examines both documentary studies and in-depth interviews through interview questionnaires with participants who are administrators and educators working at Indonesia Navy educational institutions. The experts, a total of 20 personnel, were taken by purposive sampling and focus groups, they are a voluntary group to participate in a research project in this study which aims to analyze the strategic professional leadership of human resource management towards sustainable Indonesia Navy educational institutions from research design to data methods. Indonesia Navy educational institutions are the locus of research.

In data collection, respondents were involved to synthesizing the documentary to study the content perceived to influence the challenges of strategic professional leadership of human resource management, to conduct in-depth interviews on multi-contextual and cultural perspectives through interview questionnaires in strategic professional leadership of human resource management including the role of professional leadership, leadership in change and leadership skills, quality management, human resource management, corporate atmosphere, development along with change, creativity and creative tension, correct assessment, and participation with administrators and educators. This study uses a three-stage analysis approach, namely data reduction, data organization, and data interpretation to conclusions [4]

4. RESULT AND DISCUSSION

Strategic professional leadership in human resource management (HRM) plays a critical role in ensuring the sustainability and success of naval educational institutions. These institutions require a unique blend of leadership strategies that align with their mission, vision, and operational goals. Strategic professional leadership in HRM results in a sustainable educational organization based on several factors. These twelve factors collectively contribute to effective strategic professional leadership in HRM that aims to drive sustainable development in naval educational institutions by effectively aligning organizational goals with human capital strategies over time. These factors include:

a. Visionary Leadership.

A clear and forward-looking vision is essential to guide an institution towards long-term sustainability [21]. Strategic leaders combine managerial leadership—sensitive to the past—and visionary leadership—future-oriented [22]. Leaders must articulate a compelling vision that aligns with the goals of the institution and inspires stakeholders. The emphasis on visionary leadership in the systemic adoption of learning analytics aligns with the arguments put forward [23].

Without visionary leadership, no action can be taken at any level to motivate soldiers in any organization, because the greatest task of visionary and active leadership is those work hard to understand the professional, psychological, social, and physical needs of soldiers for better results as expected [24].

b. Strategic Workforce Planning

Effective workforce planning ensures that the right personnel are recruited, trained, and retained to meet the current and future needs of the organization. HR departments can make more informed decisions about workforce planning, talent management, and overall organizational strategy by leveraging data and analytics to better understand employee behaviors, attitudes, and performance [25]. In the planning context, enabling services to successfully align their staff competencies and activities with population needs and service goals, helps to identify gaps in knowledge skills and performance gaps [26] and enhances HR operations with digital technology and models will enhance strategic workforce planning, learning, and performance management capabilities [25].

c. Talent Acquisition and Retention

Attracting and retaining highly skilled professionals is critical to maintaining high standards in education and training within naval institutions. Uncovering the strategic value-added expected from educational institutions from both talent acquisition [27] and economic perspectives requires a multidimensional and time-consuming study due to the nature of such educational institutions. Talent management is critical for businesses, which are immature but profitable. Steady growth is seen globally in international organizations, but talent acquisition and management are yet to meet international standards [28]. It is important to empower HR professionals to make data-driven decisions throughout the talent management process by enabling the evaluation of objective and subjective factors that influence talent acquisition and retention [29].

d. Leadership Development Programs

Developing future leaders in organizations ensures leadership sustainability. Structured programs that focus on leadership skills, decision-making, and adaptability are essential to sustaining institutional growth [30]. Learning programs should be designed to provide opportunities for continuous trial and error learning. Thus, effective strategic leadership development programs should include deliberate practice [31]. Educational institutions have the opportunity to incorporate skills, abilities, and habits associated with reflective learning and contextual responsiveness into leadership development programs [32] as does the Indonesian Navy. Integrating the above principles into strategic leadership development activities can begin with classroom training on a specific subject [31].

e. Performance Management Systems

Performance Management is generally part of a broader strategy that encompasses the entire division or organization and focuses on its goals [33]. Good governance of educational institutions raises issues about creating better organizational value that involves strategic management, and performance management [34]. Performance management helps organizations ensure that workers work with full ambition to contribute to achieving the organization's main goals and objectives. However, performance management sets the desire for employee performance and motivates employees to work hard in a way that is reasonable for the organization [35].

f. Employee Engagement

Engaged educators and administrators are more committed to their roles and the mission of the institution. The conceptualization of work engagement has been challenged by early groups, such as personal engagement and burnout engagement, and later groups, such as employee engagement [36]. Human resource executives worldwide understand that motivational factors influence employee engagement and retention [37]. Employee engagement is conceptualized as a multidimensional concept involving physical (behavioral), cognitive (trait), and emotional (state) components [38].

g. Diversity and Inclusion

Promoting diversity in the workforce ensures a variety of perspectives that can lead to innovative solutions to the challenges faced by naval educational institutions. Inclusive policies encourage collaboration and mutual respect [39]. An inclusive environment ensures that every student feels valued and supported, which is critical to their academic success and personal development [40]. Cultivating an inclusive culture encourages empathy, respect, and understanding among fellow students, which are essential skills in today's diverse society.

h. Change Management

Change management involves overcoming barriers related to people's mindsets and processes. Developing a new culture toward a data-driven approach requires as much effort as any other change management initiative [41]. Naval educational institutions often face dynamic challenges that require the ability to adapt to change. Change management involves a variety of techniques, forces, tools, and approaches that build, reinvent, reorganize, and rebuild systems and structures to enact and leverage change, all the way to the functional level [42]. The change management process shifts the focus of top-level managers from control to learning. As this process progresses, the roles of different managers change from missionaries who sell the basic idea, through consultants and coordinators who teach and support employees, to team leaders who sustain the change [43].

i. Ethical Leadership Practices

Maintaining high ethical standards builds trust among employees, students, and other stakeholders. Ethical leadership has been represented in the HRD literature and is also listed in classifications [44]. Ethical practices ensure transparency, fairness, and integrity in the decision-making process. The core of the ethical leadership compass Perhaps the most promising orientation toward the ethical leadership compass has emerged from the work of scholars working within the traditions of two value-based leadership theories with a focus on authenticity and integrity in the leader, and on inspiring idealized, high-level goals and objectives for followers [45].

j. Technology Integration in HRM

Technology integration in educational institutions has become a critical aspect of modern pedagogy, transforming the way educators deliver content and engage students [46]. The integration of digital tools and resources enables personalized learning experiences that cater to the varying needs and learning styles of students [47]. The shift from traditional teaching methods to technology-enhanced teaching not only increases student engagement but also prepares learners for a technology-driven future [48].

k. Sustainability-Oriented Policies

Sustainability-oriented policies in educational institutions are essential for fostering an environmentally conscious culture among students and staff [49]. These policies often encompass a range of initiatives, including integrating sustainability into the curriculum, promoting sustainable campus operations, and forming partnerships with local communities to address environmental challenges [50]. Incorporating sustainability into HR policies ensures alignment with broader environmental goals while promoting responsible resource use [51] in naval educational institutions. Ultimately, sustainability-oriented policies in educational settings play a critical role in shaping a more sustainable future by empowering individuals and encouraging collective action toward environmental stewardship.

l. Continuous Learning Culture

A culture of continuous learning in educational institutions is essential to fostering an environment that allows students and educators to thrive [52]. Encouraging lifelong learning among educators ensures that they remain informed about best practices in educational delivery methods or technical advancements relevant to naval operations. Fostering a culture of continuous learning requires a strong leadership commitment from educational administrators who prioritize the professional development of educators [53]. As educators embrace new pedagogical strategies and technologies, they inspire their students to adopt the same attitude toward their education, creating a vibrant community dedicated to growth and improvement [54].

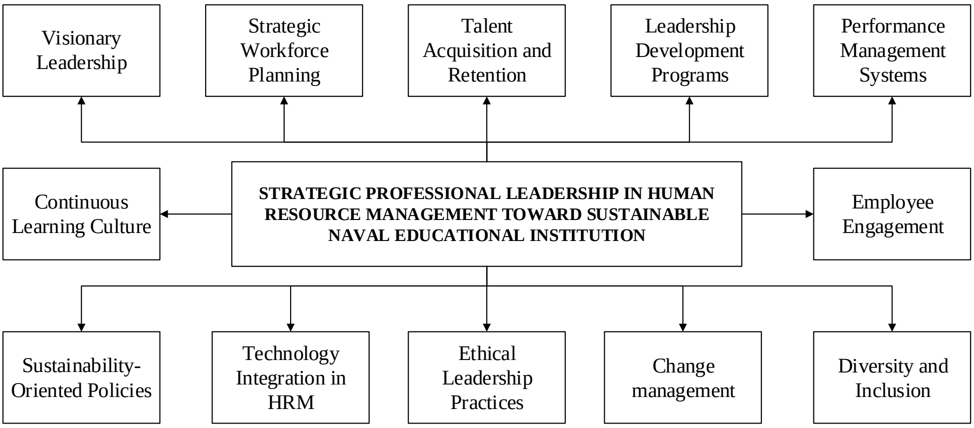

Visionary Leadership
Strategic Workforce Planning
Talent Acquisition and Retention
Leadership Development Programs
Performance Management Systems
Continuous Learning Culture
STRATEGIC PROFESSIONAL LEADERSHIP IN HUMAN RESOURCE MANAGEMENT TOWARD SUSTAINABLE NAVAL EDUCATIONAL INSTITUTION
Employee Engagement
Sustainability-Oriented Policies
Technology Integration in HRM
Ethical Leadership Practices
Change management
Diversity and Inclusion

Fig. 2. Factors of Strategic Proffessional Leadership in Human Resources Management toward Sustainable Naval Education Institution.

Implication

This study offers significant theoretical implications that can enhance understanding of the dynamics of leadership and organizational sustainability. One key implication is the integration of strategic HRM theory with the leadership framework, which suggests that effective leadership is not just about managing people but also about aligning human resource practices with broader institutional goals. By adopting a strategic approach to HRM, naval educational institutions can foster an environment that prioritizes continuous learning, innovation, and adaptability to navigate the complexities of modern maritime education.

The findings suggest that when leaders engage in strategic human resource management practices, they not only improve operational efficiency but also promote ethical standards and social responsibility within the institution. This dual focus on performance and ethics aligns with contemporary theories of sustainable leadership, which advocate a holistic approach to education that prepares future naval professionals to address global challenges while upholding the values of integrity and service.

As a practical implication, by integrating strategic HR practices, leaders can align institutional goals with broader sustainability objectives, ensuring that resources are used efficiently while promoting a culture of continuous improvement. This alignment not only enhances the quality of education provided but also prepares future naval professionals to meet the evolving demands of maritime operations and environmental management. The emphasis on sustainable practices in HR fosters a workforce that is not only skilled but also environmentally conscious and socially responsible. This approach equips graduates with the competencies necessary to address contemporary issues such as climate change and resource scarcity in naval operations.

5. CONCLUSION

Strategic professional leadership in human resource management is essential for the sustainability and success of Indonesian naval educational institutions, which is in line with the mission, vision, and operational goals. This study aims to analyze strategic professional leadership in human resource management towards sustainable marine educational institutions in Indonesia supported by strategic leadership theory, and human resource theory. The results of the study indicate that twelve factors have a collective role in contributing to effective strategic professional leadership in human resource management.

The twelve factors include 1) Visionary Leadership; 2) Strategic Workforce Planning; 3) Talent Acquisition and Retention; 4) Leadership Development Programs; 5) Performance Management Systems; 6) Employee Engagement; 7) Diversity and Inclusion; 8) Change Management; 9) Ethical Leadership Practices; 10) Technology Integration in HRM; 11) Sustainability-Oriented Policies; 12) Continuous Learning Culture

This study presents several avenues for future inquiry. First, the impact of transformational leadership styles on faculty and staff engagement, retention, and performance in these institutions. Investigating how different leadership approaches can foster a culture of sustainability and innovation could yield valuable insights into improving organizational effectiveness. Second, future research could examine the role of strategic HR practices in aligning institutional goals with national defense objectives, particularly as they relate to maritime security and environmental stewardship. This alignment is essential to developing a workforce that is not only skilled but also committed to sustainable practices. Third, another promising direction for future research lies in the integration of technology and digital tools into HR strategies at naval educational institutions. As the educational landscape continues to evolve with technological advancements, understanding how these tools can be leveraged to improve leadership effectiveness and HR processes will be important.

ACKNOWLEDGEMENT

This study was supported by Naval Staff and Command College. Appreciation and sincere thanks to all leaders of the Indonesian Navy. Researchers would like to thank all parties who have participated in completing and supporting the implementation of this research so that it can be completed smoothly.

REFERENCES

[1] O. Wiyono, B. Nurakhim, and G. J. Kiswara, "Implementasi Komponen Pendidikan terhadap Penyelenggaraan Program Studi Strategi Operasi Laut Program Magister Terapan di Seskoal," Sosio e-kons, vol. 12, no. 1, pp. 78–88, 2020.

[2] I. Isnadi, S. Suparno, I. N. Putra, and B. Sukandari, "Strategic Planning of Information and Technology Systems of Indonesian Naval Academy," Journal Asro, vol. 9, no. 2, p. 48, 2018, doi: 10.37875/asro.v9i2.77.

[3] R. Megargee, "History and Military Education," Naval War College Review, vol. 30, no. 4, pp. 3–15, 1978.

[4] P. Jedaman, S. Kenaphoom, and B. Jongmuanwai, "Strategic Professional Leadership of Human Resource Management towards Sustainable Educational Organizations, Thailand: A Recent Study," Current Research in Language, Literature and Education Vol. 4, vol. 11, pp. 30–42, 2022, doi: 10.9734/bpi/crlle/v4/2736c.

[5] P. F. Doe, "Stages of Naval Education Development in Ukraine (the 18th Century-Latter Half of the 20th Century)," Journal of Advocacy, Research and Education, vol. 5, no. 1, pp. 23–27, 2018.

[6] P. Jedaman, K. Buaraphan, P. Pimdee, C. Yuenyong, A. Sukkamart, and C. Suksup, "Analysis of sustainable leadership for science learning management in the 21st Century under education THAILAND 4.0 framework," in AIP conference proceedings, 2018, vol. 1923, no. 1.

[7] H. Suprianto, "Pengaruh Motivasi Dan Pengalaman Kerja Di Komando Pembinaan Doktrin Pendidikan Dan Latihan Angkatan Laut (Kodiklatal) Surabaya," Jurnal Manajerial Bisnis, vol. 1, no. 1, pp. 1–13, 2017, [Online] Available: http://www.jurnal.uwp.ac.id/pps/index.php/mm/article/view/20.

[8] B. J. Davies and B. Davies, "Strategic leadership," School Leadership and Management, vol. 24, no. 1, pp. 29–38, 2004, doi: 10.1080/1363243042000172804.

[9] W. G. Rowe, "Creating wealth in organizations: The role of strategic leadership," Academy of Management Executive, vol. 29, no. 4, pp. 25–37, 2001.

[10] B. Davies and B. J. Davies, "Strategic Leadership," International Encyclopedia of Education, Third Edition, pp. 34–39, 2009, doi: 10.1016/B978-0-08-044894-7.00447-4.

[11] R. Strand, "Strategic Leadership of Corporate Sustainability," Journal of Business Ethics, vol. 123, no. 4, pp. 687–706, 2014, doi: 10.1007/s10551-013-2017-3.

[12] A. A. Jaleha and V. N. Machuki, "Strategic Leadership and Organizational Performance: A Critical Review of Literature," European

Scientific Journal ESJ, vol. 14, no. 35, 2018, doi: 10.19044/esj.2018.v14n35p124.

[13] F. Kılıç, “The Role of Strategic Leadership in Innovation Performance,” Open Journal of Business and Management, vol. 10, no. 02, pp. 654–669, 2022, doi: 10.4236/ojbm.2022.102037.

[14] M. Misbah and Budiyanto, “Strategic Human Resources Management to Challenges of the Society Era 5.0,” International Conference on Business and Social Sciences (ICOBUSS) Surabaya, pp. 724–733, 2020.

[15] S. Fowler, “Toward a New Curriculum of Leadership Competencies: Advances in Motivation Science Call for Rethinking Leadership Development,” Advances in Developing Human Resources, vol. 20, no. 2, pp. 182–196, 2018, doi: 10.1177/1523422318756644.

[16] H. Karaxha, H. Karaxha, and B. Ramosaj, “The Role of the Motivation in Changes and Performance Assessment of the Managerial Staff in Kosovo Businesses,” European Scientific Journal, ESJ, vol. 14, no. 7, p. 224, 2018, doi: 10.19044/esj.2018.v14n7p224.

[17] I. Peña, G. Pardo, and V. Fernández, “Looking into the black-box : analysis of the effectiveness of human resources strategy,” Zbornik radova Ekonomskog fakulteta u Rijeci: časopis za ekonomsku teoriju i praksu, vol. 27, pp. 31–56, 2009.

[18] K. Malkamäki, E. Hiltunen, and E. Aromaa, “The Role of Trust in the Strategic Management Process: A Case Study of Finnish Grocery Retail Company Kesko Ltd,” South Asian Journal of Business and Management Cases, vol. 10, no. 1, pp. 21–34, 2021, doi: 10.1177/22779779211006801.

[19] P. N. Figueiredo and J. Piana, Technological learning strategies and technology upgrading intensity in the mining industry: evidence from Brazil, vol. 46, no. 3. Springer US, 2021.

[20] M. E. L. K. Widjaja, “Strategic Orientation and Human Resources Management in Public Sector Organizations in the Society 5.0 Era,” Proceedings of the 18th International Symposium on Management (INSYMA 2021), vol. 180, no. Insyma, 2021, doi: 10.2991/aebmr.k.210628.039.

[21] K. Piwowar-Sulej and Q. Iqbal, “Leadership styles and sustainable performance: A systematic literature review,” Journal of Cleaner Production, vol. 382, no. October 2022, p. 134600, 2023, doi: 10.1016/j.jclepro.2022.134600.

[22] D. Vera and M. Crossan, “Strategic leadership and organizational learning,” Academy of Management Review, vol. 29, no. 2, pp. 222–240, 2004, doi: 10.5465/AMR.2004.12736080.

[23] D. Gasevic, “How do we start ? An approach to learning analytics adoption in higher education,” The International Journal of Information and Learning Technology, vol. 36, no. 4, pp. 342–353, 2019, doi: 10.1108/IJILT-02-2019-0024.

[24] Z. Sahito and P. Vaisanen, “A narrative analysis of teacher educators’ motivation: Evidence from the universities of sindh, pakistan,” Journal of Language Teaching and Research, vol. 10, no. 4, pp. 673–682, 2019, doi: 10.17507/jltr.1004.02.

[25] S. Verma, N. Rana, and J. R. Meher, “Identifying the enablers of HR digitalization and HR analytics using ISM and MICMAC analysis,” International Journal of Organizational Analysis, 2023, doi: 10.1108/IJOA-01-2023-3611.

[26] J. A. Mills, A. Cieza, S. D. Short, and J. W. Middleton, “Development and Validation of the WHO Rehabilitation Competency Framework: A Mixed Methods Study,” Archives of Physical Medicine and Rehabilitation, vol. 102, no. 6, pp. 1113–1123, 2021, doi: 10.1016/j.apmr.2020.10.129.

[27] E. Caymaz, “Strategic Management of the Defense Industry: A Review on Clustering Strategy,” Journal of Defence Resources Management, vol. 24, no. April, 2022.

[28] M. Damle and B. Krishnamoorthy, “Identifying critical drivers of innovation in pharmaceutical industry using TOPSIS method,” MethodsX, vol. 9, p. 101677, 2022, doi: 10.1016/j.mex.2022.101677.

[29] R. Salehzadeh and M. Ziaeian, “Decision making in human resource management: a systematic review of the applications of analytic hierarchy process,” Frontiers in Psychology, vol. 15, no. August, pp. 1–18, 2024, doi: 10.3389/fpsyg.2024.1400772.

[30] E. F. Goldman, A. R. Scott, and J. M. Follman, “Organizational practices to develop strategic thinking",” Journal of Strategy and Management, vol. 8, no. 2, pp. 155–175, 2015, [Online]. Available: https://www.emeraldgrouppublishing.com/journal/jsma?id=JSMA.

[31] Z. Norzailan, R. B. Othman, and H. Ishizaki, “Strategic leadership competencies: what is it and how to develop it?” Industrial and Commercial Training, vol. 48, no. 8, pp. 394–399, 2016, doi: 10.1108/ICT-04-2016-0020.

[32] J. Kuntz, J. H. K. Wong, and S. Budge, “Motive, mindset and opportunity: exploring leader ambidexterity factors in health-care,” Learning Organization, vol. 30, no. 3, pp. 355–374, 2023, doi: 10.1108/TLO-12-2022-0153.

[33] M. Tanveer and A. M. Karim, “Higher education institutions and the performance management,” Library Philosophy and Practice, no. 1, pp. 1–22, 2018.

[34] B. Tjahjadi, N. Soewarno, E. Astri, and H. Hariyati, “Does intellectual capital matter in performance management system-organizational performance relationship? Experience of higher education institutions in Indonesia,” Journal of Intellectual Capital, vol. 20, no. 4, pp. 533–554, 2019, doi: 10.1108/JIC-12-2018-0209.

[35] Z. Y. Ying, “The Impact of Performance Management System on Employee performance,” vol. 02, no. 03, p. 57, 2012.

[36] H. Wittenberg, G. Eweje, N. Taskin, and D. Forsyth, “Different perspectives on engagement, where to from here? A systematic literature review,” International Journal of Management Reviews, vol. 26, no. 3, pp. 410–434, 2024, doi: 10.1111/ijmr.12361.

[37] M. Hassan, M. Jambulingam, M. N. Alam, and S. Islam, “Redesigning the retention strategy against the emerging turnover of Generation Y: Revisiting the

long-standing problems from 20Th to 21St century," Journal of Legal, Ethical and Regulatory Issues, vol. 23, no. 2, pp. 1–16, 2019.

[38] A. O. Ojo, O. Fawehinmi, and M. Y. Yusliza, "Examining the predictors of resilience and work engagement during the covid-19 pandemic," Sustainability (Switzerland), vol. 13, no. 5, pp. 1–18, 2021, doi: 10.3390/su13052902.

[39] C. C. Miller, S. S. C. Chiu, C. L. Wesley, D. Vera, and D. R. Avery, "Cognitive Diversity At the Strategic Apex: Assessing Evidence on the Value of Different Perspectives and Ideas Among Senior Leaders," Academy of Management Annals, vol. 16, no. 2, pp. 806–852, 2022, doi: 10.5465/annals.2020.0387.

[40] A. Joshi, "Legal Empowerment and Social Accountability: Complementary Strategies Toward Rights-based Development in Health?," World Development, vol. 99, pp. 160–172, 2017, doi: 10.1016/j.worlddev.2017.07.008.

[41] R. C. Reddy, D. Mishra, D. P. Goyal, and N. P. Rana, "A conceptual framework of barriers to data science implementation: a practitioners' guideline," Benchmarking, 2023, doi: 10.1108/BIJ-03-2023-0160.

[42] L. Etareri, L. Review, and L. Review, "An Analysis Framework of Change Management," Medicon Engineering Themes, vol. 3, no. 1, pp. 30–38, 2022, doi: 10.55162/mcet.03.056.

[43] A. Loku and N. Loku, "The correlation between quality change management and process implementation with financial and non-financial market performance in south-eastern Europe companies," Asian Economic and Financial Review, vol. 13, no. 8, pp. 533–546, 2023, doi: 10.55493/5002.v13i8.4816.

[44] J. R. Turner and R. Baker, "A review of leadership theories: identifying a lack of growth in the HRD leadership domain," European Journal of Training and Development, vol. 42, no. 7–8, pp. 470–498, 2018, doi: 10.1108/EJTD-06-2018-0054.

[45] M. T. Jones and C. C. J. M. Millar, "About Global Leadership and Global Ethics, and a Possible Moral Compass: An Introduction to the Special Issue," Journal of Business Ethics, vol. 93, no. SUPPL. 1, pp. 1–8, 2010, doi: 10.1007/s10551-010-0622-y.

[46] J. West and M. J. Malatji, "Technology Integration in Higher Education: The use of Website Design Pedagogy to Promote Quality Teaching and Learning," Electronic Journal of e-Learning, vol. 19, no. 6, pp. 629–641, 2021, doi: 10.34190/ejel.19.6.2557.

[47] F. A. Inan and Æ. D. L. Lowther, "Factors affecting technology integration in K-12 classrooms : a path model," pp. 137–154, 2010, doi: 10.1007/s11423-009-9132-y.

[48] G. Falloon, "From digital literacy to digital competence: the teacher digital competency (TDC) framework," Educational Technology Research and Development, vol. 68, no. 5, pp. 2449–2472, 2020, doi: 10.1007/s11423-020-09767-4.

[49] P. B. de O. Claro and N. R. Esteves, "Sustainability-oriented strategy and sustainable development goals," Marketing Intelligence &

Planning, vol. 39, no. 4, pp. 613–630, 2021.

[50] T. Schubert, H. Kroll, and C. G. Chavez, “The effects of sustainability orientation on research and teaching efficiency in German universities,” Socio-Economic Planning Sciences, vol. 88, p. 101676, 2023.

[51] C. F. Gohr, C. R. de S. Torres, and W. G. Lira, “Dynamic capabilities and sustainability-oriented innovations in higher education institutions: a case study,” Gestão & Produção, vol. 30, p. e4223, 2023.

[52] M. Babbar and T. Gupta, “Response of educational institutions to COVID-19 pandemic: An inter-country comparison,” Policy Futures in Education, vol. 20, no. 4, pp. 469–491, 2022.

[53] M. Alenezi, “Deep dive into digital transformation in higher education institutions,” Education Sciences, vol. 11, no. 12, p. 770, 2021.

[54] C.-Y. Lin and C.-K. Huang, “Employee turnover intentions and job performance from a planned change: the effects of an organizational learning culture and job satisfaction,” International journal of manpower, vol. 42, no. 3, pp. 409–423, 2021.

LEADERSHIP ACCOUNTABILITY AND ETHICAL DECISION-MAKING

Narine KARAPETYAN

General Department of Personnel, Ministry of Defense of Armenia

> *"A man of character in peace is a man of courage in war. Character is a habit, the daily choice of right and wrong. It is a moral quality which grows to maturity in peace and is not suddenly developed in war".*
>
> **General Sir James *Glover***

This article explores the critical intersection of military leadership accountability and ethical decision-making, emphasizing the profound implications of leaders' choices on personnel and society. It argues that ethical decision-making is an integral aspect of military leadership, rather than a separate concern, and advocates for an interactionist perspective that considers the dynamic interplay of leadership, character, and situational factors. The discussion delves into the necessity of holding military leaders accountable for their actions and decisions, outlining mechanisms for enforcing accountability, including internal oversight, military courts, command responsibility, and transparency. The importance of ethical training for military leaders is underscored, highlighting various ethical frameworks that guide decision-making in complex situations. The article also examines the ethical dilemmas faced by military leaders and the impact of situational factors on moral choices. Ultimately, it posits that fostering a culture of ethical decision-making within military leadership is essential for maintaining trust, integrity, and operational effectiveness.

Key words: *military leadership, ethical decision-making, accountability, ethical training, leadership theories, moral dilemmas, transparency, military ethics, command responsibility, ethical frameworks.*

1. INTRODUCTION

Leadership in the military is an essential aspect of ensuring operational success and maintaining morale among personnel. The decisions made by military leaders, especially in times of conflict or crisis, can have profound consequences for both their troops and society. Ethical decision-making in military leadership is particularly critical because of the high stakes involved, including loss of life, national security, and the well-being of soldiers and civilians.

Leadership and ethics are habitually treated as related to separate spheres. It would be better, perhaps, if leadership and ethics were treated as belonging to a single domain. Ethics is an aspect of leadership and not a separate approach that exists alongside other approaches to leadership such as the trait approach, the situational approach, etc. This holds especially true for the military, one of the few organizations that can legitimately use violence. Today, most militaries opt for a character-based approach for the ethics education of their leaders and espouse leadership theories that want leaders to be strong and visionary. Both the role of character and leadership are increasingly questioned, however, on the basis that situational factors are more influential than leadership and character. A closer look suggests that an interactionist perspective, with leadership, character, and the situation interplaying, is more accurate. As Codreanu highlights (2019) leaders must be aware "… that oblivion of minor covert details concerning integrity transgressions triggers the most appalling disasters". Therefore, it is still good leadership that keeps soldiers from crossing the line between the lawful use of force and excessive violence.

Such intersection of military leadership accountability and ethical decision-making, focusing on the role of military leaders in guiding their units, making ethical choices, and being held accountable for their actions. It will delve into key concepts, theories, and real-world examples that highlight the importance of ethical decision-making and leadership accountability in the military.

2. WHY AND HOW MILITARY LEADERSHIP SHOULD BE HELD ACCOUNTABLE

Military leadership can be defined as the act of guiding individuals or groups of military personnel to achieve mission objectives, maintain discipline, and foster unit cohesion. A good military leader possesses technical expertise, emotional intelligence, and an ability to inspire and guide others under challenging circumstances. Effective leadership ensures that soldiers are not only equipped with the necessary skills but also motivated and prepared to perform tasks efficiently and responsibly. The essence of military leadership lies in its ability to enforce the chain of command, build trust, and make decisions that are in the best interest of the mission, troops, and national security.

Accountability in military leadership refers to the obligation of military leaders to answer for their actions and decisions, particularly when those decisions have far-reaching consequences. A leader is accountable not only for their personal conduct but also for the performance of their unit or team. This accountability is enforced through military justice systems, which investigate breaches of conduct and ensure that responsible parties face appropriate consequences.

Military accountability is essential because it helps maintain order, discipline, and trust within the armed forces. It also ensures that leaders remain transparent and answerable for their actions. Ethical lapses or misconduct by military leaders can undermine public trust in the military and its mission. Therefore, holding leaders accountable is critical to maintaining the ethical standards of the profession.

Within the military, accountability is typically enforced through several mechanisms, for example ***internal oversight*** when military leaders are often subject to internal review processes, such as investigations and tribunals, to assess whether their actions meet the expected ethical and legal standards, or ***Military Courts*** in cases of serious misconduct or violations of military law, leaders can be tried by military courts, where they may face penalties ranging from reprimands to court martial. ***Command responsibility*** can also be an effective mechanism for ensuring accountability were higher-ranking officers are often held accountable for the actions of the personnel under their command. This principle ensures that leaders remain vigilant about the behavior of their subordinates and finally most critical ones such as ***transparency and reporting.*** Transparency in military accountability is a key principle for ensuring that military operations, actions, and decisions are subject to scrutiny, oversight, and responsibility. This concept helps maintain public trust, upholds human rights, and reduces the risk of abuses of power or unethical behavior. Transparency involves documenting and reporting military activities, such as combat operations, peacekeeping missions, and logistical support, to ensure that actions are understood and can be examined by oversight bodies. This may include making public key outcomes of military missions, casualty reports, and operational objectives or allow civilian oversight of military forces. This could involve independent committees, auditors, or government representatives who can assess military actions and decisions. These oversight bodies act as checks on military power and ensure that military leaders are held accountable to legal and ethical standards. In this context it would be also appropriate to note ***external oversight by International bodies*** like the United Nations, International Criminal Court, and human rights organizations often play a role in holding military forces accountable for actions that may violate international law, such as war crimes or human rights violations. Transparency helps ensure that military forces are not operating above the law.

Transparency is often enhanced by ***public access to information*** about military actions and policies is essential for transparency. This includes providing the public with insight into defense budgets, weapons systems procurement, and military strategies, though certain sensitive information may be withheld for national security reasons. In summary, military accountability through transparency is essential for ensuring that military forces operate ethically, lawfully, and responsibly. It also serves to protect the rights of civilians and maintain the integrity of the military institution. *Accountability in military leadership is necessary to uphold standards of conduct and ensure that leaders are responsible for their actions. An absence of accountability can lead to abuses of power, loss of trust, and even detrimental effects on military operations.*

3. IMPORTANCE OF ETHICAL DECISION-MAKING IN MILITARY LEADERSHIP

Ethics, ethical behavior, ethical decision-making, and ethical leadership are important terms and concepts in today's world. All possible relations, behaviors and responsibilities – what can and should or even must be done, and what not – cannot be included in formal regulations. In the grey zone of non-existent regulations people behave according to their values, knowledge and skills, personal characteristics, or in general: their ethics. *Ethics is a set of moral principles – a theory or system of moral values. It is the principles of conduct governing an individual or a group. It is a consciousness of moral importance, and a guiding philosophy.* Ethics can also be defined as a set of moral issues or aspects (such as rightness), and the discipline dealing with what is good and bad, and with moral duty and obligation (Merriam Webster Dictionary). It is interesting to note that the relationship between the military and ethics is not one-dimensional. While many authors and practitioners claim that ethics must be an important part of military work and military leadership, and of military organization in general, some see ethics and the military as incompatible, and the term military ethics as an oxymoron (Cook, 2015, p 36). However, Cook (2015, p 33–34) claims the opposite and gives some explanations: that there is no question that the military is oriented towards the public good; that military professionals consider the principle of discrimination (they discriminate between those who are enemy combatants and those who are noncombatants); that the duty of military officers is to take upon themselves any danger that the conflict introduces to noncombatants; and that military professionals must act proportionally – judgements must be made by a competent military authority on a case-by-case basis, and so on. The dangers of killing and being killed are additional strong factors in ethical military behavior.

Incidents involving military personnel testify to the importance of ethics in the military. The My Lai Massacre ((Vietnam War) (one of the most infamous ethical failures in military history)) in 1968, The Abu Ghraib prison scandal in 2003, the Haditha killings in 2005, the killing of 39 civilians by Australian Special Forces in Afghanistan between 2005 and 2016 is a recent example of such an incident. Failing leadership played an important role in these examples, in the case of Abu Ghraib especially at the senior level. In all these cases, the victims were outsiders to the organization. But militaries also have to deal with serious misbehavior among military personnel in units that are not deployed and in that part of the military organization that is never directly involved in combat. Also in such cases of misbehavior military leaders are sometimes part of the problem. But peacetime incidents notwithstanding, it is because the military is one of the rare organizations that can legitimately use violence and that its leaders hence have to lead personnel that have used or experienced violence, which explains why leadership is so important in the military. There is a rapidly growing body of literature on military ethics, military leadership, and the ethics of military leadership that wants to contribute to a better understanding of the ethical challenges for military leaders but that also wishes to help the military leaders that actually face those challenges. Military ethics exists to be of service to professionals who are not themselves specialists in ethics but who have to carry out the tasks entrusted to the profession as honorably and correctly as possible.

It is analogous to medical ethics or legal ethics in the sense that its core function is to assist those professions to think through the moral challenges and dilemmas inherent in their professional activity.

In real life ethics is, in the military and elsewhere, an important aspect of leadership and not a separate approach that exists alongside other approaches such as the trait approach, the situational approach, etc. Now, the last few decades did bring a number of leadership theories that profess to be ethical, such as transformational, authentic, spiritual, and servant leadership. It remains somewhat elusive, however, what exactly the ethical element of these theories consists of. Paying lip service to the importance of values does not make these modern leadership theories more ethical. Ethical decision-making involves evaluating situations through a lens that upholds moral values, principles, and standards of conduct. In the military, ethical decisions often involve complex scenarios where leaders must balance competing interests, such as national security, the safety of soldiers, civilian welfare, and the preservation of human rights. Several ethical frameworks can guide military leaders when faced with difficult decisions, for instance:

Deontological Ethics framework emphasizes duty and adherence to rules or laws. Military leaders adhering to deontological ethics would focus on their responsibilities to follow the rules of engagement, adhere to military codes, and uphold legal and moral duties, regardless of the potential consequences;

Utilitarianism in ethic focuses on maximizing the greatest good for the greatest number. Military leaders applying utilitarian principles may prioritize decisions that achieve the best outcome for the most people, even if they involve some level of harm or risk to a smaller group;

Virtue Ethics approach focuses on the moral character of the decision-maker. A military leader applying virtue ethics would prioritize acting with integrity, courage, and compassion, aiming to build a positive culture of leadership and ethical behavior within their unit;

The theory of *Ethical Relativism* posits that moral standards can vary depending on culture and circumstances. Military leaders guided by this framework might make decisions based on the context and specific ethical norms of the situation they are facing, although this may lead to moral ambiguity in certain cases.

Many moral philosophers appear to have a clear preference for one the three main schools in moral philosophy, be it virtue ethics, rule-based ethics, or utilitarianism. Yet in real life, most people tend to see a role for virtues and rules alike while also taking the consequences of an act into consideration. It seems that those involved in Military Leadership and Ethics 11 military ethics education are practically duty-bound to adopt a similar mixed approach. An ethics education of military leaders should, for example, have attention for rules, procedures, and codes but also for virtues and character. To state it somewhat schematically: military leaders should be an example by displaying virtues, but also maintain certain rules, and take into account the consequences of their own acts and that of their subordinates. At the same time, they should also have an eye for the situation and how it can adversely affect their own conduct and that of those they lead. Even in a time that leadership is increasingly questioned, sound leadership at all levels is what keeps military personnel from behaving unethically.

4. ETHICAL TRAINING FOR MILITARY LEADERS

Teaching ethics in the armed forces, and instilling ethical values in soldiers of different ranks, is undoubtedly a challenging task. There are numerous unresolved issues discussed by authors writing about teaching military ethics, which primarily address the following questions: *Why should ethics be taught in the military? How should ethics be taught in the military? Who should teach ethics in the military?*

Hartle (2004) articulated a vision in which war is a harsh event that creates moral ambiguity, confusion, and stress upon the conscience of the warfighter. He also stressed the importance of values and ethics for the military profession as it acts in the most moral of professions, warfighting. Howard and Korver (2008) demonstrated that ethical reasoning and action not only prevent moral lapses and failures, but also serve as a tool for human moral flourishing and well-being. Connelly and Tripodi (2012) discussed the impact of moral incompetence, ambiguity, and moral failure on operations, and post-deployment reintegration, while Toner (1995) focused on describing the honorable and shameful in military conduct and action, prescribing a method that links moral and ethical ‘goodness’ to the military profession.

The opinions listed above present two main arguments as to why soldiers should be ethical and receive ethical education: the first is that the relationship between society and the military, encompassing support, the military’s responsibility to the parent society, and soldiers as citizens, necessitates ethical soldiers and leaders of character, while the second argument is rooted in the organizational culture of the military; specifically, the nature of military work often places soldiers in moral dilemmas. Ethically educated and trained soldiers should be better equipped to navigate such dilemmas.

Robinson (2007) wrote about two approaches to achieving ethical soldiers: the first is by osmosis, which involves a slow, unseen, and gradual influence throughout one's career, and the second is the explicit teaching and training of ethics. Robinson also highlighted two types of ethics: virtue ethics, which focuses on character, and valuebased ethics, which encompasses the values upheld by society and the military.

The question of who can or should teach ethics in the military is not simple at all. Authors mostly mention philosophers, lawyers, priests (military chaplains) and military officers/commanders as teachers. When reviewing the subject of how ethics is taught, MacIntyre and O'Keefe, in An Overview of Ethics Education (in STO-TR-HFM-304, p 29), indicate that "some authors insist that the behavior of students does not improve measurably after following ethical education programs of study". But they add that "it would be premature to conclude that the teaching of ethics is a failed venture simply because overt signs of understanding are less than visible." Specifically, "moral behaviour consists of more than observable actions. It also includes less visible behaviours such as perceptions, decision making and motivation".

Aalto (in STO-TR-HFM-304, pp 34, 37) states that when thinking about teaching ethics in the armed forces and teaching military leaders, we are again faced with whether ethics can be taught and, if so, how it is being taught in a military population. For example, is it teaching, training or education? He recognizes that teaching military ethics should be included in both training and educational aspects of training. He stresses that ethics teaching is also tied to a place, a time, and a culture, so an approach which works in one military organization may not work in others.

Since ethics is such an important element of military professionalism and a factor in military work and behaviour, the armed forces need, above all, ethical leaders. Foley and other authors, in a subchapter entitled Social Psychological Perspectives of Ethical Leadership (in STO-TR-HFM-304, p 16), point out that some researchers "suggest that the leader is the single most important determinant in shaping an organization’s ethical climate, which has a significant impact on the ethical behavior of organizational members and the operational effectiveness of the military unit in garrison and in a theatre of operations.”

Ethical decision-making is not an innate skill but one that can be developed through education, training, and experience. The military has long recognized the importance of preparing leaders to confront ethical challenges and navigate complex situations with integrity. Ethics training programs, which focus on teaching moral reasoning, the application of ethical theories, and the development of leadership character, are critical in shaping the decision-making abilities of military officers. Military education aims to shape and mould the ethical character of individuals, which, in a mutually supportive and interdependent manner, influences the ethical character of the organization they belong to and the military institution they are part of.

5. ETHICAL DILEMMAS IN MILITARY LEADERSHIP

O’Keefe say (in STO-TR-HFM-304, p 30): “*If we expect to encourage ethical behaviour, we need to first ensure that people can correctly identify dilemmas when they occur.”*

Military leaders frequently encounter situations where ethical dilemmas arise. These challenges often involve a conflict between fulfilling military objectives and adhering to moral or ethical standards. One of the most critical ethical challenges for military leaders is determining when the use of force is justified. Leaders must navigate between military necessity and humanitarian concerns. Decisions regarding the use of force, particularly in civilian areas, raise moral questions about proportionality, collateral damage, and respect for human life. In term of this military leaders must ensure that their subordinates act within the boundaries of international law and the rules of engagement. Kucera, in his text Ethics and International Humanitarian Law, deals with the dissemination of international humanitarian law (IHL) to the armed forces. Among other things, he stresses: “It is a legal obligation of military leaders to ensure that their subordinates comply with the rules of IHL. However, this obligation cannot be reduced to occasional IHL lectures.” (STO-TR-HFM-304, p 45).

Any breach of these rules, such as committing war crimes, can tarnish the integrity of the military and harm civilians. Leaders are responsible for preventing and addressing misconduct within their ranks.

Soldiers and military leaders alike may experience moral injury when they are involved in actions that conflict with their ethical beliefs. This often occurs in combat situations where leaders are forced to make decisions that have devastating consequences for others. Addressing moral injury is essential to ensuring long-term psychological and emotional well-being for military personnel.

The another ethical dilemma is moral choices and temptations even though the word *temptation* rarely appears and is even more seldom discussed in leadership development circles and ethics literature, actually every leader faces ethical and moral *temptations associated with the position*. Therefore, every leader must be prepared to answer this question: What are the specific moral and ethical temptations associated with the position I hold, and am I prepared to conquer them? The purpose of this article is to identify potential temptations associated with senior military positions and offer specific practices that can prevent leaders from engaging in wrongful, immoral, and unethical behaviors.

Despite this overarching organizational commitment to ethical military leadership, history shows that, without due diligence and moral courage, leaders with great integrity, high ethical standards, and effective training, operating in "morally sound cultures," can still make less than fully ethical and moral choices with devastating consequences, especially at the senior leadership level. Research shows that any number of factors can erode or degrade the most principled leader's character, causing questionable moral choices and unethical decisions when operating within the realities, dynamics, and pressures of the modern workplace.

In his book *The Lucifer Effect*, Philip Zimbardo identifies several workplace factors that can damage the moral fiber of individuals, including negative situational and environmental forces, lack of accountability, bad bosses, toxic organizational cultures, bad group dynamics, persistent personal isolation, a significant failure, and even success. These factors confront even the most upstanding leaders, potentially allowing them to be influenced or "tempted" to engage in unethical decisions and even activities that are knowingly wrong. Therefore, every leader must be prepared to answer the question: What are the specific moral and ethical temptations associated with the position I hold, and am I prepared to conquer them?

To understand the temptations associated with military command, the structured focus groups with 271 senior military leaders at 4 different senior Service colleges had been conducted. The participants were asked to anonymously answer the following open-ended question: “Based on your experience, what are the specific temptations or opportunities for wrong doing associated with your most recent position?” During these exercises, focus group participants identified many potential temptations of command. The top 10 temptations, ranked by frequency, follow

1. Falsifying, Massaging, or Manipulating Information.
2. Misuse of Government Funds/ Resources/Personnel.
3. Inappropriate Sexual Relationships.
4. Alcohol/Substance Abuse.
5. Favoritism or Preferential Treatment.
6. “Blind Eye” and Failure to Report Wrongdoing.
7. Exerting Inappropriate Influence on Personnel Decisions.
8. Offering/Accepting Gifts or Bribes or Quid Pro Quo.
9. Hubris.
10. Seeking/Demanding Deference or Preferential Treatment.

6. CONCLUSION

Military leadership accountability and ethical decision-making are intertwined elements that are crucial to the success and integrity of the armed forces. Leadership involves the responsibility of making decisions that protect the lives of soldiers and civilians while upholding national interests. Ethical decision-making requires military leaders to balance the demands of their mission with moral considerations, ensuring that their actions reflect the values of justice, honor, and duty. In a world where military leaders are often called upon to make life-altering decisions under pressure, fostering a culture of ethical decision-making and holding leaders accountable for their actions is essential to maintaining the trust and respect of the public, the military, and the soldiers under their command.

REFERENCES

[1] Clinton Longenecker and James W. Shufelt (2021), Conquering the Ethical Temptations of Command, available at: https://cenjows.in/military-leadership-challenges-navigating-complexities-of-21st-century/, last accessed March15th 2025.

[2] Codreanu, A. (2019) The strategic place and role of integrity among governance principles and values of public administration, available at:

https://www.afahc.ro/ro/rcic/2019/rcic'19/volum_2019/259-266%20Codreanu%201.pdf, last accessed March 15th 2025.

[3] Garb,M. (2023), Military and Ethics: How are Ethical Leaders Produced?, available at: https://sciendo.com/article/10.2478/cmc-2023-0014.

[4] Olsthoorn,P. (2023) Military Leadership and Ethics, available at https://philpapers.org/archive/OLSMLA.pdf, last accessed March 15th 2025.

[5] Kapitulik, E., MacDonald,J. (2019), The Program: Lessons From Elite Military Units for Creating and Sustaining High Performance Leaders and Teams.

[6] Sinek, S.(2017) Leaders Eat Last: Why Some Teams Pull Together and Others Don't. Portfolio/Penguin.

[7] Bickel, R. (2009). The Military Leadership Handbook. Washington, DC: National Defense University Press.

[8] Mark F. Light, The Navy's Moral Compass, Naval War College Review 65, no. 3 (2012),

[9] Dilek Z. Nayir, Michael T. Rehg, and Yurdanur Asa, Influence of Ethical Position on Whistleblowing Behaviour: Do Preferred Channels in Private and Public Sectors Differ? Journal of Business Ethics 149 (2018).

[10] Zimbardo, P. The Lucifer Effect: Understanding How Good People Turn Evil (New York: Random House, 2007).

[11] Sydney Finkelstein, Jo Whitehead, and Andrew Campbell, What Drives Leaders to Make Bad Decisions, Leader to Leader, no. 53 (June 2009).

[12] Bowman, K. D. (2004). Military Ethics: An Introduction with Case Studies. New York: Routledge.

[13] Casebeer, A. L., & McCauley, C. D. (2004). Ethics Education for Soldiers and Military Leaders. Cambridge University Press.

[14] Holmes, R. (2006). Acts of War: The Behavior of Men in Battle. Free Press.

[15] Puryear, E. J. (2000). Military Ethics and Leadership. Army Command and General Staff College Press.

[16] Winslow, D. (2001). The Ethical Issues of Military Leadership. Canadian Forces Leadership Institute.

EXPLORING SUSTAINABILITY EMBEDDEDNESS AND THE ROLE OF SUSTAINABLE LEADERSHIP IN DENEL: A CASE STUDY IN THE DEFENSE SECTOR

Mocheko Tinnes PHELA, Catherine LE ROUX, Lynette CRONJE

University of South Africa, Pretoria, South Africa

Sustainability embeddedness is crucial for the long-term viability of enterprises in the defense sector, particularly within state-owned enterprises (SOEs) that face financial, governance and operational challenges. This study addresses a critical gap in literature by exploring the limiting issues inhibiting sustainability embeddedness in Denel, a key South African defense enterprise, and offers a better understanding of the role of sustainable leadership in addressing these inhibitors. Guided by a qualitative case study approach, virtual semi-structured interviews were conducted with twelve senior managers and executives at Denel. Findings identify six key inhibitors to sustainability embeddedness: Political Meddling, Working in Silos, Inadequate Communication, An Unconducive Legal Framework, Corruption, and Decreasing Budget of the Department of Defense. The study highlights the role of sustainable leadership in addressing the inhibitors to sustainability embeddedness, which includes Educating Stakeholders, Adopting Good Organizational Values, Establishing Inclusivity, Practising Total Quality Management, Fostering Stakeholder Engagement, and Continuously Improving Systems and Resource Investment. The research contributes to scholarship on sustainability integration in defense SOEs by offering practical insights for policymakers and defense industry leaders aiming to institutionalise sustainability through context-responsive leadership practices.

Key words: *Sustainability Embeddedness, Sustainable Leadership, Defense Industry, State-Owned Enterprises (SOEs), Governance Challenges, South Africa.*

1. INTRODUCTION

The sustainability of enterprises in the defense sector remains a pressing challenge. Sustainability is not just an environmental concern; it also includes economic resilience, social responsibility, and effective governance. The embeddedness of sustainability—integrating sustainable practices into core strategies, capabilities and operations—can help mitigate these challenges (le Roux and Pretorius, 2019; Korkmaz, 2024, Pálffy and Ablonczy-Mihályka, 2024). Embedding sustainability enables organizations to advance towards socially and environmentally responsible outcomes and the attainment of sustainable development goals (Aygün et al., 2024)

Despite their critical role in economic and industrial development, many SOEs continue to struggle with embedding sustainability, thereby impacting their long-term viability (Mashamaite and Raseala, 2018; Popa, 2024). A case in point is the Denel Group, a key South African defense enterprise that has faced persistent financial instability, governance challenges, and operational inefficiencies (Sithomola, 2019). Given that Denel is a strategic partner of the South African National Defence Force, these challenges have far-reaching implications in terms of national economic growth, technological innovation, employment, and global defense security (Matsiliza, 2017; Matthews and Koh, 2021). These challenges emphasize the urgent need for sustainable leadership to overcome them and embed sustainability within enterprises such as Denel.

Research on sustainability has gained traction in recent years (Le Roux and Pretorius, 2016a; Trollman and Colwill, 2021; Pálffy et al., 2024). Several studies have explored the role of sustainable leadership in fostering sustainability (Liao, 2022; Aygün, Demir, Sağbaş, 2024), while others examine financial constraints and governance failures in SOEs (Madumi, 2018; Matthews and Koh, 2021). However, limited research offers a better understanding of sustainability embeddedness in defense sector SOEs, particularly in the South African context (Mashamaite and Raseala, 2018; Thakhathi, 2016; Phela, 2024, Shamshiyeva, 2024), thus highlighting the fundamental gap and purpose of this research.

This study aims to address this gap by exploring the limiting issues inhibiting sustainability embeddedness in Denel and the role of sustainable leadership in addressing these barriers. Two research questions guided the study:

(1) What are the limiting issues inhibiting sustainability embeddedness in Denel?

(2) What is the role of sustainable leadership in addressing the limiting issues and in embedding sustainability in Denel?

By answering these questions, we aim to contribute to the growing body of literature on sustainability in the defense industry (Korkmaz, 2024; Aygün, Demir, Sağbaş, 2024). The study aims to offer insights that are applicable to other public enterprises facing similar challenges. Using a single-case design methodology employing qualitative research, we conducted interviews with Denel executives and senior managers to better understand their lived experiences regarding the phenomenon. The study's findings provide critical insights into both the inhibitors to sustainability embeddedness and the role of sustainable leadership in addressing them.

We make two primary contributions. First, we enhance the understanding of sustainability embeddedness and sustainable leadership by engaging with practitioners to provide empirical insights into these concepts. Second, by identifying the specific inhibitors to embedding sustainability at Denel, we equip leadership and management with the knowledge needed to craft effective interventions and policy recommendations. These findings may be transferable to other enterprises in the defense industry and to nations aspiring to sustain a domestic defense industry (Korkmaz, 2024; Barrera, 2024).

The remainder of this paper is structured as follows: The next section presents the theoretical framework underpinning sustainability embeddedness and sustainable leadership. This is followed by a detailed discussion of the research methodology, including data collection and analysis techniques. The findings section provides an in-depth analysis of the collected data, linking key themes to the research questions. Finally, the conclusion offers a summary of insights, practical recommendations, and suggestions for future research directions.

2. LITERATURE REVIEW

Sustainability has evolved as a crucial concept, with organizations seeking long-term resilience through environmental, social, and governance (ESG) principles. However, sustainability embeddedness is often hindered in practice. In this next section, we offer a theoretical background on sustainability and sustainability embeddedness. We also discuss the challenges faced by SOEs globally in embedding sustainability and introduce the unique context of the South African defense industry.

2.1 Sustainability

Sustainability is no longer a peripheral concern but a strategic imperative for organizations navigating the complexities of the contemporary environment. It remains a priority for organizational future performance and resilience (le Roux and Pretorius, 2019) and a featured topic in high impact, leading journals, conferences and special issue calls (Aygün, Demir, Sağbaş, 2024).

Sustainability refers to the necessity to conserve natural resources, protect the environment, and instill social fairness while also promoting economic growth (Perrott, 2015; Le Roux, 2016b, Huda, Safar, Mohamed, Jasmi, and Basiron, 2019). Sustainability promotes the idea of an assimilated value creation space, where growth and achievements for the current generation pay equal and same consideration to all the components of sustainability and to the forthcoming generations (Ojo and Oluwatayo, 2016), Sakalasooriya, 2021; Le Roux, 2016b). Organizations that prioritize sustainability are more likely to achieve long-term growth by aligning with evolving regulatory, market, and societal expectations (Tarei, Chand, Gangadhari and Kumar, 2021). Furthermore, sustainable organizations are better positioned to attract investments and foster innovation through resource-efficient practices (Aygün et al., 2024).

2.2 Sustainability embeddedness

The evolving discourse on sustainability emphasizes its multifaceted and intertwined nature which includes social equity, economic viability, and environmental responsibility. Sustainability embeddedness refers to the process of inculcating sustainability practices at all levels of the organization, beginning with the integration of sustainability into its strategic management processes (Galpin et al., 2015; Sakalasooriya, 2021; Bertels et al., 2010: Trollman and Colwill, 2021).

To achieve a workable balance between organizational objectives, society, and the environment (Valente, 2015), the inclusion of each of these elements needs to be embedded into core business (Pálffy et al. 2024). Le Roux and Pretorius (2016) describe sustainability embeddedness as a process of ingraining sustainability practices into the everyday operations of an organization, with the ultimate objective of long-term performance and survival. Taken together, the literature on sustainability embeddedness emphasizes the importance of a fundamental shift in organizational culture toward sustainability by promoting values, norms, and behaviors aligned with long-term environmental, social, and economic goals (Williams et al. 2021; Thakhathi et al., 2019; Trollman and Colwill, 2021).

Central to the achievement of sustainability embeddedness is the important role of sustainable leadership. The following section discusses sustainable leadership and its role in embedding sustainability.

2.3 Sustainable leadership

Sustainability is a prolonged expedition that requires sustainable leadership, accountable decision-making, and an understanding of sustainability precepts and practices (Pearse and Dimovski, 2015). The University of Cambridge Institute (2017:9) defines sustainable leadership as:

> *... individuals who are compelled to make a difference by deepening the awareness of themselves in relation to the world around them. In doing so they adopt new ways of seeing, thinking and interacting that result in innovative and sustainable solutions.*

Sustainable leadership is considered a key factor or mediator in the achievement of sustainability embeddedness (Mukherjee, 2020; le Roux and Pretorius, 2016). According to Wamu, Winkler and Lundsten (2023), and Burmeister and Eriksson (2019), sustainability embeddedness depends on sustainable leaders creating a shared vision amongst stakeholders and promoting transparency in the production and distribution processes. Simiyu (2015) argues that sustainable leadership is essential for unfreezing organizational members' incorrect behaviors and attitudes towards sustainability, and for subsequently refreezing and cementing sustainability (Avery and Bergsteiner, 2011; Thakhathi et al., 2019). Through sustainable leadership practices, sustainable leaders aim to develop a change in attitudes and connections that generate lasting value for all the organization's stakeholders.

Sustainable leaders embed sustainability within the organization through sustainable practices and strategies (Thakhathi, 2016; Bulmer et al., 2021). Sustainable activities and stakeholder input are incorporated into organizational plans (Pearse and Dimovski, 2015; Ligita and Erika, 2014). The role of leadership is key to organizational sustainability embeddedness because it reflects the level of harmonisation through different styles and techniques to change the organization for the better (Zogjani and Raçi, 2015). A sustainable leadership role is assumed when leaders or sustainability champions within the organization have a clear understanding of what needs to be done to achieve the set sustainability targets (Liao, 2022; Kolzow, 2015).

2.4 The limiting issues inhibiting sustainability embeddedness

Despite the pivotal role of sustainable leaders in driving sustainability embeddedness, organizations still face barriers that hinder their transition to becoming sustainable organizations. These efforts are often constrained by systemic, organizational, and behavioral challenges (Le Roux and Pretorius, 2016a). Even the most committed sustainable leaders encounter obstacles that slow or derail sustainability adoption, requiring them to develop a deeper understanding of the inhibitors to sustainability embeddedness.

According to the literature, sustainability embeddedness is constrained by various limiting issues acting as barriers to how organizations adopt sustainability and transition into sustainable organizations (Bulmer et al., 2021; Tarei et al., 2021; Bartel et al., 2017). Trollman and Colwill (2021) found that the limiting issues to sustainability include economic system constraints and a lack of support for ecocentric business models. Le Roux and Pretorius (2016) identified the following limiting issues of sustainability embeddedness as: (1) Professing what is right - where employees believe that sustainability is the right thing to do and that being sustainable is essential for the organization's survival (Jones, 2021) but struggle to make sustainable decisions. (2) Green distraction - leaders reported that employees do not understand the true meaning of sustainability embeddedness. Rather than viewing the elements of sustainability (environmental, social, and economic) as interconnected, they treat them as separate concerns (Halldórsdóttir, 2014). (3) Not my job - this entails some practitioners' beliefs that sustainability is not their responsibility but someone else's work (Halldórsdóttir, 2014). (4) Past performance anchor - refers to a belief by stakeholders that the organization has performed well in the past, which keeps them anchored to previous practices and delays the shift to embeddedness (Eze et al., 2023; Ayandibu et al., 2019). (5) Fire fighter - reflects the hurried reactions and actions by practitioners to the demands, opportunities, and issues relating to their organizational operational requirements (Halldórsdóttir, 2014; Jones, 2021).

To overcome these inhibitors, sustainable leaders draw on sustainability-focused strategic discourse to combat misguided beliefs and practices acting as barriers to achieving a common sustainability purpose (le Roux, 2016b; Jones, 2021). Strategic discourse helps leaders align towards a shared vision of future strategy among stakeholders (Thakhathi et al., 2019; Orujov and Mammadzada Mahammadali, 2024). However, the persistence of barriers to sustainability embeddedness, suggests that further research is needed, particularly within the defense industry.

2.5 State-owned enterprises and sustainability

State-owned enterprises (SOEs) are public enterprises partially or wholly owned by the government to provide essential services like water, electricity, finance, energy, communication, and transport, among other services (Qhobosheane, 2018; Mashamaite and Raseala, 2018). SOEs are enterprises established by the government to achieve social responsibilities such as creating job opportunities and accomplishing economic responsibility (Muller et al., 2015; Madumi, 2018; Fourie, 2014). SOEs are required to run proficiently to boost the Return on Investment (ROI) for the government, its primary shareholder (Christiansen, 2013; Afrika, 2020).

According Moeljadi, Sutrisno and Susilo (2024), SOEs make significant contributions to local, regional, and international economic advancement by attracting and sourcing capital equipment, finance, and collaborations to boost economic growth. SOEs are also known to act as drivers in strengthening the capabilities of naval armaments. The sustainability of SOEs is of particular importance in a developing country like South Africa, given the extensive social, economic, and environmental needs in these countries (Madumi, 2018; Fourie, 2014). Unfortunately, many African SOEs have a long history of poor performance dating back to the 1970's, due to socio-economic circumstances adopted at the time, as well as leadership challenges (Limbo, 2019).

Prior to 1994, South African SOEs were employed as instruments to help the Apartheid government survive obstacles (e.g international sanctions) and were essential to grow the economy (Kanyane and Sausi, 2015). Post-1994, South Africa's democratic government inherited a public system that lacked accountability and transparency within its control systems (Muller et al., 2015). Consequently, the government repurposed SOEs to support the objective of becoming a developmental state. The SOEs were tasked with advancing economic growth, developing skills and innovation, and enhancing service delivery, while promoting social and environmental sustainability (Muller et al., 2015; Fourie, 2014).

2.6 The South African defense industry

The South African defense industry was developed between the years 1965 and 1990 to offer a range of capabilities through technological innovation (NDIC, 2020). Since 1999, the defense industry has been underperforming, which has resulted in reductions in employment levels within the sector (Matthews and Koh, 2021). The South African Defence Industry Strategy (NDIC, 2020) asserts that the defense industry holds the potential to significantly impact the profile of the South African economy. Such a shift would change the economy from one focused on agriculture and mining to one that also focuses on engineering, and is technology-directed, focusing on high-end software and electronics. According to Gopaul and Oosthuizen (2021), the defense industry can be a significant agent for enlarging and developing the national skill base, furthering national industrialisation policies, bringing foreign currency earnings from export linked services, and creating job opportunities.

The defense industry primarily focuses on the design, development, and manufacturing of weapons, munitions, pyrotechnics, equipment systems, and other materials for the Defense Force or for exports (Defence Review, 2015). Korkmaz (2024) observed that, unlike other sectors, the defense industry can be significantly influenced by political fluctuations and international relations.

South Africa has three SOEs within the defense industry, namely: Armscor, CSIR-DPSS (Council for Scientific and Industrial Research-Defense, Peace, Safety and Security), and Denel. Armscor is an SOE responsible for defense acquisition in compliance with defense material and remains an intelligent buyer within the defense industry (Defence Review, 2015). This SOE also contracts, conducts, and coordinates research and innovation to advise the Defense Force and local industry.

On the other hand, CSIR-DPSS ensures product development possibilities, thereby strengthening competencies in the industry and the broader national system of innovation and further signifies local manufacturing competencies (Defence Review, 2015). CSIR-DPSS develops technology to a level of readiness for absorption by industry to be used in further research and development.

Denel is the largest of South Africa's state-owned arms companies. It focuses on aerospace and military technology, as well as defense innovation and security in the defense sector of South Africa (Denel Group, 2019). Denel is the focal case of this research and is introduced in the next section.

2.7 Denel Group

Denel was established in 1992 as a commercially driven global enterprise with a mandate to develop, design, manufacture, support, and sustain defense materials (NDIC, 2020). Denel provides turnkey solutions for defense equipment to its clients (Denel Group, 2015) and full lifecycle support in the military territory (Denel Group, 2020).

Denel represents 0.86% of the GDP in South Africa (Martin, 2021; NDIC, 2020), and it governs four out of the seven broad areas of the domestic defense market. These areas include aerospace, ammunition, weapon systems, and military vehicles. In addition, it is a holding enterprise that is structured into three major categories; namely, Aerospace, Ordnance, and Commercial and Information Technology (Denel Group, 2020; NDIC, 2020). The SOE's footprint also extends to the larger South African manufacturing sector, through its outsourcing of important components of production and the procurement of raw materials (Defence Review, 2015; Denel Group, 2019). Furthermore, Denel's shift towards globalisation was aimed at ensuring an adequate capital boost (offering quality and affordability), increased access to global markets, a wider product range, and increased capacity utilisation within its production establishments (DPE, 2021).

Despite these efforts, Denel has reported its financial struggles and instigated a series of turnaround interventions. As part of these turnarounds, Denel management shifted focus towards the amalgamation of strategies to secure internal restructuring, Denel's executive management focused on budgeting, ensuring suitable strategic equity shareholders, and made public commitments to embedding sustainability in their public reports (Defence Review, 2015; 2019; 2020).

Since 2019, Denel has employed specific steps to responsibly use limited natural resources to preserve the environment (Denel Group, 2020), thus making it an information-rich case (Moeljadi et al., 2024). Denel's strategic role as an SOE, combined with its unique sustainability challenges, presents an instrumental case for exploring the limiting issues inhibiting sustainability embeddedness. Insights from this study, and particularly the role of sustainable leadership, can extend beyond Denel, offering broader implications for SOEs, defense industries, and sustainability transitions in highly regulated and state-controlled enterprises (Shamshiyeva, 2024).

3. RESEARCH METHODOLOGY

To explore the limiting issues inhibiting sustainability embeddedness at Denel, a qualitative case study approach was adopted. After obtaining permission from

Denel and the University of South Africa's Ethics Committee, executives and senior managers working at Denel were purposefully selected, given their responsibility for the strategic formulation and direction in the organization. The executives and senior managers voluntarily participated by engaging in semi-structured interviews on MS Teams, which were approximately 51 minutes each. Data was gathered from multiple departments within Denel to obtain a comprehensive understanding of the case. The participants averaged 14 years of Denel work experience, and the interviews continued until data saturation was reached at 12 participants (Popa, 2024). Theoretically driven questions were employed such as: Do you think sustainability embeddedness is important at Denel? How does sustainability adoption occur in Denel? What practices do you employ to embed sustainability in Denel? Do you consider yourself to be a sustainable leader at Denel and why? What needs to be done for Denel to become a sustainable organization?

The interviews, which were recorded and transcribed, yielded in-depth insights and rich data into sustainability inhibitors and on the role of sustainable leadership within the organization. To uphold our commitment to confidentiality, pseudonyms were used, and we also strived to add rigor and trustworthiness to the study by incorporating member checking into our protocol. Participants confirmed that the transcripts reflected their lived experiences (Salkind, 2014).

We imported the data into Atlas ti. software for qualitative thematic analysis. We then employed both an inductive and deductive approach to make sense of the lived experiences of participants (Salkind, 2012), with the intention to build theory from the case study (Yin, 2018). Through studying the transcripts, we allowed the participants to describe the phenomenon of interest by looking for patterns and meaning. Afterwards, we applied a deductive approach by using theory and literature from other studies to support the emerging findings. A visual representation of the research process is depicted in **Figure 1**:

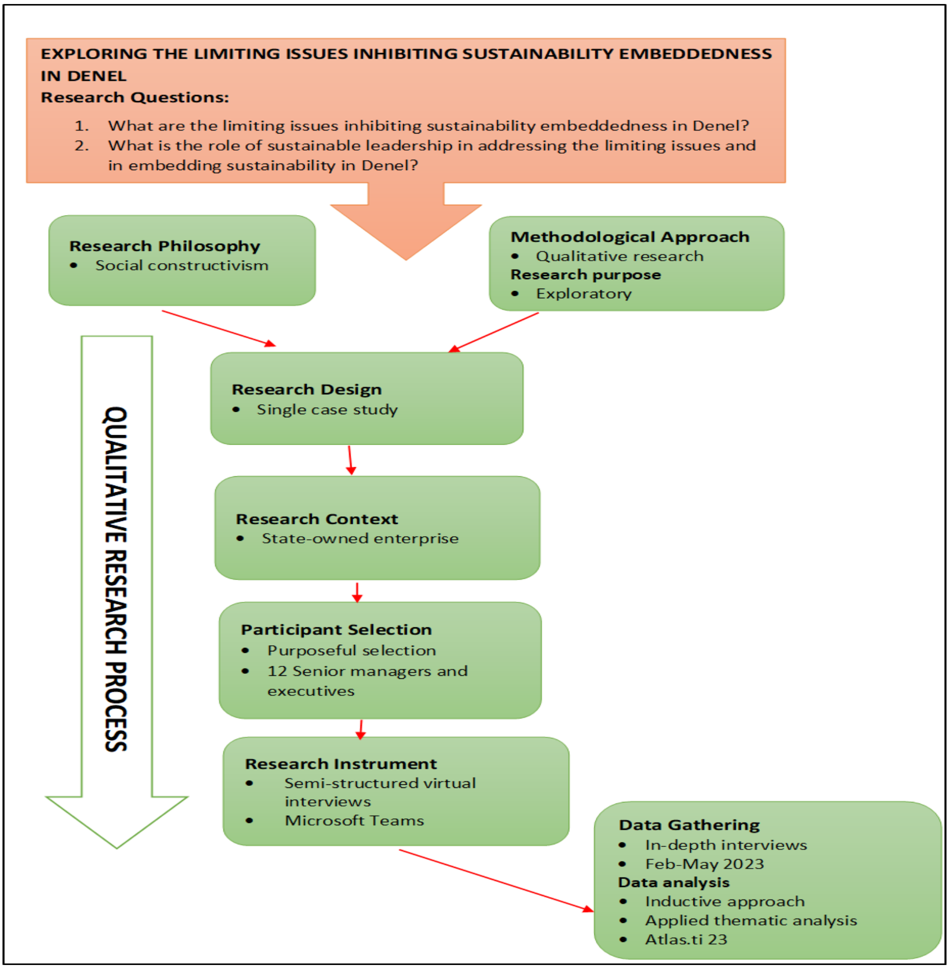

EXPLORING THE LIMITING ISSUES INHIBITING SUSTAINABILITY EMBEDDEDNESS IN DENEL
Research Questions:
1. What are the limiting issues inhibiting sustainability embeddedness in Denel?
2. What is the role of sustainable leadership in addressing the limiting issues and in embedding sustainability in Denel?
Research Philosophy
• Social constructivism
Methodological Approach
• Qualitative research
Research purpose
• Exploratory
QUALITATIVE RESEARCH PROCESS
Research Design
• Single case study
Research Context
• State-owned enterprise
Participant Selection
• Purposeful selection
• 12 Senior managers and executives
Research Instrument
• Semi-structured virtual interviews
• Microsoft Teams
Data Gathering
• In-depth interviews
• Feb-May 2023
Data analysis
• Inductive approach
• Applied thematic analysis
• Atlas.ti 23

Figure 1: Qualitative research process

4. FINDINGS

Before introducing the six inhibitors to sustainability embeddedness at Denel, and the role of sustainable leadership in mitigating these inhibitors and promoting sustainability embeddedness, we begin by providing context to these findings by offering insight from participants' understanding of the case (4.1-.4.3).

4.1 Strategic importance of Denel

Participants confirmed Denel as a critical entity within the South African defense sector, not only for military capability but also for national economic and engineering skill development. Charles outlined its dual strategic role:

"Denel is important for two reasons: one, its level of dependence from a military point of view for South Africa in particular. The second thing is that it creates capacity for intellectual capital for the country. Denel does a lot of engineering work, and from that engineering work, which is specifically military in nature, that can be diffused into the bigger economic areas of the organization." (Charles)

Isaac reinforced this perspective, noting Denel's technological contributions beyond defense:

"Most of the technologies that are currently used in South Africa came from Denel's innovations and Armscor. Initially, those were conceptualised for military use, but they have since been diversified for everyday use by everybody. So you cannot underestimate the value that Denel brings to the country. But secondly, and this is the important part, Denel carries a certain portion of South Africa's engineering base. I'm talking about the brains of South Africa." (Isaac)

Participants associated Denel's continuity as being essential to national security, as emphasized by Isaac and Hilary: *"The very sovereignty of South Africa, which is directly, by legislation coupled to the mandate of the South African Defence Force cannot be divorced from the existence of Denel either, because without Denel, the Defense Force will not be able to fulfill its constitutional mandate of ensuring or safekeeping our sovereignty."* (Isaac)

"In our case, in terms of security, Denel is important in that regard — to make sure that we keep the sovereignty of the country within our own borders. I don't think it's any government's wish to see or rely on a particular country's technology to protect themselves." (Hilary)

4.2 Participants' understanding of Sustainability

The executives and senior managers demonstrated a clear understanding of sustainability and its critical role in ensuring organizational longevity and strategic focus.

Charles and Isaac highlighted the significance of sustainability in securing Denel's reputation and continuity:

"Well, sustainability can be the business being able to continue operating in the short and long term. It is not only about profitability, because profitability can be a short-term event, but it is the ability of business to exist profitably in a longer term." (Charles)

"Sustainability has to do with regeneration. It has got to do with longevity. It has got to do with

durability, being able to withstand various tests that may come one's way." (Isaac)

Sustainability was also linked to strategic decision-making and future planning. Gabriel underscored its role in maintaining Denel's vision:

"The advantages… look, if you want to be sustainable you need to be competitive. So one of the advantages is that you need to always be innovative, to come up with ideas, to come up with new products." (Hilary)

Isaac elaborated on the link between sustainability and organizational growth:

"The biggest thing for me as far as sustainability is concerned, we are all looking for growth. You can't find growth without sustainability. In fact, I dare say that one of the direct outcomes of being sustainable is that you are automatically able to grow." (Isaac)

Sustainability was associated with Denel's ability to maintain business operations over the long term.

4.3 Sustainability embeddedness at Denel

Sustainability embeddedness was articulated as forming part of procurement practices and environmental responsibility. Benny illustrated how sustainability influences decisions:

"…we're obviously procuring with the intention of things like, almost like buying green, if I can call it that. I think there's something called the green procurement that we have to look at. But also in terms of the social element, in terms of how do we invest in our people, in our communities, and things like that. And ultimately, also combining that with the objectives of the organization in terms of where the organization wants to go in the future." (Benny)

Charles highlighted the broader cultural implications of sustainability embeddedness:

"Sustainability embeddedness in our organization means that the concept of sustainability is entertained with all the activities of the business throughout the value chain. Today the big issue is about climate change. The effects of climate change caused by how we produce things today. So it means in that embeddedness becomes part of the culture of the organization. Then that culture is linked to policies, practices, training and awareness among all employees and management." (Charles)

The findings reveal that participants understood sustainability as being integral to Denel's strategic vision, despite Denel's challenges. The following sections (4.4-4.5) present the findings from the case study, providing answers to the study's two research questions.

4.4 Inhibitors to Sustainability Embeddedness at Denel

The following findings emerged as the inhibitors to sustainability embeddedness at Denel.

1. Political Meddling

Political interference was identified as a significant constraint to achieving sustainability embeddedness. This interference was perceived to affect decision-making processes by prioritising political interests over Denel's sustainability objectives.

Abram noted, *"...as the disadvantages of SOEs is the political meddling, right? Instead of a decision just to be commercial on price, and so on, politics get involved also. And then the profit motive is not as strong as if it was a total private company."* (Abram)

Benny supported this finding, stating, "I think that's the problem right now and sometimes I do think there's too much political interference that doesn't allow people necessarily to move." (Benny)

The impact of political influence on sustainability was elaborated upon by Hilary: "...there's a lot of external influence in terms of politics, geopolitics and all that, and some of the policies, government policies, are not geared toward an engineering company which needs to compete with the private sector." (Hilary)

Political meddling was considered an inhibitor to sustainability embeddedness and performance because of the inefficiencies and misalignment it created.

2. Working in Silos

Working in silos emerged as another inhibitor to sustainability embeddedness, restricting collaboration and communication between different teams and departments.

John highlighted this issue: "Okay, as I said before, in Denel, we mostly, always had a culture of doing things in isolation. [...] And it always boils down to that isolation and doing things in your own little corner and doing things with your friends. You don't want to be part of a team; you want to talk to your own people." (John)

This was reinforced by Kham who linked siloed working to internal conflicts: "The other challenge is that in different departments people are still working in silos. When you start working in silos, people are conniving behind progress…" (Kham)

This finding revealed how a disjointed working culture reduces the cooperation necessary for the achievement of sustainability initiatives. The silos were perceived to impede the sharing of knowledge and the development of integrated action plans necessary for sustainability.

3. Inadequate Communication

Another significant inhibitor, leading to misalignment and inefficiencies in sustainability initiatives, was the poor communication within the organization as described by participants.

Freddy elaborated on this issue: “It's communication, especially on the decision-makers' part and that mostly they take decisions in the boardrooms, which are decisions that will affect the people on the ground and in most cases the people on the ground don’t have a say, and they don’t give inputs in those decisions that normally at the end affects them.” (Freddy)

Gabriel added, “… the inhibition of sustainability comes as a result of the message not getting to the right people that are ultimately entrusted with ensuring that Denel operates, Denel produces and so on.” (Gabriel)

Hilary emphasized this point by indicating that “…the leadership should have a direct communication with their employees.” (Hilary)

These findings reveal how ineffective communication obstructed Denel’s ability to implement and sustain sustainability initiatives.

4. Unconducive Legal Framework

An unconducive legal framework was identified as another constraint, with lengthy bureaucratic processes hindering efficiency and sustainability.

Hilary illustrated the consequences of these legal constraints on Denel’s sustainability: “We always complain about the PFMA (Public Finance Management Act) and all that, that it actually hinders our competitiveness in the market, because we compete with the international market.” (Hilary)

A tangible example of these inefficiencies was provided by Freddy: “I can make a small example, like if I have to buy screws, to make a weapon, and in those screws you find that it can take me 20 minutes to just go buy the screws, for R50, but because of these processes that I have to follow, for me to get those R50 screws, I might end up losing that R500 that I was going to get.” (Freddy)

These regulatory barriers were reported to have prevented Denel from responding swiftly and effectively to sustainability opportunities.

5. Corruption

Corruption was reported as an inhibitor to sustainability embeddedness, diverting organizational objectives towards self-serving interests and fostering a dishonest culture.

Participants Charles and Hilary expressed that sustainability was inhibited by corruption. Charles shared: “Because there is also reality about fraud and corruption, which was part of the element of what happened during the state capture” (Charles)

“Remember, I said there’s too much interference, either by corruption, either by, I don’t know” (Hilary)

Gabriel referred to the corruption scandals in the news: “… Denel went to the Zondo Commission, it's a clear sign that somebody did something wrong. Very, very wrong.” (Gabriel)

John explained that dishonesty was entrenched within the organization: “Okay, as I said before, in Denel, we've always had a culture of not trusting each other. And we've always had a culture of not being honest and doing things with your friends.”(John)

The participants reported that they perceived the corruption as inhibiting sustainability. It was reported to have affected the company’s reputation by diverting resources away from sustainability goals.

6. Decreasing Budget of the Department of Defense

The declining budget allocated to the defense industry was another inhibitor found in this study. Participants expressed that the reduced funding affected Denel’s ability to carry out sustainability initiatives.

Charles highlighted this financial constraint: “…the market is limited for defense which is locally, the local budget for instance is limited. It’s not increasing. In fact, it is decreasing. Competition becomes a real issue for the organization because if you don’t have adequate funding it is not easy to complete by improving the programs.” (Charles)

The impact of the declining budget was explained by Emanuel “…but the issues that we have been facing for the past few years was that the company was at the brink of low orders, due to a reduced defense budget.” (Emanuel)

Moses reinforced this perspective, stating: “I will say… continuous cost-cutting measures in terms of your operational expenses and in terms of your resources, your people, your equipment that you use.”

The reduction in financial resources from the South African government was described as a limiting issue affecting Denel's ability to invest in its people, operations, and sustainability programs. This was found to affect research and development and the achievement of sustainability goals.

Addressing these inhibitors was reported as being essential to advancing the organization's sustainability agenda and ensuring long-term operational viability. Next, we discuss how the participants perceived the role of sustainable leadership in addressing these inhibitors to sustainability embeddedness.

4.5 Role of Sustainable Leadership in addressing the inhibitors to sustainability embeddedness

The participants identified the following roles as essential to overcoming the inhibitors and to embedding sustainability at Denel.

1. Educating Stakeholders

The findings revealed that a critical role of sustainable leadership was the education of stakeholders regarding sustainability. Leaders were reported to be central to encouraging to activating and embedding sustainability.

Benny emphasized that: "It's about educating the stakeholders around sustainability. Not just educating, but also looking at implementing some of the best practices that are out there in terms of sustainability and teaching people what it is to do what is right. I think sustainability is also about doing the right thing" (Benny)

This view was reinforced by Emanuel, who noted: "I think it's more about learning and explaining and teaching as well, so that we can have everyone on the same level." (Emanuel)

Policies were associated with sustainability education, which was considered an important responsibility of sustainable leaders. Charles shared that: "Policies that promote sustainability must be effectively communicated and understood by everyone in the organization." (Charles)

By ensuring that stakeholders understand and support sustainability initiatives, sustainable leaders mitigate the effects of political meddling by shifting the focus from external interference to ethical and sound decision-making.

2. Adopting Good Organizational Values

Sustainable leadership was also reported to play a fundamental role in fostering a culture in which sustainability is embedded within organizational values. These values were seen as drivers of ethical behavior, enhanced accountability, and an environment conducive to sustainability.

Benny highlighted this aspect, stating: “Sustainability is also about doing the right thing.” Similarly, Charles reinforced the need for sustainable leaders to promote ethical practices: “Consistently applying and abiding by good values of the organization that promote sustainable business just to show, for instance, that business doesn’t exist on an island.” (Charles)

Gabriel further asserted that sustainability values should be embedded into organizational culture: “They must just also add a sustainability conscious. If that can be added into our culture, because your values speak to your culture.” (Gabriel)

Isaac highlighted the need for confident, sustainable leaders to instil these values, stating: “We have got leadership that is not self-confident in their own ability to get things done.” (Isacc)

By embedding strong values, sustainable leaders address corruption and foster an environment of transparency that counters the self-serving interests often derailing sustainability efforts.

3. Establishing Inclusivity

Ensuring inclusivity within the organization was identified as another critical leadership role. Sustainable leaders create inclusive structures by refining policies and procedures, ensuring that all employees contribute to and benefit from sustainability initiatives.

Hilary, described this role, stating: “As part of my initiative, I’m trying to rectify the issue of policies and procedures, which also rebuilds the organization’s structure, so that everyone can feel they belong and are part of the solution.” (Hilary)

Freddy supported this view adding: “The way they explain the plans, and how they’re going to be executed, and the involvement of all parties in that plan and the execution of the plan.” (Freddy)

By fostering inclusivity, sustainable leaders can address the siloed working culture, ensuring that sustainability efforts are integrated across departments for cohesive and collective progress.

4. Practising Total Quality Management

Total quality management (TQM) emerged as a key approach in embedding sustainability by improving operational efficiency, ensuring compliance, and maintaining high standards. TQM principles were considered important in how sustainable leaders drive sustainability objectives.

John highlighted his commitment to embedding sustainability by adopting this approach: “I'm also currently drafting a template for documents and policies that will tell the organization, this is how you do your decision analysis. This is how we prioritize your projects. This is how you do a feasibility study. This is how you qualify project. So I'm busy with all those initiatives." (John)

Charles reinforced the importance of driving compliance in achieving quality and sustainability. He noted, "The infrastructure for compliance oversees quality issues, environmental issues, and so on." (Charles)

Similarly, Daniel stated, "Your quality systems, your contracting models, and all signing of the certificate of conformance must be part of that process" (Daniel)

This key role of sustainable leadership could address the unconducive legal framework. Through compliance and quality processes, the inhibitor may be overcome to support sustainability.

5. Fostering Stakeholder Engagement

Sustainable leaders play a critical role in engaging employees, suppliers, and key stakeholders to align them with sustainability objectives. Strong engagement builds trust, enhances collaboration, and facilitates the successful implementation of sustainability initiatives.

Freddy highlighted this role, stating, "In my role, it is crucial to communicate clearly to make sure projects are executed on time." (Freddy)

Gabriel supported this perspective, adding, "I fully engage with my team, communicate with them regularly, receive feedback, and guide them." (Gabriel)

Hilary further stressed the importance of strategic communication with all stakeholders, "Through dialogue, communication, and alignment with stakeholders, we can overcome those things [challenges]." (Hilary)

Sustainable leadership that embraces this role could counter ineffective communication, ensuring that sustainability messages are effectively communicated and that all stakeholders are aligned in driving sustainability initiatives forward.

6. Continuously improving systems and resource investment

The continuous improvement of organizational systems and investment in resources is another crucial role of sustainable leadership. This was reported to facilitate efficiency and the long-term viability of sustainability initiatives.

Moses emphasized this, stating: "Continuous improvement in processes, cost-cutting measures, and investment in resources, people, and equipment is essential." He further highlighted the need for strategic agility: "Decisions must be made quicker, more strategic decisions that can actually help the company to grow… The turnaround time of approvals of such decisions must be made quicker, and the company must actually be allowed to be self-sustainable…We need to be able to operate like a private company" (Moses)

John reinforced this role by indicating: "One of our interventions as the organization is to formalise this process of business excellence initiatives… and optimise all our policies, systems, processes, procedures, and work instructions" (John)

Through continuous improvement and investment, sustainable leaders mitigate the challenges posed by the decreasing budget of the Department of Defense, ensuring that Denel remains agile, competitive, and sustainable despite financial constraints.

The findings in the study underscore the essential roles of sustainable leadership in overcoming the barriers to sustainability embeddedness at Denel.

5. DISCUSSION

This study was guided by two research questions: (1) What are the limiting issues inhibiting sustainability embeddedness in Denel? and (2) What role does sustainable leadership play in addressing these limiting issues and embedding sustainability in Denel?

In response to the first research question, the study identifies six inhibitors to sustainability embeddedness at Denel. These include political meddling, working in silos, ineffective communication, an unconducive legal framework, corruption, and a decreasing defense budget. These challenges align with existing literature, particularly the findings of Sithomola (2019), Madumi (2018), and Popa (2024), who highlight similar constraints, including maladministration, leadership deficiencies, ambiguous mandates, mistrust, debt burdens, and weak managerial accountability. Furthermore, the study's findings at Denel align with those of Korkmaz (2024), who established that political fluctuations and international relations exert considerable influence over the defense industry.

To address the second research question, the study illustrates the crucial role of sustainable leadership in overcoming these limitations. Sustainable leaders counteract the identified inhibitors by educating stakeholders, adopting good values, establishing inclusivity, ensuring total quality management, engaging stakeholders, and continuously improving organizational systems and resource investment. These roles were not merely aspirational but were enacted through practices such as convening cross-functional task teams, initiating ethical and green procurement, and championing internal knowledge-sharing to break down silos. Collectively, these sustainable leadership roles establish a strategic foundation for advancing sustainability within Denel, thereby ensuring long-term resilience and sustainability embeddedness.

Consistent with Le Roux and Pretorius (2016), senior managers and executives at Denel recognized the importance of sustainability and its direct connection to organizational longevity. However, they encountered challenges translating this recognition into sustainable decision-making within their operational context (Jones, 2021). The inhibitors identified in this study corroborate existing literature while offering practical insights into the lived experiences of defense industry professionals. They foreground how sustainable leaders operationalized sustainable values in day-to-day decisions—such as mediating conflicts arising from budget constraints or resisting external political pressure. In doing so, this study offers concrete illustrations of leadership-in-action within a contested operational landscape.

Moreover, the study builds on the recent contributions of Shamshiyeva (2024) by emphasizing the necessity of cultural and managerial transformations in achieving strategic objectives within Defense enterprises. The enhanced understanding of sustainable leadership's role in navigating complex challenges within a defense-sector company aligns with Barrera's (2024) findings, which highlight the significance of adaptive leadership in addressing the defense industry landscape. Similarly, echoing Le Roux and Pretorius (2016b) as well as Barrera (2024), this study emphasizes that purpose-driven communication and strategic discourse are critical in an increasingly volatile, uncertain, complex, and ambiguous (VUCA) environment.

Given the unique and unpredictable nature of the defense sector (Codreanu, 2016; 2022), sustainable leaders in defense enterprises must focus on the reported core components of their role as part of their approach. These elements are instrumental in fostering trust and coordinating activities effectively (Popa, 2024). Policymakers designing governance and sustainability frameworks should carefully consider the supporting mechanisms that enable sustainable leadership in institutionalising sustainability.

This study's findings underscore the indispensable role of sustainable leadership in addressing the inhibitors to sustainability embeddedness within state-owned enterprises (SOEs). Addressing governance challenges and cultivating an organizational culture centred on sustainability are likely to contribute to the long-term viability of Denel and comparable enterprises. By overcoming the inhibitors to embedding sustainability and adopting sustainable leadership practices, enterprises in the Defense sector can enhance resilience and ethical governance to navigate the evolving challenges in their operating environments. Policymakers may benefit from incorporating leadership development programs that specifically address context-sensitive challenges such as political interference. This could equip leaders to sustain change in volatile institutional settings.

6. MANAGEMENT RECOMMENDATIONS

The findings highlight several critical areas for management intervention to advance sustainability within the organization. A key recommendation is for senior management to undertake a strategic review of resource allocation, aligning organizational resources with sustainability objectives. By prioritising investments in revenue-generating activities and sustainability targets, the organization can better manage budget constraints while maintaining progress toward environmental and ethical commitments. In conjunction with this, the implementation of sustainability system checks is essential for the ongoing monitoring and evaluation of sustainability strategies.

Furthermore, sustainable leadership should focus on reviewing and refining organizational policies and procedures to facilitate sustainability initiatives (Sharafizad et al., 2022; Le Roux and Pretorius, 2016a). While senior management reported an understanding of sustainability principles, there is a need for structured sustainability policy workshops to ensure employees at all levels gain a comprehensive understanding of policies, such as green procurement. These training initiatives could enhance policy implementation, improve efficiency, and foster organizational agility.

To address ethical concerns and mitigate risks associated with corruption and political interference, management should develop a robust code of ethics, reinforced by stringent hiring processes. This code can serve as a foundation for establishing clear behavioral expectations and corresponding consequences for unethical conduct, helping to cultivate a sustainability-driven organizational culture (Mishra and Aithal, 2022). Additionally, integrating sustainability values into the onboarding process for new employees will further embed these principles into the organizational ethos, ensuring alignment with sustainability objectives from the start.

Given its critical role in fostering sustainability-driven innovation and ensuring long-term viability, an increased investment in research and development (R&D) is recommended (Sarpong et al., 2023). Expanding R&D initiatives will support the development of new sustainability-focused technologies and practices, positioning the organization as a leader in sustainable management.

Effective communication also emerged as a pivotal factor in successful change management. Sustainable leaders must evaluate and refine the frequency and clarity of internal communication, ensuring that sustainability objectives are well understood and embraced across all organizational levels. Assessing employees' reception of sustainability messaging and employing improved discursive tactics can enhance cooperation (Orujov et al. 2024), foster shared understanding, and facilitate the organization's sustainability transition. Improved communication strategies will also strengthen change management efforts (Wippermann, 2017; Codreanu, 2022) by providing a clear roadmap for the transition.

By implementing these recommendations, management can cultivate a culture of sustainability that facilitates the organization's long-term resilience within the defense industry.

7. CONCLUSION

By examining the inhibitors to sustainability embeddedness in Denel, this research offers critical insights into the governance and leadership challenges that hinder long-term resilience in defense enterprises. The study highlights the urgent need for sustainable leadership as a strategic enabler in mitigating financial instability and fostering innovation in the defense industry. Given the sector's reliance on long-term planning, technological advancements, and regulatory compliance, embedding sustainability within strategic and operational processes is essential for ensuring future viability. In contexts such as Denel, it is vital that leadership enactment extends beyond compliance to actively influence institutional direction —an insight that may inform public policy on SOE governance and defense sustainability mandates.

Through a qualitative case study, the findings identified six key inhibitors. These inhibitors align with existing literature on governance and leadership challenges within state-owned enterprises (SOEs) in the defense sector. The study further highlighted the pivotal role of sustainable leadership in overcoming these barriers. By fostering an organizational culture centred on sustainability, sustainable leaders can enhance resilience and long-term viability within defense enterprises.

While this study contributes to the understanding of sustainability embeddedness in SOEs, it is subject to certain limitations. The research focused on a single organization within the South African defense industry, and whilst the findings are not generalizable, they are potentially transferable. Future research should expand to include other SOEs and defense enterprises across different geographical and economic settings.

Methodologically, a single qualitative case study was applied to gather in-depth data from the lived experiences of senior managers and executives at Denel. The interviews did not include insights from middle management, frontline employees, or external stakeholders. Incorporating a broader range of perspectives could provide a more comprehensive understanding of sustainability implementation across organizational levels. Data gathering was conducted virtually, which may have constrained the depth of observational insights. Future studies could benefit from in-person engagements, longitudinal observations, or mixed-method approaches to explore causal relationships and track sustainability outcomes over time. Given the financial challenges that emerged in the findings of this study, future research could examine the impact of budget constraints on sustainability initiatives and overall organizational performance in defense organizations.

Despite these limitations, the study offers valuable insights into the role of sustainable leadership in addressing sustainability inhibitors within the defense sector. By adopting the sustainable leadership practices and embedding sustainability principles into organizational processes, defense enterprises can navigate complex and volatile landscapes while fostering long-term sustainability of national defense enterprises.

REFERENCES

[1] Afrika, S.L.S. 2020. State Aid to State-Owned Enterprises in South Africa: The need for a comprehensive state aid policy, a competition law inquiry. Thesis (LLD). University of Stellenbosch.

[2] Ayandibu, A.O., Ngobese, S., Ganiyu, I.O. and Kaseeeram, I. Constraints that Hinder the Sustainability of Small Businesses in Durban, South Africa, *Journal of Reviews on Global Economics*, Vol. 8, pp. 1402-1408, 2019.

[3] Aygün, S., Demir, B. and Sağbaş, M., Examining the Relationship between Sustainable Development and Digital Leadership using Bibliometric Analysis Method, *Journal of Defense Resources*

Management, Vol. 15, No. 2, pp. 122–135, 2024.

[4] Avery, G.C. and Bergsteiner, H., Sustainable Leadership Practices for Enhancing Business Resilience and Performance, *Strategy & Leadership*, Vol. 39 No. 3, pp. 5-15, 2011.

[5] Bartel, C., Aerni, P. and Schluep, I., What does Embeddedness Mean in the Context of Corporate Sustainability ? Executive Summary, CCRS policy panel and plenary discussions, 19 January. Zurich: Center for Corporate Responsibility and Sustainability (CCRS) at the University of Zurich, 2024.

[6] Barrera, M. S., Strategies for Enhancing Military Leadership: A case study of VUCA Prime in the Colombian Aerospace Force. *Journal of Defense Resources Management*, Vol. 15 No. 1. pp. 95 – 108, 2024

[7] Bertels, S., Papania, L. and Papania, D., Embedding Sustainability in Organizational Culture, A Systematic Review of the Body of Knowledge, Network for Business Sustainability, 2010, Available from: https://embeddingproject.org/pub/resources/EP-Embedding-Sustainability-in-Organizational-Culture.pdf.

[8] Bulmer, E., Riera, M. and Rodríguez, R., The Importance of Sustainable Leadership Amongst Female Managers in the Spanish Logistics Industry: A cultural, ethical and legal perspective, *Sustainability*, Vol. 13, No. 12, pp. 1-19, 2021.

[9] Burmeister, A. and Eriksson, M., (2019) Exploring Sustainability Strategy Implementation in SMEs: A Case Study of Internal Communication Processes in Sweden. MBA thesis. Umeå University, Umeå, Sweden.

[10] Codreanu, A., A VUCA Action Framework for a VUCA Environment: Leadership Challenges and Solutions, *Journal of Defense Resources Management*, Vol. 7 No. 2, pp. 31–38, 2016.

[11] Codreanu, A., Leadership Prerequisites, Actions, and Standards of Behavior in Change Management', *Journal of Defense Resources Management*, Vol. 13 No. 2, pp. 137–152, 2022.

[12] Christiansen, H., (2013) *Balancing Commercial and Non-Commercial Priorities of State-Owned Enterprises*, OECD Publishing, Paris.

[13] Department of Public Enterprises (DPE), . Annual Performance Plan, 1-107, 2021

[14] Denel Group, Denel SOC integrated report, 1-240, 2015.

[15] Denel Group, Denel SOC integrated report, 1-244, 2019..

[16] Denel Group, Denel SOC integrated report, 1-260, 2020.

[17] Eze, E.C., Sofolahan, O. and Omoboye, O.G., Assessment of Barriers to the Adoption of Sustainable Building Materials (SBM) in the Construction Industry of a Developing Country, *Frontiers in Engineering and Built Environmen*t, Vol. 3 No.3 pp. 153-166, 2023.

[18] Fourie, D., The Role of Public Sector Enterprises in the South African Economy, *African Journal of Public Affairs*, Vol. 7 No.1 pp. 31-40, 2014.

[19] Galpin, T., Whitttington, J.L. and Bell, G., Is your Sustainability Strategy Sustainable? Creating a Culture of Sustainability, *Corporate Governance*, Vol. 15 No.1 pp. 1-17, 2015.

[20] Gopaul, K. and Oosthuizen, R., (2021) A Framework to Analyse a National Defense Industrial Base in a Globalised Market: The Case of the South African Defense industry: Proceedings of

the 15th INCOSE SA Annual Conference, Pretoria, 15-16 September. International Council on Systems Engineering.

[21] Halldórsdóttir, E., (2014) Limitations of Sustainability Implementation Amongst Project Managers, Case Study in an Icelandic energy company. MSc thesis. Chalmers University of Technology, Gothenburg.

[22] Huda, M., Safar, J., Mohamed, A.K., Jasmi, K.A. and Basiron, B., Transformational Islamic leadership: A Case Study from Singapore, *Global Perspectives on Teaching and Learning Paths in Islamic Education*, 76-91, 2019.

[23] Jones, J.M., (2021) Strategies to Overcome Constraints for Small Business Sustainability. PhD dissertation. Walden University, Minneapolis.

[24] Kanyane, M.H. and Sausi, K., Reviewing State-Owned Entities' Governance landscape in South Africa, *African Journal of Business Ethics*, Vol. 9 No.1 pp. 1-81, 2015.

[25] Kolzow, D.R., (2015) Leading from within: Building organisational Leadership Capacity, International Economic Development Council, p. 1-314

[26] Madumi, P., (2018) Are State-Owned Enterprises (SOES) Catalysts for or Inhibitors of South African Economic Growth? Proceedings of the 3rd Annual International Conference on Public Administration and Development Alternatives, Stellenbosch University, 04-06 July. IPADA.

[27] Martin, G., (2021) SA Defense Budget Falling to only 86% of GDP, DefenseWeb. Available from: https://www.Defenseweb.co.za/featured/sa-Defense-budget-falling-to-only-86-of-gdp/. [Accessed: 06 November 2022].

[28] Mashamaite, K. and Raseala, P., Transgression of Corporate Governance in South Africa's State-Owned Enterprises, *Journal of Sociology*, Vol. 16, No.1, pp. 124-134, 2018.

[29] Matthews, R. and Koh, C., The Decline of South Africa's Defense Industry, *Defense & Security Analysis*, Vol. 37, No 3, pp. 251-273, 2021.

[30] Mishra, A.K. and Aithal, P.S., Considerations and Conundrums that Confronted throughout the Recruiting Process, *International Journal of Research - Granthaalayah*, Vol. 10, No. 11, pp.18-31, 2022.

[31] Mukherjee, A., Leadership for Creating Sustainability within the Organisation: An Empirical Study, *The IUP Journal of Organisational Behaviour*, pp. 1-17, 2020.

[32] Muller, S.M, Amra, R. and Jantjies, D., (2015) Report on State-Owned Enterprises for Standing Committee on Finance, Parliament, Republic of South Africa, 1-62.

[33] National Defense Industry Council (NDIC), (2020) South African Defence Industry Strategy, pp. 1-20.

[34] Korkmaz, G., Supply Chain Risks and Management Strategies in the Defense Industry. *Journal of Defense Resources Management*, Vol. 15, No. 1, pp. 35–60, 2024.

[35] Liao, Y., Sustainable Leadership: A literature Review and Prospects for Future Research. *Frontiers in Psychology*, Vol. 13,- pp. 11, 2022.

[36] Ligita, Š. and Erika, Ž., Sustainable Leadership: The New Challenge for Organisations, *Forum Scientiae Oeconomia*, Vol. 2, No. 1, pp. 1-14, 2014.

[37] Limbo, C.M., (2019) An Analysis of the Performance of State-Owned Enterprises in Namibia : Case Studies in the Transport Sector. PhD (Economic and Management Sciences) Stellenbosch University.

[38] Le Roux, C., and Pretorius, M. Conceptualizing the Limiting Issues Inhibiting Sustainability Embeddedness, *Sustainability,* Vol. 8, No 4, pp. 1-22, 2016a.

[39] Le Roux, C and Pretorius, M., Navigating Sustainability Embeddedness in Management Decision-Making. *Sustainability, Special issue: How Better Decision-Making Helps to Improve Sustainability*, Vol 8, No. 5 p. 444, 2016b.

[40] Le Roux, C and Pretorius, M., Exploring the Nexus between Integrated Reporting and Sustainability Embeddedness, *Sustainability, Accounting, Management and Policy (SAMP) Journal. Special issue: The Nexus Between Integrated Thinking, Integrated Reporting and Governance,* Vol. 10, No. 5, pp. 822-843, 2019.

[41] Ojo, A.O. and Oluwatayo, I.B., (2016) Drivers and Challenges of Sustainable Development in Africa: Proceedings of the 3rd International Conference on African Development Issues, Covenant University Repository. 523-526.

[42] Orujov, R. and Mammadzada Mahammadali, V., The Effective Application of Strategic Communication in the Field of National Security', *Journal of Defense Resources Management*, Vol. 14, No. 2, pp. 57–66, 2024.

[43] Pálffy, Z., Ablonczy-Mihályka, L. and Kecskés, P., A Sustainable Model of Corporate Embeddedness: Navigating through a Fuzzy Concept, *Journal of Community Positive Practices,* Vol. XXIV, No. 2, pp, 115-135, 2024.

[44] Pearse, N. and Dimovski, V., Strategic Decision Making for Organisational Sustainability: The Implications of Servant Leadership and Sustainable Leadership Approaches, *Economic and Business Review*, Vol. 17, No.3, pp. 273-290, 2015.

[45] Perrott, B., The Sustainable Organisation: Blueprint for an Integrated Model, *Journal of Business Strategy*, Vol. 35, No. 3, pp. 26–37, 2015.

[46] Phela, M. T., (2024) Exploring the Limiting Issues Inhibiting Sustainability Embeddedness in Denel. Dissertation. University of South Africa, Pretoria

[47] Popa, B. M., Navigating Communication through the Challenges of the Actual Geopolitical Context. *Journal of Defense Resources Management*, Vol. 15, No. 2, pp. 184–193, 2024.

[48] Qhobosheane, L.A.M., (2018), The Impact of Political Interference on the State-Owned Companies: A case on SABC. LL.M. dissertation. University of Free State, Bloemfontein.

[49] Sakalasooriya, N., Conceptual Analysis of Sustainability and Sustainable Development. *Open Journal of Social Sciences*, Vol. 9, No. 3, pp. 396-414, 2021.

[50] Sarpong, D., Boakye, D., Ofosu, G. and Botchie, D., The three Pointers of Research and Development (R&D) for Growth-Boosting Sustainable Innovation System, *Technovation*, Vol. 122, pp. 1-9.

[51] Salkind, N.J. (2014) *Exploring research*. 8th Edition. Pearson Education International, Upper Saddle River, N.J..

[52] Sharafizad, J., Redmond, J. and Parker, C., The Influence of Local Embeddedness on the Economic, Social, and Environmental Sustainability Practices of Regional Small Firms, *Entrepreneurship and Regional Development*, Vol. 34, No. 1-2, pp. 57-81.

[53] Shamshiyeva, N., Military Culture and Defense Management in Azerbaijan: Contemporary

Transformations, *Journal of Defense Resources Management*, Vol. 15, No. 2, pp. 194–205, 2024.

[54] Simiyu, N.A., Role of Leadership in Organizational Development, School of Business, Technical University of Mombasa, *Journal of Management Studies*, 2015.

[55] Sithomola, T., (2019) Leadership Conundrum in South Africa's State-Owned Enterprises, (June), 62-80. Available from: https://ujcontent.uj.ac.za/vital/access/services/Download/uj:32937/SOURCE1?view=true. [Accessed: 07 July 2020].

[56] Tarei, P.K., Chand, P., Gangadhari, R.K. and Kumar, A., Analysing the Inhibitors of Complexity for Achieving Sustainability and improving Sustainable Performance of Petroleum Supply Chain, *Journal of Cleaner Production*, 310, 2021.

[57] Thakhathi, A. (2016) Strategising Practices of Sustainability Champions: A Case Study at a State-Owned Enterprise. Dissertation. University of South Africa, Pretoria.

[58] Thakhathi, A, Le Roux, C and Davis, A., Sustainability Leaders' Influencing Strategies for Institutionalising Organisational Change towards Corporate Sustainability: A Strategy-as-Practice Perspective, *Journal of Change Management*, 2019.

[59] Trollman, H. and Colwill, J., The Imperative of Embedding Sustainability in Business: A Model for Transformational Sustainable Development, *Sustainable Development*, Vol. 29, No.5, pp. 974-986, 2021.

[60] University of Cambridge Institute for Sustainability Leadership (CISL), (2017) A Report Commissioned by the British Council. Global Definitions of Leadership and Theories of Leadership Development: Literature Review, pp. 2-50.

[61] Valente, M., Business Sustainability Embeddedness as a Strategic Imperative: A Process Framework, *Business and Society*, Vol. 54, No. 1, pp. 126-142, 2015.

[62] Wamu, S., Winkler, K. and Lundsten, J., (2023) Sustainability Leadership and Employee Satisfaction in Small and Medium-sized Enterprises, An Exploratory Study in Germany and Sweden. Malmö University.

[63] Williams, T., Edwards, M., Angus-Leppan, T., and Benn, S., Making Sense of Sustainability Work: A Narrative Approach, *Australian Journal of Management*, Vol. 46, No. 4, pp. 740-760. https://doi.org/10.1177/03128978447

[64] Wippermann, F., Instigating the Permanent Change of Business Models, *Business Management Dynamics*, Vol. 6, No. 9, pp. 25-38, 2017.

[65] Yin, R.K., (2018) *Case Study Research and Applications: Design and Methods* (6th ed.). Sage, Thousand Oaks, CA.

[66] Yusuf, R.N.. Moeljadi, M., Sutrisno, S., Susilo, A.K., Strategic Advantage of State-Owned Enterprises (SOEs) Development Policies in Strengthening Naval Armaments, *Journal of Defense Resources Management*, Vol. No.2, pp. 51-66, 2024.

[67] Zogjani, J. and Raçi, S., The Role of Leadership in Achieving Sustainable Organizational Change and the Main Approaches of Leadership during Organizational Change, *Academic Journal of Interdisciplinary Studies*, Vol. 4, No. 3, pp. 65-70, 2015.

FOOD SECURITY AND ITS IMPACT ON SAUDI ARABIA'S NATIONAL SECURITY AND GULF SECURITY

Bader Al HARBI[*], **Faiz MMT MARIKAR**[**]

[*] National Defence College, Colombo 03, Sri Lanka
[**]General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka

This study investigates the relationship between food security and national security in Saudi Arabia and the Gulf region. It examines the impact of food insecurity on Saudi national security and the broader Arabian Gulf security, identifies the major challenges and limitations facing current food security policies and programs, and proposes strategic recommendations for enhancing food security. The study reveals direct impacts such as social unrest, economic instability, health implications, and migration, while also highlighting indirect impacts including political instability, economic consequences, social fragmentation, demographic pressures, and regional instability. The identified challenges encompass climate change, water scarcity, reliance on food imports, inefficient agricultural practices, socioeconomic disparities, and limited technology adoption. To address these challenges, the study recommends prioritizing comprehensive food security policies, increasing investments in agriculture, research, and infrastructure, and fostering collaboration among governments, international organizations, academia, and the private sector. The findings underscore the significance of addressing food security to ensure national and regional stability and resilience in the face of evolving food security concerns.

Key words: *Food security, national security, Saudi Arabia, Gulf region*

1. INTRODUCTION

Food security is a significant concern for Saudi Arabia and the Gulf region due to their substantial reliance on food imports and susceptibility to environmental and economic disruptions (Alrobaish et al., 2021). The Kingdom has several difficulties jeopardising food security, such as rapid population increase, acute water scarcity, the effects of climate change, and evolving dietary trends (Lambert & Hashim, 2017). Food insecurity in the region can profoundly affect national and regional security, leading to economic instability, social discontent, and political turmoil (Haque, & Khan, 2022).

Saudi Arabia, the largest economy in the Gulf area and a vital strategic hub, confronts considerable dangers, as any disruption to food supplies or escalation in food prices might generate enormous ripple effects throughout the region and beyond (Mohieldin et al., 2024). In recent years, Saudi Arabia and other countries in the Gulf have initiated various programs and initiatives to bolster food security, encompassing investments in advanced agricultural technology, aquaculture development, food processing, and policies designed to minimise food waste and enhance food safety (Al-Khateeb et al., 2021). Nonetheless, much effort is required to tackle the fundamental causes of food insecurity and to guarantee the stability and security of the region's food supply amidst increasing demand and climate change.

The security of the countries in the Gulf Cooperation Council (GCC) is increasingly endangered by intellectual movements that advocate extremist ideologies, incite violence, and destabilize the area. Saudi Arabia, as a member of the GCC, has been actively involved in addressing these concerns (Hameed et al., 2022). However, the ongoing threat posed by extremism continues to persist. To address this problem, the study could comprehend the complex characteristics of extremist beliefs, the different routes to radicalization, and how extremist organizations manipulate technology and social media platforms. The existence of unrest in nearby regions adds complexity to the task of combining security measures with concerns about civil liberties. Additionally, the significance of international cooperation further complicates attempts to tackle these dangers. Evaluating the efficacy of extremism programs is intricate because of their subtle and enduring effects. It is crucial to tactfully negotiate cultural and religious sensitivities to avoid estranging communities. Adapting policies comprehensively to respond to emerging threats is vital for enhancing the security of GCC members and ensuring durable regional peace, notwithstanding investments in counterterrorism efforts and measures for de radicalization.

The aim of this research is to examine the relationship between food security and Saudi national security, as well as its impact on Gulf security. Therefore, the objectives have been established in the following manner: To assess the impact of food insecurity on Saudi national security and the Arabian Gulf security. To identify the major challenges and limitations facing current policies and programs for enhancing food security in Saudi Arabia and the Gulf and evaluate their effectiveness in addressing food insecurity.

The framework shown in Figure 1 suggests that food security is the independent variable that can have an impact on the dependent variables of Saudi national security and Gulf security. The control variables of population and climate change are likely to influence the relationship between food security and the dependent variables, and the intermediate variables of political stability and military capability may mediate the relationship.

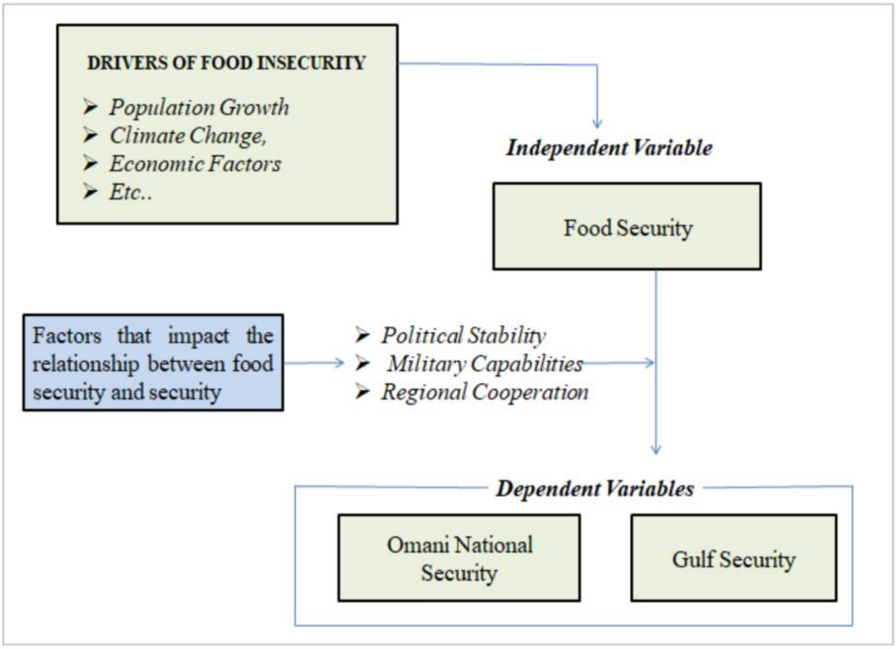


Fig. 1 Conceptual Framework
Source: author’s own work

The proposed relationship suggests that food security, as an independent variable, may directly or indirectly influence the dependent variables of Saudi national security and Gulf security. The relationship is shaped by control variables such as population and climate change, which impact food availability and access. Additionally, intermediate variables like political stability and military capability affect the Kingdom's capacity to address food-related challenges and ensure security.

Food security represents a significant challenge in Saudi Arabia and the broader Gulf region, attributed to dependence on food imports, susceptibility to external influences like climate change, and a rising demand for food. The literature indicates a strong correlation between food security and national and regional security, with food shortages potentially resulting in social unrest, political instability, and conflict.

1.1. Research Methodology

The methodology for conducting the search will entail a series of steps, which will be carried out systematically and transparently to minimize potential bias and ensure reproducibility of the search results.

Research Design: The research will utilize a descriptive research design that aims to describe the current state of food security and its impact on Saudi national security and Gulf security. Secondary data sources will be used to collect data on food security and national security indicators.

Data Sources: Secondary data sources will be obtained from various sources such as government reports, academic articles, and international organizations' publications. The sources will be identified and reviewed through a systematic literature search using online databases.

Data Collection: Data will be collected by conducting a comprehensive review of the existing literature on food security, national security, and their relationship in Saudi Arabia and the Gulf region. The review will include a qualitative synthesis of the findings, and the main themes and patterns will be identified.

Data Analysis: The data collected through the literature review will be analyzed using a thematic analysis approach. The themes and patterns identified in the literature will be categorized into different groups and subgroups. The findings will then be presented in a descriptive format, highlighting the relationships and interactions between food security and national security in Saudi Arabia and the Gulf region.

2. RESULTS AND DISCUSSION

Food Security Categories. Food security is a complex and multifaceted concept that encompasses various dimensions related to the availability, access, utilization, and stability of food. As a result, different forms or categories of food security have been developed to help understand and address the different aspects of this complex issue. These categories shown in Figure 2, each of these categories has its own unique characteristics and challenges and understanding them is crucial for developing effective policies and programs to ensure access to sufficient and nutritious food for all.

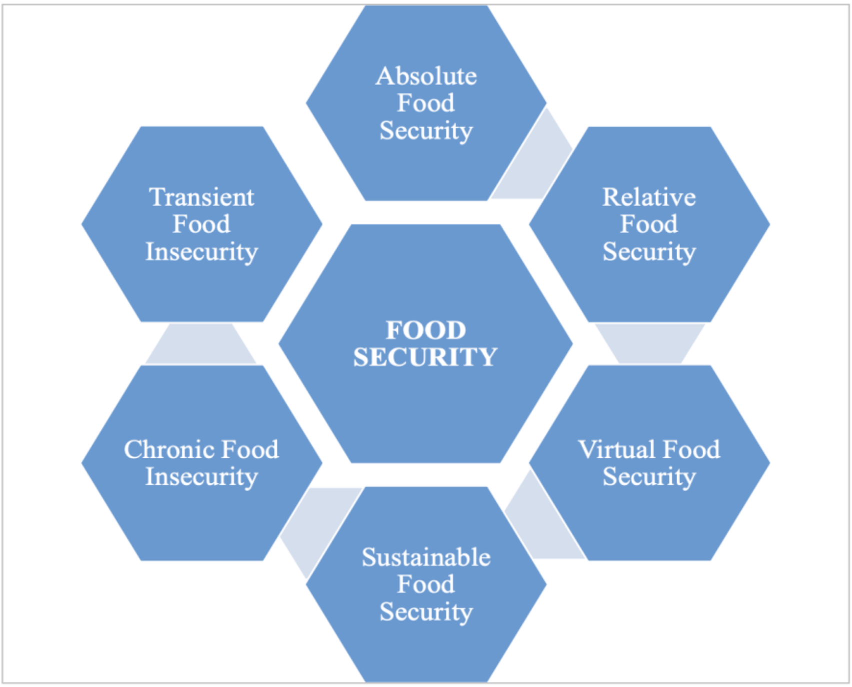


Fig. 2 Food Security Categories Diagram
Source: author's own work

Absolute Food Security: Also known as self-sufficiency, means that a country can produce enough food domestically to meet its local demand, with the possibility of exporting the surplus. In this case, the country does not depend on imports to ensure food security. Self-sufficiency is a desirable state for many countries, as it reduces the dependence on other nations and can boost the domestic economy.

Relative Food Security: Refers to a country's ability to provide some food and nutritional resources either wholly or partly and to ensure the minimum level of food requirements on a regular basis. In this case, the country may depend on imports to complement its domestic food production, but it has established policies and mechanisms to ensure that the population has access to a sufficient quantity and quality of food.

Apparent or Virtual Food Security: Is a situation where a country produces 90% or more of a certain material from its domestic production, but imports most of its inputs, such as seeds, fertilizers, and machinery. In this case, the country's domestic production figures can be misleading, and its food security may not be as robust as it seems.

Sustainable Food Security: Refers to a long-term strategy that aims to increase agricultural productivity while enhancing the productive capacity of natural resources. This involves promoting sustainable agricultural practices, such as crop rotation, soil conservation, and water management, to ensure that the production capacity of the land is maintained over time.

Chronic Food Insecurity: Refers to inadequate food production due to a constant deficit in food acquisition. This is a persistent and long-term problem that affects the population's health and well-being. Chronic food insecurity can be caused by a combination of factors, such as poverty, conflict, climate change, and lack of investment in agriculture.

Transient Food Insecurity: It is a temporary decline in a household's ability to acquire sufficient food, such as in the case of natural disasters, food price instability, and loss of employment. This type of food insecurity is usually short-term and can be mitigated through emergency relief programs, such as food aid, cash transfers, and employment schemes.

Dimensions of Food Security. Food security is a critical issue that affects individuals, households, and communities worldwide. It is a multi-dimensional concept that encompasses various aspects of food availability, access, utilization, and stability.

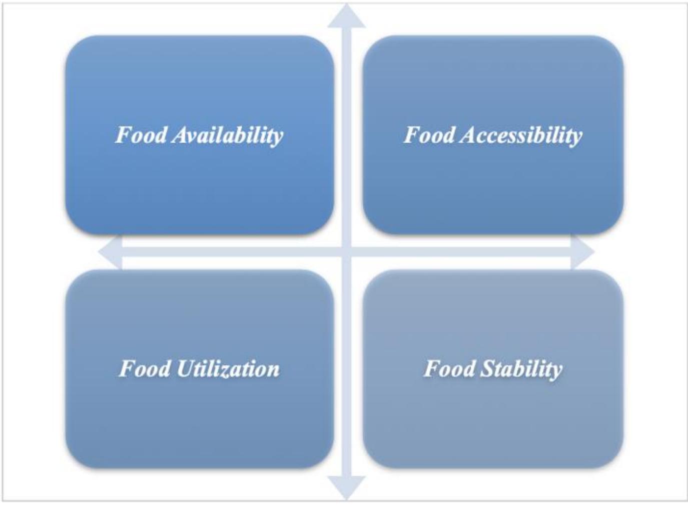


Fig. 3 Dimensions of Food Security diagram
Source: author's own work

The first dimension of food security is availability, which refers to the physical presence of food in sufficient quantities at national, regional, and local levels (Figure 3). Availability involves the production, storage, and distribution of food. A country with a high level of agricultural production and adequate storage facilities can ensure the availability of food. For example, Saudi Arabia has invested significantly in agricultural technology and storage infrastructure to enhance food availability (El-Dukheri, 2024).

The second dimension of food security is accessibility, which refers to the ability of individuals and households to obtain food through markets, trade, and social safety nets. Accessibility involves economic, social, and physical access to food. For example, Saudi Arabia has implemented various social welfare programs to ensure food accessibility for vulnerable populations (Alrobaish et al., 2021).

The third dimension of food security is utilization, which refers to the ability of individuals and households to consume food that meets their dietary needs and preferences. Utilization involves the quality and safety of food, as well as knowledge and behaviours related to food preparation and consumption. For example, Saudi Arabia has implemented comprehensive food safety regulations and nutritional education programs (Ayad et al., 2022).

The fourth dimension of food security is stability, which refers to the ability of individuals and households to maintain food security over time, even in the face of shocks and stresses such as natural disasters, economic downturns, or conflicts. For example, Saudi Arabia has established strategic food reserves and diversified its food import sources to ensure stability (Elrasheed, 2024).

Food insecurity poses significant challenges to national security in both Saudi Arabia and the Gulf region. Direct impacts include social unrest, economic instability, dependency on imports, health implications, and migration and displacement. Social unrest arises from inadequate access to food, leading to public dissatisfaction, protests, and potential violence, particularly in densely populated urban areas of the Kingdom. Economic instability occurs due to decreased productivity, increased healthcare costs, disruptions in agriculture, and supply chain disruptions, with Saudi Arabia spending approximately SAR 87 billion annually on food imports (Alderiny et al., 2020). Dependency on imports exposes the Kingdom to fluctuations in global food prices and supply disruptions, with over 80% of food requirements being imported. Health implications include malnutrition, weakened immune systems, and increased vulnerability to diseases, affecting approximately 12% of the Saudi population (Bin Sunaid et al., 2021). Migration and displacement occur as people, particularly from rural agricultural areas, are compelled to search for better access to food and economic opportunities in urban centres, straining resources and potentially causing conflicts.

The indirect impacts of food insecurity encompass political instability, economic consequences, social fragmentation, demographic pressures, and regional instability. Political instability arises from discontent, protests, and challenges to government authority, affecting national security particularly in regions with high unemployment rates (Albejaidi & Nair, 2021). Economic consequences include hindered economic growth, decreased productivity, and limited resources for addressing security challenges, with an estimated annual economic impact of SAR 23 billion (Alharbi et al., 2021). Social fragmentation arises from divisions due to competition for resources, deepening inequalities, and social unrest, particularly evident in the Kingdom's rapidly urbanizing areas. Demographic pressures arise from increased poverty, unemployment, and migrations driven by food insecurity, straining resources and contributing to social tensions, especially given Saudi Arabia's 1.7% annual population growth rate. Regional instability emerges when neighbouring countries face food insecurity, leading to resource conflicts and regional tensions impacting national security, particularly relevant given the Kingdom's strategic position in the Gulf region.

Current policies and programs for enhancing food security in Saudi Arabia and the Gulf face significant challenges and limitations. Climate change, water scarcity, and limited arable land pose major obstacles to agricultural production and food self-sufficiency, with only 1.6% of the Kingdom's land being arable (Al Naimi, 2022). The reliance on food imports makes the region vulnerable to global price fluctuations and supply disruptions. Inefficient water management practices and unsustainable agricultural methods further exacerbate the problem, with agriculture consuming approximately 84% of Saudi Arabia's water resources (Alrwis et al., 2021). Additionally, socio-economic disparities, lack of access to resources for small-scale farmers, and limited technology adoption hinder progress. While efforts have been made to enhance food security through investment in agricultural infrastructure, technology adoption, and diversification of food sources, the effectiveness of these policies and programs in fully addressing food insecurity remains a continuous challenge.

In this study indicate that food insecurity substantially affects security at both national and regional levels via various pathways. The study illustrates that food insecurity can significantly weaken political systems, provoke social unrest, and jeopardise economic stability. Limited food access and rising prices can lead to public dissatisfaction, which may manifest as protests that have the potential to escalate into more severe conflicts. The data indicates that food insecurity exacerbates social inequalities and economic vulnerabilities, creating further security challenges. Food-related hardships often lead to population displacement and migration as communities pursue improved opportunities, thereby straining resources in destination areas and increasing social tensions. The health consequences of food insecurity, notably prevalent malnutrition and heightened vulnerability to diseases, exacerbate security issues by undermining community resilience.

This study concludes, based on comprehensive data analysis and contextual examination, that a significant correlation exists between food insecurity and security threats in KSA and the Arabian Gulf region. The empirical evidence robustly corroborates our initial hypothesis, illustrating the complex relationship between food security and regional stability**.**

3. CONCLUSION

This study has identified multiple effective strategies to tackle the intricate challenges confronting Oman and the Arabian Gulf region in achieving food security. Our findings highlight the essential need for a comprehensive and cohesive strategic framework. A comprehensive framework should include various interconnected aspects of food security, such as improved agricultural productivity, effective water resource management, reinforced climate resilience strategies, and streamlined trade networks. The research underscores the importance of ongoing investment in research and development, systematic capacity-building initiatives, strategic land use planning, comprehensive waste reduction programs, and robust social safety net mechanisms. The study concludes that adopting sustainable agricultural practices, fostering technological innovation, and cultivating solid collaborative relationships among key stakeholders in both the public and private sectors are fundamentally important. Moreover, these initiatives require robust policy frameworks and governance structures to guarantee their sustainability and effectiveness in meeting regional food security goals. This comprehensive strategy, underpinned by evidence-based policymaking and intersectoral collaboration, signifies the region's most effective route to achieving sustainable food security.

4. RECOMMENDATIONS

The Saudi government must give top priority to the development and implementation of comprehensive food security policies to address these pressing issues. These policies must incorporate the following identified strategies and methods:

The government should prioritize the creation and implementation of comprehensive food security policies that align with Vision 2030's goals, incorporating modern agricultural technologies and sustainable practices. This includes expanding the current SAR 5 billion agricultural technology investment program to cover 75% of the Kingdom's farming operations by 2026 (Bin Sunaid et al., 2021).It is essential to increase investments in agriculture, research and development, and infrastructure to facilitate the transition to more sustainable and resilient food systems. Collaboration between Saudi government entities, international organizations, the academic community, and the private sector is essential for knowledge sharing, technology transfer, and coordinated efforts to address food security issues. Food security strategies should prioritize the incorporation of climate change adaptation and mitigation measures, particularly given Saudi Arabia's vulnerability to rising temperatures and water scarcity. To promote sustainable consumption patterns, reduce food waste (currently at 33%), and increase nutritional awareness, public awareness campaigns and educational programs should be initiated through a coordinated national strategy. Strengthening social safety nets, targeting vulnerable populations and ensuring their access to adequate and nutritious food should be a priority. To assess the efficacy of implemented strategies and make necessary adjustments, continuous monitoring, evaluation, and adaptive management techniques should be utilized through the newly established National Food Security Monitoring Centre.

5. FUTURE WORK

To increase our comprehension of regional dynamics and develop context-specific solutions for Saudi Arabia, additional research is required in the following areas: Economic viability studies of implementing proposed strategies and policies, particularly focusing on the cost-effectiveness of water conservation technologies and desert agriculture. Evaluation of social and environmental impacts of agricultural interventions in the Kingdom's different ecological zones.

Investigation of potential implementation barriers, especially regarding technology adoption among small-scale farmers. Research on the role of technology, digitalization, and precision agriculture in enhancing food security in Saudi Arabia, with particular emphasis on artificial intelligence and IoT applications. Studies on the integration of traditional knowledge with modern agricultural practices in the Saudi context. Analysis of climate change impacts on future food security scenarios specific to Saudi Arabia's geographical conditions. Assessment of the effectiveness of regional cooperation mechanisms in enhancing food security. Investigation of innovative financing mechanisms for food security projects in the Kingdom. This research agenda should be pursued through collaborative efforts between Saudi research institutions, international partners, and the private sector, with adequate funding and support from relevant government agencies.

6. RESEARCH LIMITATIONS

During the conducting of this thesis and during the analysis of the necessary files and books, the researcher revealed some of the determinants, which are as follows: Limited Data Availability: Due to the sensitive nature of national security issues, challenge in accessing reliable and comprehensive data, which can limit the scope of study. Lack of Empirical Studies: While there are many theoretical and conceptual studies on the link between food security and national security, there is a lack of empirical research that examines the causal relationships between these variables. Lack of Longitudinal Studies: Few studies have examined the long-term trends in food security and its impact on national security in the region, which can limit our understanding of how these issues are evolving over time. Methodological Limitations: Different studies use different methods and definitions of food security, making it difficult to compare results across studies and draw firm conclusions.

REFERENCES

[1] Albejaidi, F. and Nair, K.S., 2021. *Nationalisation of health workforce in Saudi Arabia’s public and private sectors: A review of issues and challenges*. Journal of Health Management, 23(3), pp.482-497.

[2] Alderiny, M.M., Alrwis, K.N., Ahmed, S.B. and Aldawdahi, N.M., 2020. *Forecasting Saudi Arabia’s production and imports of broiler meat chickens and its effect on expected self-sufficiency ratio*. Journal of the Saudi Society of Agricultural Sciences, 19(4), pp.306-312.

[3] Alharbi, A.S., Halikias, G., Rajarajan, M. and Yamin, M., 2021. *A review of effectiveness of Saudi E-government data security management*. International Journal of Information Technology, 13, pp.573-579.

[4] Al-Khateeb, S.A., Hussain, A., Lange, S., Almutari, M.M. and Schneider, F., 2021. *Battling food losses and waste in Saudi Arabia: mobilizing regional efforts and blending indigenous knowledge to address global food security challenges*. Sustainability, 13(15), p.8402.

[5] Al Naimi, S.M., 2022. *Economic diversification trends in the Gulf: The case of Saudi Arabia.* Circular Economy and Sustainability, pp.1-10.

[6] Alrobaish, W.S., Vlerick, P., Luning, P.A. and Jacxsens, L., 2021. *Food safety governance in Saudi Arabia: Challenges in control of imported food*. Journal of Food Science, 86(1), pp.16-30.

[7] Alrwis, K.N., Ghanem, A.M., Alnashwan, O.S., Al Duwais, A.A.M., Alaagib, S.A.B. and Aldawdahi, N.M., 2021. *Measuring the impact of water scarcity on agricultural economic development in Saudi Arabia.* Saudi Journal of Biological Sciences, 28(1), pp.191-195.

[8] Ayad, A.A., Abdulsalam, N.M., Khateeb, N.A., Hijazi, M.A. and Williams, L.L., 2022. *Saudi Arabia household awareness and knowledge of food safety*. Foods, 11(7), p.935.

[9] Bin Sunaid, F.F., Al-Jawaldeh, A., Almutairi, M.W., Alobaid, R.A., Alfuraih, T.M., Bensaidan, F.N., Alragea, A.S., Almutairi, L.A., Duhaim, A.F., Alsaloom, T.A. and Jabbour, J., 2021. *Saudi Arabia's healthy food strategy: Progress & hurdles in the 2030 road*. Nutrients, 13(7), p.2130.

[10] El-Dukheri, I., 2024. *The Implications of Agricultural Saudi Arabia Investment Abroad on Food Security*. In Food and Nutrition Security in the Kingdom of Saudi Arabia, Vol. 2: Macroeconomic Policy and Its Implication on Food and Nutrition Security (pp. 97-127). Cham: Springer International Publishing.

[11] Elrasheed, M.M., 2024. *Strategic Food Reserve Management and Food Security in Saudi Arabia.* In Food and Nutrition Security in the Kingdom of Saudi Arabia, Vol. 1: National Analysis of Agricultural and Food Security (pp. 405-424). Cham: Springer International Publishing.

[12] Hameed, S., Quamar, M.M. and Kumaraswamy, P.R., 2022. *GCC. In Persian Gulf 2021–22: India's Relations with the Region* (pp. 503-534). Singapore: Springer Nature Singapore.

[13] Haque, M.I. and Khan, M.R., 2022. *Impact of climate change on food security in Saudi Arabia: a roadmap to agriculture-water sustainability.* Journal of Agribusiness in Developing and Emerging Economies, 12(1), pp.1-18.

[14] Lambert, L.A. and Hashim, H.B., 2017. *A century of Saudi-Qatari food insecurity: paradigmatic shifts in the geopolitics, economics and sustainability of Gulf states animal agriculture*. The Arab World Geographer, 20(4), pp.261-281.

[15] Mohieldin, M., Amin-Salem, H., El-Shal, A. and Moustafa, E., 2024. *Navigating the Storms. The Political Economy of Crisis Management and Reform in Egypt*, pp.59-107.

IDENTIFICATION OF KEY FACTORS IN THE DEVELOPMENT OF NAVAL BASES IN MAINTAINING MARITIME SECURITY IN INDONESIA

Atiq ALFIANSYAH, Yoyok NURKARYA, Joko PURNOMO

Indonesia Naval Technology College, Morokrembangan, Surabaya, Indonesia

The dynamics of the strategic environment in ALKI II continue to evolve due to geopolitical changes, increased international trade activities, and the potential for increasingly complex maritime security threats. This condition demands the optimization of the role of the Naval base as an operational control center in maintaining regional stability and sovereignty. The base must be able to function effectively in maritime surveillance, improve operational readiness, and strengthen its ability to respond to various threats, both from state and non-state actors.

This study aims to analyze the factors that influence the development of naval bases in supporting Indonesia's maritime defense and security. Using the Delphi method approach, this study involved 15 experts in the field of maritime defense and security. Through a systematic analysis process, this study succeeded in identifying 39 main factors that play a role in the development of the Naval base. These factors include aspects of base infrastructure, level of expertise, territorial control, operating patterns, defense, coastal defense, political, economic, social and technological aspects.

The results of this research are expected to be the basis for the formulation of a strategy to strengthen naval bases that are more adaptive, modern, and able to respond to future maritime security challenges effectively and sustainably.

Key words: *Development Planning, Naval Base, Delphi, Maritime Security.*

1. INTRODUCTION

The development of the strategic environment at the global level shows that there is increasingly intense competition between the world's great powers (Zendelovski, 2024). In modern geopolitical dynamics, countries with superior military capabilities tend to have a stronger bargaining position in relations (Nye & Keohane, 1990). This is due to their ability to defend sovereignty, protect national interests, and project power in various strategic areas (Budiana & Budiman, 2024).

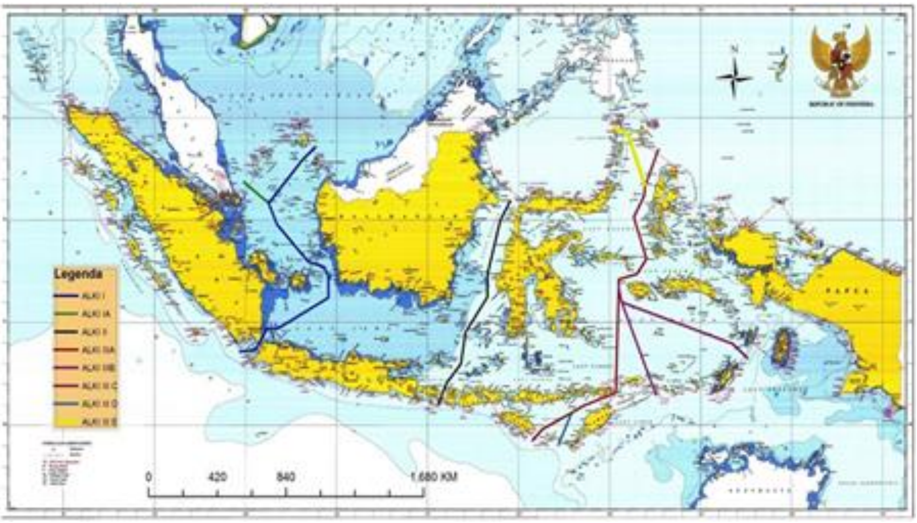


Fig. 1. Map of the Sea Channel of the Indonesian Archipelago.

Indonesia as the largest archipelagic country in the world plays an important role in the global maritime map with its abundant marine resource potential, as well as a strategic crossing route in the Indonesian Archipelago Sea Channel (ALKI) for international shipping connecting the Indian Ocean and the Pacific Ocean (Cribb & Ford, 2009). This strategic position makes Indonesia not only a center of maritime economic activities, but also a region that is vulnerable to various global interests (Attamimi, 2024). As a result of increasingly fierce global competition, various potential threats have emerged that can disrupt national security stability (Horowitz et al., 2022). These threats are not only conventional, but also increasingly complex and vary with the times. Conflicts of interest between countries often trigger tensions in various strategic sectors, including economic, political, and defense. Traditional forms of threats faced include military conflicts, territorial violations, and foreign infiltration that can threaten the country's sovereignty. Meanwhile, non-traditional threats are on the rise, such as piracy in the waters, smuggling of illegal goods, human trafficking, as well as cybercrime that attacks national digital infrastructure (Arto et al., 2019). In addition, terrorist activities are also a serious threat that has the potential to shake the stability of the country. Not only that, the uncontrolled exploitation of natural resources also causes environmental damage that has an impact on ecosystem sustainability and community welfare.

In addition, military dominance also plays a role in determining the direction of global policy, both in economic, diplomatic, and security aspects (Buyukakinci, 2024). Therefore, Indonesia needs to strengthen its maritime defense to be able to face various increasingly complex challenges. One of the strategic steps that can be taken is to increase the capacity and infrastructure of the Navy base (Amelia et al., 2022). Naval bases must continue to function optimally in accordance with their role and not experience decreased effectiveness (degradation) in the face of various threats, disturbances, obstacles, and challenges. Thus, the Naval base can continue to operate optimally in maintaining the sovereignty and security of Indonesia's maritime territory.

This research aims to identify the factors necessary in the development of a Naval base. The implementation of this research is important to provide an overview of efforts to maintain sovereignty and maintain national security stability, especially in ALKI areas that are vulnerable to various threats, both traditional and non-traditional (Sartono et al., n.d.). In addition, this research contributes to the field of maritime defense by formulating base development strategies that are adaptive, effective, and in accordance with global challenges. The analysis is carried out based on various key aspects, including base infrastructure, personnel competence, territorial control, operating patterns, and coastal defense, so as to create sustainable and optimal maritime security.

This research is supported by sea power theory, maritime security theory and base theory. Statistical descriptive qualitative methods are used in the research to analyze survey data and factors of the Navy base, qualitative methods use approaches such as delphi to explore the opinions of relevant experts in the field of maritime defense involving 15 (fifteen) experts from stakeholders academia and practitioners, this consensus is important to understand the relationship between strategic variables and produce solutions based on collective thinking, While descriptive statistics are used to analyze the data obtained such as the assessment scale in the questionnaire, identifying priorities and patterns of relationships between elements.

This research offers several contributions. First, the study develops a theoretical framework that integrates various theories to provide a deeper understanding of how bases can adapt to changing threats and defense needs. Second, in terms of practical implications, this study provides concrete recommendations for infrastructure development, the application of advanced technologies and policies related to sustainable base management. These recommendations not only enhance Indonesia's maritime defense capacity, but also offer practical guidance for policy-making and operational management of bases, so that they can be better prepared to face evolving global challenges.

2. LITERATURE REVIEW

2.1. Sea Power Theory

The Sea Power theory developed by Alfred Thayer Mahan is one of the important pillars in the study of maritime power. Mahan emphasized the importance of the strength of the sea fleet supported by maritime infrastructure, namely the existence of bases or ports that have a strategic role for ships sailing (MacHaffie, 2020).

Sea power is not only about having a powerful warship, but also the ability to maintain and project that power (Grove, 2021). This is where the importance of the seabase lies. The base is a critical element that allows fleet operations to take place effectively and sustainably. Without an adequate base, sea power will lose its flexibility, logistics become disrupted, and power projection capabilities are limited (Marsetio, 2019).

2.2. Marine Safety Theory

Maritime security theory refers to multidimensional efforts to address threats in the maritime region that include inter-state conflicts, maritime terrorism, piracy, illegal trade, and environmental damage.

As a dynamic concept, maritime security is often considered a buzzword in international relations, reflecting uncertainty in definition but creating a foundation for cross-actor coordination. Bueger (2015) in his article proposes three main approaches to understand maritime security, namely First, through the maritime security matrix which connects security with other concepts such as marine safety, sea power, blue economy and resilience (Chapsos, 2016); Second, a securitization framework that explores how threats are politically constructed (Piedade, 2016); Third, the theory of security practices that focus on real actions such as maritime patrols and law enforcement (Bueger, 2013).

Wibawa et al (2021) emphasized this theory emphasizing the need for international and cross-sectoral collaboration to create inclusive and sustainable security in the maritime region.

2.3. Base Theory

Bases are one of the pillars in military strategy that underlie the planning and implementation of armed forces operations in various parts of the world (Zulham & Saragih, 2019). Alfred Thayer Mahan (1890) first emphasized the importance of a strong base as a key element in creating maritime dominance and maintaining the stability of global trade routes. The effectiveness of a base is determined by its location, especially in a major trade route or strategic area (Bell & Griffis, 2015). In addition, technological developments in the 20th century added new dimensions to this theory, such as air bases, cross-domain bases, to space bases that integrate radar, satellite communications, and air defense systems.

In the 21st century, the concept of military bases continues to evolve by adopting a forward operating bases (FOB) approach to support military operations in conflict areas (Wong, 2006). FOBs are designed to be smaller but flexible, such as those applied by the United States military in the wars in Afghanistan and Iraq.

In the modern context, bases are becoming an integral part of multi-domain strategies that span land, sea, air, cyber, and space, making them relevant in the face of traditional and non-traditional threats such as terrorism, piracy, as well as cyberattacks. The base also functions to support operations through five main functions: rebase, refuelling and replenishment, repair, and rest and recreation (Okol, 2015).

3. METHOD

The type of research used in this study is categorized as qualitative research with descriptive statistics referring to (Widyaksa et al., 2024). This study uses literature from journal articles, interviews, and observations as a method of data collection. Data was collected through questionnaires given to 15 expert panels to reach consensus using the Delphi method, with the aim of identifying factors influencing the development of the Naval Base.

To analyze the survey data, a descriptive statistical approach is used, which presents statistics and percentages of each aspect of the criteria. The Delphi method is applied in two stages, namely the pre-Delphi study and the successive Delphi study.

In the pre-Delphi stage, research indicators were identified based on the approach developed by (Okoli & Pawlowski, 2004). Furthermore, the data that has been collected is analyzed using Nvivo software for qualitative analysis and Microsoft Excel for quantitative analysis.

3.1. Selection criteria for the expert panel

The Delphi method relies on the selection of experts who have in-depth insight into the issue under study (Flanagan et al., 2016). In qualitative research, the role of experts is crucial, so demographic details that explain their credentials are needed. This step aims to assess the level of expertise and ensure that they are truly competent in contributing to the research. The selection of experts is carried out based on predetermined criteria, such as education level, field of expertise, experience, and professional activities.

These criteria are designed to maintain the credibility of the research by ensuring that the experts involved are reputable and respected individuals in their fields. Previous research has also confirmed that the selected experts must have a strong scientific foundation, as well as sufficient experience and skills to support the validity of the research results.

Table 1. Demographic information of the experts.

Characteristics	**Amount**	**Percentage**
	n	**%**
Rank		
Major	1	0,07
Liutenant Colonel	4	0,27
Colonel	10	0,67
Work Experience		
16 Y-20 Y	1	0,07
21 Y- 25 Y	4	0,27
> 25 Y	10	0,67
Graduate		
Post Graduate	13	0,87
Doctoral/Phd	2	0,13

3.2. Delphi Method

The Delphi method was developed by Derlkey and his associates at the Rand Corporation, California in the 1960s. The Delphi method is a method that harmonizes the communication process of a group so that an effective process is achieved in obtaining solutions to complex problems. The Delphi method aims to reach consensus from a series of information mining processes. In carrying out the Delphi method, opinions and judgments from experts and practitioners are needed (Halim et al., 2021). In carrying out the Delphi method, opinions and judgments from experts and practitioners are needed.

In the Delphi method, 10-15 problem topic items are suggested, while the number of respondents is suggested between 15-20 respondents (Lee et al., 2020). The process of implementing the Delphi method is approximately 45 days with a span of two weeks per round of the panel. The consensus process in the Delphi method occurs when there is a percentage of 80% of all members with a score scale of 0-7. Gunduz & Elsherbeny (2020) suggest at least 70% with the average value of each item of questionnaire points being three or four Likert scales and having a median score of at least 3.25.

According to Karakikes & Nathanail (2020), there are three main steps in this process, namely:

a) The first questionnaire was sent to the expert panelists to ask them for some of their opinions (from experience or within their assessments), some predictions and also their recommendations.
b) In the second round, a summary of the results of the first questionnaire was sent to each expert panelist to be able to re-evaluate their first assessment on the questionnaire using the set criteria.
c) In the third round, the questionnaire was given again with information about the results of the panelists' assessment and the consensus results. The panelists were asked again to revise their opinions or explain the reasons for disagreeing with the group consensus.

3.3. Content Validation Index (CVI)

The Content Validity Index (CVI) is an important method for assessing the content validity of an instrument and is widely used in various fields of research. The CVI measures the level of agreement among experts regarding the relevance or representativeness of each item in an instrument. This method provides insight into the validity of content, both at the level of a specific item (Item-level CVI/I-CVI) and as a whole in a single instrument (Instrument-level CVI). The CVI calculation is carried out based on the evaluation of experts on each item, taking into account the extent to which the item is relevant or represents the concept being measured (Almanasreh et al., 2018).

To explore the factors that influence the panel's agreement regarding the achievement of Minimum Essential Strength (MEF) in a domain during the Delphi process, standard mean and deviation calculations were used to measure the degree of factor convergence. A panel of experts assessed the level of importance of each goal using a 5-point Likert scale, which helps in understanding the extent to which agreement was reached among the experts (Stancine et al., 2019). To assess the validity of the content, this study used the item-level content validity index (I-CVI) and the scale-level average content validity index (S-CVI/Ave). S-CVI/Ave is determined by dividing the number of I-CVI scores by the number of items. An S-CVI/Ave of ≥0.8 is considered acceptable, while an S-CVI/Ave of ≥0.90 indicates excellent overall content validity. On the other hand, I-CVI is calculated from the number of experts who assess an item ≥3 divided by the total number of experts, with I-CVI ≥0.78 acceptable. The literature suggests that for a new assessment instrument to be considered valid, it must achieve a total CVI of ≥0.90 or 90% and I-CVI of ≥0.78 or 78% (Marisa, 2021).

In these cases, the S-CVI/Universe method is not used due to the large size of the expert panel, potentially leading to results to an unacceptable level. Moreover, this approach does not take into account the possibility of coincidental agreement among experts (Roya & Behrooz, 2017) emphasizing the method's reliance on expert consensus without adjustment for the randomness of the answers.

In exploring the factors that influence the panel's consensus regarding the achievement of Minimum Essential Forces (MEFs) in a given domain (during the Delphi round), mean and standard deviation are calculated to measure factor convergence. The assessment of the importance of each goal by a panel of experts is facilitated through a 5-point Likert scale (Stancine et al., 2019).

To assess the validity of the content, this study used the item-level content validity index (I-CVI) and the scale-level average content validity index (S-CVI/Ave). S-CVI/Ave is determined by dividing the number of I-CVI scores by the number of items. An S-CVI/Ave of ≥0.8 is considered acceptable, while an S-CVI/Ave of ≥0.90 indicates excellent overall content validity. On the other hand, I-CVI is calculated from the number of experts who assess an item ≥3 divided by the total number of experts, with I-CVI ≥0.78 acceptable. The literature suggests that for a new assessment instrument to be considered valid, it must achieve a total CVI of ≥0.90 or 90% and I-CVI of ≥0.78 or 78% (Marisa, 2021).

In these cases, the S-CVI/Universe method is not used due to the large size of the expert panel, potentially leading to results to an unacceptable level. Moreover, this approach does not take into account the possibility of coincidental agreement among experts (Roya & Behrooz, 2017) emphasizing the method's reliance on expert consensus without adjustment for the randomness of the answers.

4. RESULT

The identification of factors influencing the development of a Naval base is carried out through a comprehensive literature review as well as insights from experts in the field of maritime defense. To obtain accurate and objective data, this study involved a panel of 15 professionals, academics, and stakeholders who have experience and expertise in the military and maritime defense fields. This study uses the Delphi method, which aims to evaluate and reach consensus among experts on the main criteria in the development of a Naval base from a military point of view.

As a first step, the list of factors relevant to the development of the Naval base is systematically compiled based on the results of literature studies and input from experts. This list is then entered into a questionnaire specifically designed to gauge the level of agreement among the expert panel. Each expert was asked to respond to the criteria that had been compiled by expressing their agreement or disagreement using verbal variables. Through this process, research can identify the factors considered most crucial in the development of the Naval base, so that it can be the basis for the formulation of more effective and sustainable strategies.

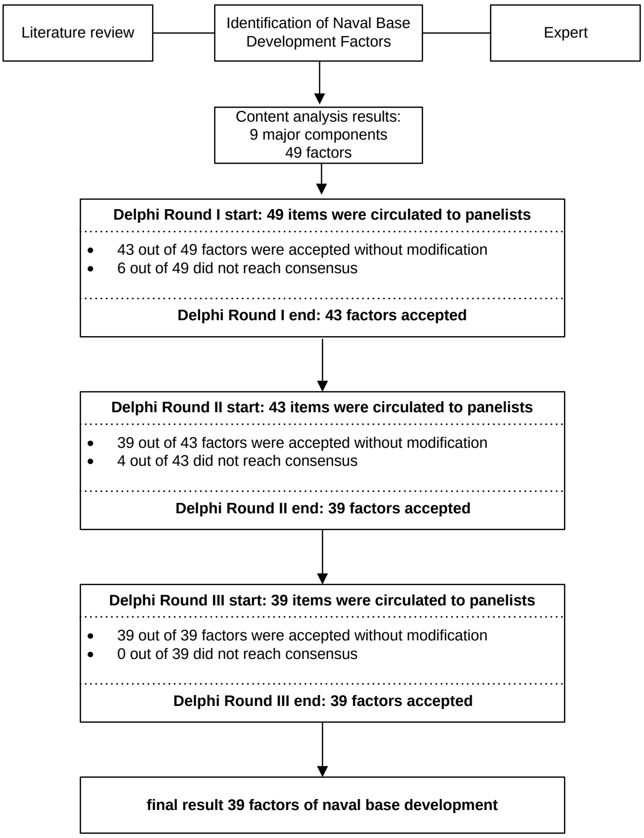

Literature review
Identification of Naval Base Development Factors
Expert
Content analysis results:
9 major components
49 factors
Delphi Round I start: 49 items were circulated to panelists
• 43 out of 49 factors were accepted without modification
• 6 out of 49 did not reach consensus
Delphi Round I end: 43 factors accepted
Delphi Round II start: 43 items were circulated to panelists
• 39 out of 43 factors were accepted without modification
• 4 out of 43 did not reach consensus
Delphi Round II end: 39 factors accepted
Delphi Round III start: 39 items were circulated to panelists
• 39 out of 39 factors were accepted without modification
• 0 out of 39 did not reach consensus
Delphi Round III end: 39 factors accepted
final result 39 factors of naval base development

Fig. 2. Proposed research framework).

Round 1: The initial round involved distributing a Google Form questionnaire to 15 expert panelists. This questionnaire outlines the research and its objectives and includes 9 variable aspects: 6 items on the infrastructure of the Naval Base, 5 items on personnel competence, 6 items on territorial control, 5 items on operating patterns, 6 items on coastal defense, 7 items on politics, 5 items on economics, 5 items on social, 4 items on technology. Using a Likert scale of 1-5 for the assessment, the assessment of completion time is between 10-15 minutes. The analysis shows that all aspects are very important in the preparation of the assessment tool, as evidenced by the average level of importance of each dimension being above 3 (mean). The item-CVI score ranges from 0.73 to 1, validating all items. The set achieved an S-CVI of 87% (≥0.8 acceptable) and an I-CVI of 82% (I-CVI ≥0.78 acceptable), without any suggestion for modification of themes or indicators (Lakmini et al., 2023). The first round resulted in the elimination of 1 operational pattern item, 2 coastal defense items, 1 political item, 1 economic item, 1 social item, thus shrinking from 49 items to 43 items.

Round 2: Two weeks later, the second round asked experts to assess the CVI of the remaining 43 items across 9 variable aspects. Item-CVI ranges from 0.73 to 1. Again validating all items on a Likert scale of 1-5 for the assessment, the completion time assessment estimates a time of about 10-15 minutes. This round achieves an S-CVI of 90% and an I-CVI of 82% which reaffirms the fundamental nature of all dimensions, as the average importance rating of each dimension remains above 3 (mean). This round resulted in the elimination of 4 items including 1 operation pattern item, 1 political item, 1 social item, 1 technology item so that it was reduced from 43 items to 39 items.

Round 3: After reformulation, the instrument undergoes a third round of evaluation to assess its final validity. The consensus was almost unanimous, with an I-CVI value of 83% for almost all items, which shows 100% agreement among experts. This results in an impressive S-CVI of 100%. Given the excellent S-CVI and I-CVI values, this round effectively completed the overall validity phase of the instrument, thus neveraging the need for further evaluation. All items fall into the valid or highly valid category, reaching consensus in the Delphi process.

Table 2. Expert judgment results in the first, second, and third rounds.

SN	Aspects	Item	Delphi Round I			Delphi Round II			Delphi Round III		
			A	I-CVI	Category	A	I-CVI	Category	A	I-CVI	Category
1	Infrastructure of the Indonesian Navy Base	Functions of 5R Base	14	0,93	Highly Valid	14	0,93	Highly Valid	14	0,93	Highly Valid
2		Base Defense Facilities	15	1,00	Highly Valid	15	1,00	Highly Valid	15	1,00	Highly Valid
3		*Early Wearning System* (EWS) Radar	15	1,00	Highly Valid	12	0,80	Valid	12	0,80	Valid
4		*Cyber Command*	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
5		Ground Based Air Defense (GBAD)	15	1,00	Highly Valid	12	0,80	Valid	12	0,80	Valid

SN	As-pects	Item	Delphi Round I			Delphi Round II			Delphi Round III		
			A	I-CVI	Cate-gory	A	I-CVI	Cate-gory	A	I-CVI	Cate-gory
6		Naval Post	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
7	Skill Level	Level of Expertise	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
8		Experience	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
9		Personnel Readiness	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
10		Organizational Structure	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
11		Training and Exercises	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
12	Territorial Control	Regional Geostrategic Awareness	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
13		Intelligence Capability	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
14		Hydrographic and Oceanographic Conditions	13	0,87	Highly Valid	14	0,93	Highly Valid	14	0,93	Highly Valid
15		Maritime Surveillance System	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
16		Rapid Response to Incidents	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
17		AI for ISR (Intelligence, Surveillance, and Reconnaissance)	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
18	Operating	Operational Interoperability	13	0,87	Highly Valid	14	0,93	Highly Valid	14	0,93	Highly Valid

SN	Aspects	Item	Delphi Round I			Delphi Round II			Delphi Round III		
			A	I-CVI	Category	A	I-CVI	Category	A	I-CVI	Category
19		Operational Tactics	14	0,93	Highly Valid	11	0,73	Less Valid			
20		Base Presence and Readiness	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
21		C4ISR Command and Control System	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
22		Strategic Planning of Operations	11	0,73	Less Valid						
23	Coastal Defense	Marine Battalion for Base Defense	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
24		Patrol Ships	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
25		Fixed & Mobile Missile System	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
26		Sonar	11	0,73	Less Valid						
27		Sonobuoy	11	0,73	Less Valid						
28		Anti-Submarine Warfare (ASW) Defense	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
29	Politics	National Defense and Security Policy	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
30		Sovereignty and Legal Status	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
31		**Regional Cooperation**	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
32		Domestic Political Stability	11	0,73	Less Valid						

SN	Aspects	Item	Delphi Round I			Delphi Round II			Delphi Round III		
			A	I-CVI	Category	A	I-CVI	Category	A	I-CVI	Category
33		**Territorial Violations by Neighboring Countries**	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
34		Dynamic Foreign Politics	12	0,80	Valid	11	0,73	Less Valid			
35		Geopolitical Tensions	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
36	Economics	Increased Investment Around the New Capital (IKN)	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
37		**Maritime Economic Potential**	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
38		Increased Defense Budget	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
39		Dependence on Resources	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
40		Global Trade Disruptions	11	0,73	Less Valid						
41	Social	Increased Public Awareness	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
42		Community Involvement in Regional Security	13	0,87	Highly Valid	13	0,87	Highly Valid	13	0,87	Highly Valid
43		Human Resource Development	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
44		Local social disturbances	11	0,73	Less Valid						
45		Illegal activities	12	0,80	Valid	11	0,73	Less Valid			

SN	Aspects	Item	Delphi Round I			Delphi Round II			Delphi Round III		
			A	I-CVI	Category	A	I-CVI	Category	A	I-CVI	Category
46	Technology	Digital Transformation	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
47		Implementation of Cyber Defense System	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
48		Cyber threats to modern technological systems	12	0,80	Valid	12	0,80	Valid	12	0,80	Valid
49		Dependence on foreign technology	12	0,80	Valid	11	0,73	Less Valid			

Table 3. Factors related to the development of naval bases

Code	Factors	Sources
C1	5R Base Functions	(De Yoshinov, 2022); (Suryawan, 2023); (Fajar et al., 2020)
C2	Base Defense Facilities	(Wallin, 2022); (Cabestan, 2021); (Hammes, 2021)
C3	*Early Wearning System* (EWS) Radar	(Cusson et al., 2021); (Rød et al., 2024); (Guzzetti et al., 2020)
C4	*Cyber Command*	(Lindsay, 2021); (Amro & Gkioulos, 2022); (Koo et al., 2020); (Slayton, 2021)
C5	Ground Based Air Defense (GBAD)	(Bronk et al., 2022); (A. Ahmad et al., 2024); (Bjerke & Valaker, 2022)
C6	Naval Post	(Russell, 2020); (Speller, 2023)
C7	Level of Expertise	(Klein & Hoffman, 2020); (Singhal et al., 2025); (Wolff et al., 2021)
C8	Experience	(Bion & Hinshelwood, 2023); (Andresen et al., 2020); (Lau et al., 2022)

Code	Factors	Sources
C9	Personnel Readiness	(Lubis et al., 2022); (Nwagwu, 2020); (Bloshchynskyi et al., 2021); (Frolova et al., 2020)
C10	Organizational Structure	(Verhoef et al., 2021); (Fuertes et al., 2020); (Paltridge, 2021)
C11	Training and Exercises	(Zatsiorsky et al., 2020); (Association, 2021); (Atakan et al., 2021); (Stensvold et al., 2020)
C12	Regional Geostrategic Awareness	(Lipkan et al., 2023); (MAISAIA, 2024); (Khan et al., 2023)
C13	Intelligence Capability	(Peppler, 2020); (Lina Mohammad Ahakhatreh, 2022)
C14	Hydrographic and Oceanographic Conditions	(Daudén-Bengoa et al., 2020); (de Freitas et al., 2023); (Pnyushkov et al., 2022)
C15	Maritime Surveillance System	(Liu et al., 2021); (Gamage et al., 2023); (AlMansoori et al., 2020)
C16	Rapid Response to Incidents	(Dias et al., 2020); (Reaser et al., 2020); (Reeves et al., 2020)
C17	AI for ISR (Intelligence, Surveillance, and Reconnaissance)	(Hintz, 2020); (Hong, 2020); (Cheng et al., 2022)
C18	Operational Interoperability	(Kasunic & Anderson, 2004); (Wegner, 1996); (Ford et al., 2007)
C19	Base Presence and Readiness	(Choucri et al., 2003); (Westgarth, 2023); (Schurger et al., 2021)
C20	C4ISR Command and Control System	(Y. Li et al., 2021); (Hordiichuk et al., 2024)
C21	Marine Battalion for Base Defense	(Berger, 2021); (Carter, 2022); (Fogle, 2022)
C22	Patrol Ships	(Suardi et al., 2022); (Rahmaji et al., 2022)
C23	Fixed & Mobile Missile System	(Cui et al., 2022); (Bronk et al., 2022)
C24	Anti-Submarine Warfare (ASW) Defense	(Peters, 2021); (Tirk & Salisbury, 2024)

Code	Factors	Sources
C25	National Defense and Security Policy	(S. Ahmad, 2022); (Bondarenko et al., 2022)
C26	Sovereignty and Legal Status	(Bondarenko et al., 2022); (Manurung et al., 2023)
C27	**Regional Cooperation**	(Zhang et al., 2024); (Armstrong & Drysdale, 2022)
C28	**Territorial Violations by Neighboring Countries**	(Ramírez, 2022); (Z. Li, 2022)
C29	Geopolitical Tensions	(Cheikh & Zaied, 2023); (Mignon & Saadaoui, 2024)
C30	Increased Investment Around the New Capital (IKN)	(Oduma et al., 2021); (Shang et al., 2024)
C31	**Maritime Economic Potential**	(Prasetyo et al., 2023); (Carvalho et al., 2021)
C32	Increased Defense Budget	(Robertson, 2022); (Becker, 2021)
C33	Dependence on Resources	(Nandi et al., 2021); (Maja & Ayano, 2021); (Wang & Azam, 2024)
C34	Increased Public Awareness	(Omoyajowo et al., 2022); (Okoye et al., 2021)
C35	Community Involvement in Regional Security	(Rijal, 2023); (Acharya, 2021)
C36	Human Resource Development	(Darman et al., 2023); (Hamouche, 2023); (Votto et al., 2021)
C37	Digital Transformation	(Kraus et al., 2021); (Fernandez-Vidal et al., 2022)
C38	Implementation of Cyber Defense System	(AL-Dosari et al., 2024); (Husák et al., 2021)
C39	Cyber Threats to Modern Technology Systems	(Aslan et al., 2023); (Y. Li & Liu, 2021)

5. DISCUSSION

Faced with the increasingly complex dynamics of geopolitical developments and Indonesia's strategic geographical condition as an archipelagic country, it is important for Indonesia to have a comprehensive marine security strategy. As stated in the introduction to this study, maritime security is a crucial aspect in maintaining state sovereignty and regional stability. One of the key steps in realizing an effective maritime security strategy is through the development of naval bases that can support maritime defense operations optimally.

In this context, the identification of naval bases is of great importance to ensure that its development is in accordance with national strategic needs. By identifying the main factors that affect the development of naval bases, it is hoped that the policies taken can be based on accurate data and holistic considerations. The results of the analysis show that there are 39 main sub-factors that contribute to the development of the Naval base, including **5R Base Functions**. The function of the base, which includes Rebase, Replenishment, Repair, Rest, and Recreation, is a vital element in supporting maritime operations in a sustainable manner. According to Song & Panayides (2012), bases with 5R functions are able to improve logistical and operational sustainability in modern maritime conflicts.

1) **Base Defense Facilities**. Improved defense facilities, such as radars, bunkers, and air defense systems, are essential to protect the base from external attack. Ashraf et al (2022) emphasized that the modernization of defense facilities can strengthen the security of strategic bases.
2) **Early Warning System (EWS) Radar**. The Early Warning System (EWS) Radar plays a crucial role in improving the ability to detect various maritime threats, such as foreign vessels, unidentified aircraft, and illegal activities in Indonesian waters (Neild et al., 2007). The implementation of EWS Radar at the TNI Navy base allows for threat identification from the beginning, so that preventive measures or responses can be carried out effectively.
3) **Cyber Command**. With the increasing risk of hacking, sabotage, and digital espionage, Cyber Command ensures the security of radar, monitoring, and command control (C4ISR) systems. In addition, according to Scherrer & Grund (2009), this unit is responsible for early detection of threats, the development of data encryption, as well as the training of personnel in cybersecurity
4) **Ground Based Air Defense (GBAD)**. Ground Based Air Defense (GBAD) protects against air threats such as attacks on enemy aircraft, drones, and missiles. Therefore, according to

Nikolakakos et al (2022), improving technology and coordination in the GBAD system is urgently needed to maintain the readiness and security of military bases.

5) **Naval Post.** The Naval Post (Posal) serves as a leading surveillance point that strengthens control of the maritime area. In the context of ALKI II, the existence of strategic Posal supports early detection of illegal activities, such as piracy, smuggling, or territorial violations. A study by Simanjuntak (2021) shows that small surveillance posts equipped with modern communication technology are able to increase the effectiveness of maritime security.
6) **Level of Expertise**. The quality of personnel with high skills greatly determines the operational success of the base. Expertise in navigation, electronic warfare, and the operation of advanced technologies (such as drones and radar) are required to deal with modern threats (Taufiqoerrochman, 2018).
7) **Experience**. Personnel with good experience in the field of maritime operations are better able to deal with complex situations, such as conflicts in the waters or asymmetric threats. Widisantoso (2024) shows that operational experience reduces the risk of failure in critical missions.
8) **Staff Readiness**. Operational readiness includes physical health, mental readiness, and personnel availability for operational tasks. According to BNPB (2016), high readiness increases the ability to respond to threats that arise suddenly.
9) **Organizational Structure**. A clear and integrated organizational structure makes it easier to make decisions and coordinate between units. Norman & Pahlawati (2024) show that organizations with adaptive structures are more resilient in dealing with unexpected situations.
10) **Training and Exercises**. Periodic exercises improve technical skills and inter-unit coordination. Suharyo (2017) emphasized the importance of scenario-based simulation as an effective training method in dealing with threats at sea.
11) **Regional Geostrategic Awareness**. An understanding of geostrategic conditions, including trade routes, ocean currents, and vulnerable points, is critical to designing an effective security strategy. Santoso (2023) stated that geostrategic analysis

improves maritime risk mitigation capabilities.

12) **Intelligence Capability**. Intelligence capabilities play a crucial role in early detection of threats. Ford & Rosenberg (2005) show that the integration of intelligence data increases the effectiveness of marine defense strategies.
13) **Hydrographic and Oceanographic Conditions**. Hydrographic and oceanographic conditions are highly influential in navigation, water safety, and warship operations. Factors such as water depth, ocean currents, tides, and seafloor structure determine the feasibility of the dock, vessel maneuverability, and the effectiveness of the underwater detection system (Fiedler & Talley, 2006).
14) **Maritime Surveillance System**. Technology-based surveillance systems, such as radars and drones, provide full visibility into operational areas. Stefanus & Adiyanto (2015) note that modern maritime surveillance systems are able to detect the movements of small vessels that are difficult to track with conventional radar.
15) **Rapid Response to Incidents**. The ability to respond quickly to incidents, such as ship accidents or pirate threats, is a top priority. Sarjito et al (2023) emphasize that fast response times prevent the escalation of threats in maritime areas.
16) **AI for ISR (Intelligence, Surveillance, and Reconnaissance)**. AI enables real-time monitoring through drones, sensors, and satellites, as well as processing intelligence data faster and more accurately (Buchter, 2018).
17) **Operational Interoperability**. Interoperability improves the efficiency of joint operation between units. Yani & Montratama (2015) mention interoperability as a key element in maritime security alliances.
18) **Base Presence and Readiness**. The physical presence of base elements, such as patrol boats, helicopters, and UAVs, increases the base's ability to maintain operational areas. Tanjung (2020) shows that the presence of these elements has a preventive effect on illegal activities.
19) **C4ISR Command and Control System**. The Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) system enables strategic coordination. Ye et al (2022) call C4ISR the backbone of modern maritime operations.
20) **Marine Battalion for Base Defense**. Marine battalions are the main force for defending

bases from direct threats. According to Kharish et al (2022), trained marine battalions improve integrated defenses in strategic bases.

21) **Patrol Ships**. Patrol boats play a strategic role in maritime surveillance. Supandi (2015) emphasized that fast patrol boats (FPVs) are effective in securing economic exclusive zones (EEZs).

22) **Fixed & Mobile Missile System**. Fixed and moving missile systems become the main defense of strategic bases. Sarjito (2023) mentioned that the flexibility of missile systems can prevent asymmetric threats.

23) **Anti-Submarine Warfare (ASW) Defense**. Anti-Submarine Defense (ASW) ensures security from underwater threats. Syahferzi (2022) shows that modern ASW technologies, such as sonar and underwater drones, are very effective at protecting bases.

24) **National Defense and Security Policy**. National Defense policies that emphasize the importance of maritime security are a great opportunity for the development of bases (Sarjito et al., 2023). Strategies such as the vision of the "World Maritime Axis" and the National Defense Strategic Plan support the development of military infrastructure in strategic areas.

25) **Sovereignty and Legal Status**. The affirmation of international law such as UNCLOS provides a legal basis for defending the FTAA and strengthening the base (Yustitianingtyas, 2015).

26) **Regional Cooperation**. Regional cooperation is an important element in maintaining maritime security stability, especially in strategic areas such as ALKI II which involves various countries with common interests. Through initiatives such as joint military exercises, intelligence information exchange, and strengthening maritime diplomacy, countries in the region can improve their collective capabilities in dealing with threats such as piracy, smuggling, and territorial conflicts (Al Syahrin, 2018).

27) **Territorial Violations by Neighboring Countries**. Territorial violations by neighboring countries are a serious threat that can trigger diplomatic tensions and disrupt regional stability (Zacher, 2001). These incidents are often linked to overlapping claims to strategic maritime zones or natural resources in disputed waters. This kind of violation not only has an impact on national security but also suppresses the state's ability

to defend its territorial sovereignty (Brown, 1996).

28) **Geopolitical Tensions**. Geopolitical tensions involving major countries and regional powers have the potential to extend to the ALKI II region, which is a strategic trade route and a region of high maritime security importance. These tensions can arise from territorial disputes, military power rivalries, or ideological differences between countries that have interests in the region. As conveyed by Purwantoro (2023), geopolitical tensions often trigger an arms race, the deployment of military forces in sensitive areas, and the risk of increasing open conflicts that can disrupt economic stability and maritime security in the region.

29) **Increased investment around the new capital (IKN).** Investment in the port and infrastructure sectors supports the Indonesian Navy base as a logistics and operational center (Limas et al., 2021). Local economic development also increases public support for military operations (Ginting et al., 2024).

30) **Maritime Economic Potential**. As an international trade route, ALKI II plays a strategic role in ensuring the smooth running of global trade (Kusuma et al., 2020).

31) **Increased Defense Budget**. Increasing the defense budget is a strategic step to support the development of military bases, especially in areas with strategic value such as ALKI II (Maesza et al., 2022). Larger budgets allow for the modernization of facilities, the procurement of advanced technologies, and the capacity building of personnel operating at the base (Geng & Doberstein, 2008).

32) **Dependence on Resources**. Reliance on resources such as high operational costs and the need to continuously update defense infrastructure and technology often create significant economic burdens if not managed efficiently Hillman et al (2009), highlight that budget constraints can hinder the modernization of military facilities, thereby reducing the ability of bases to deal with modern maritime threats

33) **Increased Public Awareness**. Increasing public awareness of the importance of maritime security encourages collaboration with the Indonesian Navy in protecting maritime areas (Sumarlin et al., 2023).

34) **Community Involvement in Regional Security**. Community involvement in maintaining

regional security, especially in strategic maritime areas such as ALKI II, plays an important role in supporting national defense efforts (Palar et al., 2022). Community participation can be done through community-based surveillance, suspicious activity reporting, and collaboration with security forces in identifying local threats, such as smuggling or piracy.

35) **Human Resource Development**. The development of human resources (HR) around military bases opens up significant opportunities to provide intensive training to local communities, which can ultimately support base operations while increasing community capacity. According to Tang & Zhang (2021), the development of local human resources has a positive impact on socio-economic stability, as people not only acquire new skills but also get better job opportunities.

36) **Digital Transformation**. Digitalization supports operational efficiency through geographic information systems (GIS) and technology-based surveillance. This makes patrol planning and logistics easier (Parung et al., 2021).

37) **Implementation of Cyber Defense System**. The implementation of a strong cyber defense system is an urgent need to protect critical infrastructure, especially in military bases and strategic areas such as ALKI II. According to Naseer (2020), the application of artificial intelligence-based security technology and advanced encryption can provide more proactive protection against cyber threats. In addition, intensive training for personnel to increase cyber awareness and establish rapid incident response procedures is an important step to ensure operational sustainability and security of critical infrastructure.

38) **Cyber Threats to Modern Technology Systems**. Cyberattacks targeting critical infrastructure, such as communications systems, automated weaponry, and surveillance devices, can significantly cripple base operations. Subagyo (2015) stated that cyberattacks not only have the potential to damage hardware and software, but can also access strategic data that can be used by foreign parties or terrorist groups.

Implications

This research provides strategic implications for the development of naval bases in maintaining

Indonesia's maritime security. The identification of the main factors that affect the effectiveness of the base shows the need for planning based on operational needs, infrastructure capacity building, and optimization of inter-agency coordination.

From a policy perspective, these findings underscore the importance of regulatory reforms that support the strengthening of bases as a key element of national maritime defense. Practically, the results of this study encourage increased investment in surveillance technology and logistics readiness to ensure the resilience and responsibility of bases against maritime threats.

The academic implications of this study lie in its contribution to the strategic literature of maritime defense, particularly in the context of the management of naval bases. Thus, this research not only provides an empirical basis for policymakers but also enriches the academic discourse in maritime security strategies. The implementation of the results of this research is expected to strengthen Indonesia's maritime defense posture in facing threat dynamics in strategic waters.

6. CONCLUSIONS

This research confirms that the development of naval bases has a strategic role in maintaining Indonesia's maritime security, especially in areas with high levels of vulnerability. Based on the analysis conducted, the main factors that affect the effectiveness of the base include infrastructure, human resources, technology, and policies and regulations that support the base's operations. The integration of these factors is essential in increasing combat readiness and deterrence against various maritime threats, both conventional and non-conventional.

The results of this study also show that the modernization of bases, through the improvement of supporting facilities and the adoption of digital-based technology, can improve operational efficiency and strengthen the ability to detect early threats in the first place.

In terms of policy, reforms are needed in the planning and management of bases to be more adaptive to threat dynamics and geopolitical changes in the region. Data-driven approaches and strategic studies are crucial in ensuring that the development of the base is in line with national defense needs. The implications of this study not only provide recommendations for policymakers, but also open up opportunities for further research on the optimization of base-based maritime defense strategies.

This study confirms that the transformation of naval bases is not just a necessity, but a necessity in facing future maritime security challenges. The implementation of these findings is expected to strengthen Indonesia's maritime defense posture and ensure sustainable national maritime stability and sovereignty.

Future Research

This research opens up opportunities for further studies related to the development of naval bases in the face of increasingly complex maritime security challenges. One of the future research directions is a more in-depth analysis of the optimization of the design and location of the base to improve operational efficiency and strategic carrying capacity. In addition, further research may focus on the integration of advanced technologies, such as artificial intelligence (AI) and satellite-based surveillance systems, to improve early detection capabilities and rapid response to maritime threats.

Further studies can also explore base defense scenarios under various geopolitical conditions, particularly in the context of the dynamics of the Indo-Pacific region. Simulation and modeling-based approaches can be used to evaluate the effectiveness of marine defense strategies in a variety of threat scenarios. In addition, research on cross-sectoral collaboration, both between domestic agencies and international cooperation, can provide further insights into how naval bases can play a key role in a broader maritime defense system.

ACKNOWLEDGEMENT

This research is supported by the TNI Navy Command and Staff School which has provided insight and expertise in assisting this research.

REFERENCES

[1] G. Zendelovski, “Great Power Strategic Competition in the Contemporary Security Environment,” Annu. Fac. Philos. Skopje, vol. 77, no. 1, pp. 329–359, 2024.

[2] J. S. Nye and R. O. Keohane, Power and interdependence. HarperCollins, 1990.

[3] M. Budiana and B. Budiman, “Sovereignty Dynamics in the US-China Geopolitical Conflict in the South China Sea,” J. Sos. Sains dan Komun, vol. 3, no. 01, pp. 29–37, 2024.

[4] R. Cribb and M. Ford, “Indonesia as an archipelago: Managing islands, managing the seas,” ISEAS-Yusof Ishak Institute, 2009.

[5] S. Attamimi, “Global South Corridor sebagai Instrumen Diplomasi Indonesia dalam Implementasi Kerja Sama Konektivitas Maritim,” J. Hub. Luar Negeri, vol. 9, no. 2, pp. 182–209, 2024.

[6] M. C. Horowitz, G. C. Allen, E. B. Kania, and P. Scharre, Strategic competition in an era of artificial intelligence. Center for a New American Security, 2022.

[7] R. S. Arto, L. Y. Prakoso, and D. Sianturi, “Strategi Pertahanan Laut Indonesia dalam Perspektif Maritim Menghadapi Globalisasi,” J. Strateg. Pertahanan Laut, 2019.

[8] E. Buyukakinci, “Adapting Military Doctrines to Shifting Power Dynamics in the International System: Looking beyond Unipolarity through the Analyses of Charles Kupchan,” Güvenlik Strat. Derg, no. Special Is, pp. 65–89, 2024.

[9] P. Amelia, A. Lathifah, and I. N. A. Yasa, “Analysis of the impact of maritime sector development in supporting Indonesian Navy Ship operations,” Procedia Comput. Sci., vol. 197, pp. 317–325, 2022.

[10] B. P. Sartono, L. Y. Prakoso, and D. Sianturi, “THE INDONESIAN GOVERNMENT AUTHORITY IN SECURING INDONESIAN ARCHIPELAGO SEA LANES (ASLs/ALKI)”.

[11] J. MacHaffie, “The geopolitical roots of China’s naval modernisation,” Aust. J. Marit. Ocean Aff, vol. 12, no. 1, pp. 1–15, 2020.

[12] E. Grove, The future of sea power. Taylor & Francis, 2021.

[13] Marsetio, “Sea Power” Indonesia 2019-2024. 2019.

[14] C. Bueger, “What is maritime security?” Mar. policy, vol. 53, pp. 159–164, 2015.

[15] I. Chapsos, “Is maritime security a traditional security challenge?” Explor. Secur. Landsc. Non-Traditional Secur. Challenges, pp. 59–78, 2016.

[16] J. Piedade, “From politicization to securitization of maritime security in the Gulf of Guinea,” Croat. Int. Relations Rev., vol. 22, no. 75, pp. 69–85, 2016.

[17] C. Bueger, “Communities of security practice at work? The emerging African maritime security regime,” African Secur., vol. 6, no. 3–4, pp. 297–316, 2013.

[18] A. Wibawa, M. R. Iswardhana, and H. C. Chotimah, “Interaksi Antar-lembaga dan Reformasi Tata Kelola Keamanan Maritim Indonesia: Bakamla RI,” 2021.

[19] M. Zulham and H. M. Saragih, “Strategi Indonesia dalam Mewujudkan Poros Maritim Dunia di Tengah Kebijakan Jalur Sutra Maritim China,” Popul. J. Sos. dan Hum., vol. 4, no. 1, pp. 49–61, 2019.

[20] A. T. Mahan, “Alfred-Mahan-Influence-of-Sea-Power-on-History-1890,” 1890.

[21] J. E. Bell and S. E. Griffis, “Military applications of location analysis,” Appl. Locat. Anal., pp. 403–433, 2015.

[22] L. Wong, CU@ the FOB: How the forward operating base is changing the life of combat soldiers. Strategic Studies Institute, US Army War College, 2006.

[23] S. S. Okol, “23. Jurnal Aplikasi Fuzzy Multi Criteria Decision Making (Fmcdm) Dalam Pemodelan Penentuan Lokasi Pengembangan Pangkalan Angkatan Laut,” Apl. Fuzzy Multi Criteria Decis. Mak. Dalam Pemodelan Penentuan Lokasi Pengemb. Pangkalan Angkatan Laut, vol. 3, no. 1, pp. 465–480, 2015.

[24] A. Widyaksa, U. Subakti, O. S. Suharyo, J. Purnomo, and A. K. Susilo, “Impact Assessment Of Minimum Essential Force (MEF) Achievement Of Indonesian Navy Using Integrated

Delphi-Ahp-Topsis," J. Marit. Res., 2024.

[25] C. Okoli and S. D. Pawlowski, "The Delphi method as a research tool: An example, design considerations and applications," Inf. Manag., vol. 42, no. 1, pp. 15–29, 2004, doi: 10.1016/j.im.2003.11.002.

[26] T. Flanagan, R. Ashmore, D. Banks, and D. MacInnes, "The Delphi method: Methodological issues arising from a study examining factors influencing the publication or non-publication of mental health nursing research," Ment. Heal. Rev. J., vol. 21, no. 2, pp. 85–94, 2016.

[27] E. C. Halim, A. Andi, and J. Rahardjo, "Aplikasi Interpretive Structural Modeling (ISM) pada Faktor-faktor Penyebab Keterlambatan Proyek Konstruksi di Surabaya," Dimens. Utama Tek. Sipil, vol. 8, no. 1, pp. 60–77, 2021.

[28] J. Lee, S. H. Lee, and G. T. Chang, "Expert consensus on the development of a health-related questionnaire for the pediatric field of Korean medicine: a Delphi study," BMC Complement. Med. Ther., vol. 20, pp. 1–13, 2020.

[29] M. Gunduz and H. A. Elsherbeny, "Operational framework for managing construction-contract administration practitioners' perspective through modified Delphi method," J. Constr. Eng. Manag., vol. 146, no. 3, p. 4019110, 2020.

[30] I. Karakikes and E. Nathanail, "Using the delphi method to evaluate the appropriateness of urban freight transport solutions," Smart Cities, vol. 3, no. 4, pp. 1428–1447, 2020, doi: 10.3390/smartcities3040068.

[31] E. Almanasreh, R. Moles, and T. F. Chen, "Research in Social and Administrative Pharmacy Evaluation of methods used for estimating content validity," Res. Soc. Adm. Pharm., no. xxxx, pp. 0–1, 2018, doi: 10.1016/j.sapharm.2018.03.066.

[32] K. Stancine et al., "Development and content validation of an instrument to support pharmaceutical counselling for dispensing of prescribed medicines," no. September 2018, pp. 1–8, 2019, doi: 10.1111/jep.13102.

[33] R. da Silva; R. de C. Marisa, "Contributions of the Delphi technique to the validation of an occupational therapy assessment in the visual impairment field 1," Brazillian J. Occup. Ther., pp. 1–15, 2021.

[34] F. Roya and F. Behrooz, "Item Selection and Content Validity of the Risk Factors of Post-Intubation Tracheal Stenosis Observation Questionnaire for ICU-Admitted Patients Study design," vol. 16, no. 1, pp. 22–33, 2017.

[35] S. M. De Yoshinov, "Marine Defense Strategy with Military Base Development on the Outside Island as a Leading Defense and Defense Mobility," J. Strateg. Pertahanan Laut, vol. 8, no. 1, pp. 74–80, 2022.

[36] A. Suryawan, "Optimization of Logistics Support on Natuna Island as a Base Carrier in Uploading the Sovereignty of the Republic of Indonesia," Int. J. Soc. Manag. Stud., vol. 4, no. 4, pp. 18–25, 2023.

[37] R. Fajar, A. Rahman, and A. Nugroho, "The Development Strategy of Fasharkan Lantamal Ix Xyz from class C Fasharkan type to Fasharkan class A Koarmada Iii with Swot and Ism

Approach," In Sttal Postgraduate-International Conference, 2020.

[38] M. Wallin, US military bases and facilities in the Middle East. JSTOR, 2022.

[39] J.-P. Cabestan, "China's military base in Djibouti: A microcosm of China's growing competition with the United States and new bipolarity," in China's Big Power Ambition under Xi Jinping, Routledge, 2021, pp. 169–185.

[40] T. X. Hammes, "The tactical defense becomes dominant again," Jt. Force Q., vol. 103, pp. 10–17, 2021.

[41] D. Cusson, C. Rossi, and I. F. Ozkan, "Early warning system for the detection of unexpected bridge displacements from radar satellite data," J. Civ. Struct. Heal. Monit., vol. 11, no. 1, pp. 189–204, 2021.

[42] E. G. Rød, T. Gåsste, and H. Hegre, "A review and comparison of conflict early warning systems," Int. J. Forecast., vol. 40, no. 1, pp. 96–112, 2024.

[43] F. Guzzetti et al., "Geographical landslide early warning systems," Earth-Science Rev., vol. 200, p. 102973, 2020.

[44] J. R. Lindsay, "Cyber conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem," Intell. Natl. Secur., vol. 36, no. 2, pp. 260–278, 2021.

[45] A. Amro and V. Gkioulos, "From click to sink: Utilizing ais for command and control in maritime cyber-attacks," in European Symposium on Research in Computer Security, Springer, 2022, pp. 535–553.

[46] J. Koo, S.-R. Oh, S. H. Lee, and Y.-G. Kim, "Security architecture for cloud-based command and control system in IoT environment," Appl. Sci., vol. 10, no. 3, p. 1035, 2020.

[47] R. Slayton, "What Is a Cyber Warrior? The Emergence of US Military Cyber Expertise, 1967–2018 (Winter 2021)," 2021.

[48] J. Bronk, N. Reynolds, and J. Watling, "The Russian air war and Ukrainian requirements for air defence," 2022.

[49] A. Ahmad, R. Amjad, A. Basharat, A. A. Farhan, and A. E. Abbas, "Fuzzy knowledge based intelligent decision support system for ground based air defence," J. Ambient Intell. Humaniz. Comput., vol. 15, no. 4, pp. 2317–2340, 2024.

[50] H. M. Bjerke and S. Valaker, "Command and control in a fifth generation air force: Coordination requirements of air operations with F-35 and the command and control-system of the norwegian armed forces," Scand. J. Mil. Stud., vol. 5, no. 1, 2022.

[51] J. Russell, Innovation, Transformation, and War: Counterinsurgency Operations in Anbar and Ninewa Provinces, Iraq, 2005-2007. Stanford University Press, 2020.

[52] I. Speller, Understanding naval warfare. Routledge, 2023.

[53] G. A. Klein and R. R. Hoffman, "Seeing the invisible: Perceptual-cognitive aspects of expertise," in Cognitive science foundations of instruction, Routledge, 2020, pp. 203–226.

[54] K. Singhal et al., "Toward expert-level medical question answering with large language models," Nat. Med., pp. 1–8, 2025.

[55] C. E. Wolff, H. Jarodzka, and H. P. A. Boshuizen, "Classroom

management scripts: A theoretical model contrasting expert and novice teachers' knowledge and awareness of classroom events," Educ. Psychol. Rev., vol. 33, no. 1, pp. 131–148, 2021.

[56] W. Bion and R. Hinshelwood, Learning from experience. Routledge, 2023.

[57] L. Andresen, D. Boud, and R. Cohen, "Experience-based learning," in Understanding adult education and training, Routledge, 2020, pp. 225–239.

[58] H. Lau, M. Michel, J. E. LeDoux, and S. M. Fleming, "The mnemonic basis of subjective experience," Nat. Rev. Psychol., vol. 1, no. 8, pp. 479–488, 2022.

[59] A. S. Lubis, P. Lumbanraja, Y. Absah, and A. S. Silalahi, "Human resource competency 4.0 and its impact on Bank Indonesia employees' readiness for transformational change," J. Organ. Chang. Manag., vol. 35, no. 4/5, pp. 749–779, 2022.

[60] W. E. Nwagwu, "E-learning readiness of universities in Nigeria-what are the opinions of the academic staff of Nigeria's premier university?," Educ. Inf. Technol., vol. 25, no. 2, pp. 1343–1370, 2020.

[61] I. Bloshchynskyi et al., "Formation of psychophysical readiness of cadets for future professional activity," Open Sports Sci. J., no. 14, pp. 1–8, 2021.

[62] O. Y. Frolova, L. V Fomina, and Z. N. Shmeleva, "The personnel competence qualification formation in the agro-industrial complex production systems: managerial aspect," in IOP Conference Series: Earth and Environmental Science, IOP Publishing, 2020, p. 22029.

[63] P. C. Verhoef et al., "Digital transformation: A multidisciplinary reflection and research agenda," J. Bus. Res., vol. 122, pp. 889–901, 2021.

[64] G. Fuertes, M. Alfaro, M. Vargas, S. Gutierrez, R. Ternero, and J. Sabattin, "Conceptual framework for the strategic management: a literature review—descriptive," J. Eng., vol. 2020, no. 1, p. 6253013, 2020.

[65] B. Paltridge, Discourse analysis. Springer, 2021.

[66] V. M. Zatsiorsky, W. J. Kraemer, and A. C. Fry, Science and practice of strength training. Human kinetics, 2020.

[67] N.-N. S. & C. Association, Essentials of strength training and conditioning. Human kinetics, 2021.

[68] M. M. Atakan, Y. Li, Ş. N. Koşar, H. H. Turnagöl, and X. Yan, "Evidence-based effects of high-intensity interval training on exercise capacity and health: A review with historical perspective," Int. J. Environ. Res. Public Health, vol. 18, no. 13, p. 7201, 2021.

[69] D. Stensvold et al., "Effect of exercise training for five years on all-cause mortality in older adults-the Generation 100 study: randomised controlled trial," bmj, vol. 371, 2020.

[70] V. Lipkan, O. Kuznichenko, and A. Ivanov, "Geoeconomics as a tool of modern geostrategy," Balt. J. Econ. Stud., vol. 9, no. 1, pp. 113–123, 2023.

[71] V. Maisaia, "The Fifth War Generation and its Geostrategic Implications on The Black Sea Security Dimension: New Trends, New Tendencies," in Proceedings Of The International Scientific Conference Strategies XXI-National Defence

College, Carol I National Defence University Publishing House, 2024, pp. 85–94.

[72] S. Khan, Z. Ahmad, and M. Ullah, “China’s geostrategic interest in the Indian Ocean Region,” Qlantic J. Soc. Sci. Humanit., vol. 4, no. 4, pp. 141–161, 2023.

[73] B. Peppler, “Towards a conceptual framework for intelligence capability,” J. Aust. Inst. Prof. Intell. Off., vol. 28, no. 2–3, pp. 37–50, 2020.

[74] S. I. S. A.-H. Lina Mohammad Ahakhatreh, “Impact of business intelligence capabilities on the competitive performance of Islamic banks in Jordan,” J. Hunan Univ. Nat. Sci., vol. 49, no. 10, 2022.

[75] G. Daudén-Bengoa, S. P. A. Jiménez-Rosenberg, J. C. Compaire, L. del Pilar Echeverri-García, P. Pérez-Brunius, and S. Z. Herzka, “Larval fish assemblages of myctophids in the deep water region of the southern Gulf of Mexico linked to oceanographic conditions,” Deep Sea Res. Part I Oceanogr. Res. Pap., vol. 155, p. 103181, 2020.

[76] A. A. de Freitas et al., “Atmospheric and oceanic patterns associated with extreme drought events over the Paraná hydrographic region, Brazil,” Climate, vol. 11, no. 1, p. 12, 2023.

[77] A. V Pnyushkov, G. V Alekseev, and A. V Smirnov, “On the Interplay between freshwater content and hydrographic conditions in the Arctic Ocean in the 1990s–2010s,” J. Mar. Sci. Eng., vol. 10, no. 3, p. 401, 2022.

[78] R. W. Liu, W. Yuan, X. Chen, and Y. Lu, “An enhanced CNN-enabled learning method for promoting ship detection in maritime surveillance system,” Ocean Eng., vol. 235, p. 109435, 2021.

[79] C. Gamage, R. Dinalankara, J. Samarabandu, and A. Subasinghe, “A comprehensive survey on the applications of machine learning techniques on maritime surveillance to detect abnormal maritime vessel behaviors,” WMU J. Marit. Aff., vol. 22, no. 4, pp. 447–477, 2023.

[80] A. A. AlMansoori, I. Swamidoss, S. Sayadi, and A. Almarzooqi, “Analysis of different tracking algorithms applied on thermal infrared imagery for maritime surveillance systems,” in Artificial Intelligence and Machine Learning in Defense Applications II, SPIE, 2020, pp. 30–40.

[81] A. de O. Dias, A. Bernardes, L. D. P. Chaves, H. M. Sonobe, C. M. C. Grion, and M. do C. F. L. Haddad, “Critical incidents as perceived by rapid response teams in emergency services,” Rev. da Esc. Enferm. da USP, vol. 54, p. e03595, 2020.

[82] J. K. Reaser, S. W. Burgiel, J. Kirkey, K. A. Brantley, S. D. Veatch, and J. Burgos-Rodríguez, “The early detection of and rapid response (EDRR) to invasive species: a conceptual framework and federal capacities assessment,” Biol. Invasions, vol. 22, pp. 1–19, 2020.

[83] J. J. Reeves et al., “Rapid response to COVID-19: health informatics support for outbreak management in an academic health system,” J. Am. Med. Informatics Assoc., vol. 27, no. 6, pp. 853–859, 2020.

[84] K. J. Hintz, Sensor management in ISR. Artech House, 2020.

[85] C. S. Hong, “Automation and Artificial Intelligence for Naval ISR: Us Navy vs. China’s Navy,” 2020, Monterey, CA; Naval Postgraduate School.

[86] H. Cheng, E. Conway, T. Heggedahl, J. Morgan, and B. Schlessman, “Explore AI and machine learning for future ISR collection planning and management,” in Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications IV, SPIE, 2022, pp. 352–360.

[87] M. Kasunic and W. Anderson, “Measuring systems interoperability: Challenges and opportunities,” Softw. Eng. Meas. Anal. Initiat., 2004.

[88] P. Wegner, “Interoperability,” ACM Comput. Surv., vol. 28, no. 1, pp. 285–287, 1996.

[89] T. Ford, J. Colombi, S. Graham, and D. Jacques, “The interoperability score,” in Proceedings of the Fifth Annual Conference on Systems Engineering Research, 2007, pp. 1–10.

[90] N. Choucri et al., “Global e-readiness-for what,” Cent. Ebus. MIT, 2003.

[91] D. Westgarth, “The perception of readiness,” BDJ Pract., vol. 36, no. 10, pp. 14–18, 2023.

[92] A. Schurger, J. Pak, and A. L. Roskies, “What is the readiness potential?,” Trends Cogn. Sci., vol. 25, no. 7, pp. 558–570, 2021.

[93] Y. Li, H.-Z. Huang, and T. Zhang, “Reliability analysis of C4ISR systems based on goal-oriented methodology,” Appl. Sci., vol. 11, no. 14, p. 6335, 2021.

[94] V. Hordiichuk, P. Snitsarenko, N. Andriianova, B. Molodetskyi, and Y. Kapran, “Advanced information technologies (C4ISR) in the peacekeeping field service,” Adv. Inf. Syst., vol. 8, no. 4, pp. 93–102, 2024.

[95] G. D. H. Berger, “Marine Corps Support to Joint Operations in Contested Littorals,” Mil. Rev., vol. 1, 2021.

[96] C. J. Carter, “21st-Century Marine Corps’ Commandos,” Mar. Corps Gaz., 2022.

[97] J. Fogle, “Advanced Base Defense Doctrine, War Plan Orange, and Preparation at Midway: Were the Marines Ready?,” Open Mil. Stud., vol. 2, no. 1, pp. 66–83, 2022.

[98] A. I. W. Suardi, T. H. M. U. Pawara, and T. H. Alamsyah, “Patrol ship design to guard the natuna seas,” Int. J. Mar. Eng. Innov. Res, vol. 7, no. 3, pp. 171–179, 2022.

[99] T. Rahmaji, A. R. Prabowo, T. Tuswan, T. Muttaqie, N. Muhayat, and S.-J. Baek, “Design of fast patrol boat for improving resistance, stability, and seakeeping performance,” Designs, vol. 6, no. 6, p. 105, 2022.

[100] L. Cui, N. Jin, S. Chang, Z. Zuo, and Z. Zhao, “Fixed-time ESO based fixed-time integral terminal sliding mode controller design for a missile,” ISA Trans., vol. 125, pp. 237–251, 2022.

[101] J. Peters, “Below the surface: undersea warfare challenges in the 21st century,” in From the North Atlantic to the South China Sea, Nomos Verlagsgesellschaft mbH & Co. KG, 2021, pp. 93–110.

[102] E. Tirk and D. Salisbury, “China Maritime Report No. 38: PLAN Anti-Submarine Warfare Aircraft-Sensors,

Weapons, and Operational Concepts," 2024.

[103] S. Ahmad, "Cyber Security Threat and Pakistan's Preparedness: An Analysis of National Cyber Security Policy 2021," Pakistan J. Humanit. Soc. Sci. Res., vol. 5, no. 1, p. 33, 2022.

[104] S. Bondarenko, A. Bratko, V. Antonov, R. Kolisnichenko, O. Hubanov, and A. Mysyk, "Improving the state system of strategic planning of national security in the context of informatization of society," J. Inf. Technol. Manag., vol. 14, no. Special Issue: Digitalization of Socio-Economic Processes, pp. 1–24, 2022.

[105] Y. S. Manurung, S. Maarif, T. S. L. Toruan, and Y. Swastanto, "Indonesian National Defense Strategy in the Asean Region of the 21st Century Based on Defense System and Security Population Demography," JMKSP (Jurnal Manajemen, Kepemimpinan, Dan Supervisi Pendidikan), vol. 8, no. 2, pp. 936–945, 2023.

[106] X. Zhang, Y. Lu, Y. Xu, C. Zhou, and Y. Zou, "Governing regional inequality through regional cooperation? A case study of the Guangdong-Hong Kong-Macau Greater Bay area," Appl. Geogr., vol. 162, p. 103135, 2024.

[107] S. P. Armstrong and P. Drysdale, "The economic cooperation potential of East Asia's RCEP agreement," East Asian Econ. Rev., vol. 26, no. 1, pp. 3–25, 2022.

[108] W. A. Ramírez, "Resistance to territorial and maritime delimitation judgments of the International Court of Justice and clashes with 'territory clauses' in the Constitutions of Latin American states," Leiden J. Int. Law, vol. 35, no. 1, pp. 185–208, 2022.

[109] Z. Li, "The ideograph of Territorial Sovereignty: Framing of China's Belt and Road Initiative by the Times of India," Int. Commun. Gaz., vol. 84, no. 6, pp. 570–588, 2022.

[110] N. Ben Cheikh and Y. Ben Zaied, "Investigating the dynamics of crude oil and clean energy markets in times of geopolitical tensions," Energy Econ., vol. 124, p. 106861, 2023.

[111] V. Mignon and J. Saadaoui, "How do political tensions and geopolitical risks impact oil prices?," Energy Econ., vol. 129, p. 107219, 2024.

[112] C. O. Oduma et al., "Increased investment in gametocytes in asymptomatic Plasmodium falciparum infections in the wet season," BMC Infect. Dis., vol. 21, pp. 1–10, 2021.

[113] Y. Shang, Q. Yang, and Y. Pu, "Role of foreign direct Investment and political openness in boosting the eco-tourism sector for achieving sustainability," Humanit. Soc. Sci. Commun., vol. 11, no. 1, pp. 1–8, 2024.

[114] K. A. Prasetyo, A. Ansori, and B. Suseto, "Maritime defense strategy education as an effort of the Indonesian government in maintaining maritime security," Int. J. Asian Educ., vol. 4, no. 1, pp. 58–67, 2023.

[115] F. Carvalho, J. Portugal-Pereira, M. Junginger, and A. Szklo, "Biofuels for maritime transportation: A spatial, techno-economic, and logistic analysis in Brazil, Europe, South Africa, and the USA," Energies, vol. 14, no. 16, p. 4980, 2021.

[116] P. E. Robertson, "The real military balance: International comparisons of defense spending," Rev. Income Wealth, vol. 68, no. 3, pp. 797–818, 2022.

[117] J. Becker, “Rusty guns and buttery soldiers: Unemployment and the domestic origins of defense spending,” Eur. Polit. Sci. Rev., vol. 13, no. 3, pp. 307–330, 2021.

[118] S. Nandi, J. Sarkis, A. Hervani, and M. Helms, “Do blockchain and circular economy practices improve post COVID-19 supply chains? A resource-based and resource dependence perspective,” Ind. Manag. Data Syst., vol. 121, no. 2, pp. 333–363, 2021.

[119] M. M. Maja and S. F. Ayano, “The impact of population growth on natural resources and farmers’ capacity to adapt to climate change in low-income countries,” Earth Syst. Environ., vol. 5, no. 2, pp. 271–283, 2021.

[120] J. Wang and W. Azam, “Natural resource scarcity, fossil fuel energy consumption, and total greenhouse gas emissions in top emitting countries,” Geosci. Front., vol. 15, no. 2, p. 101757, 2024.

[121] K. Omoyajowo, M. Raimi, T. Waleola, O. Odipe, and A. Ogunyebi, “Public awareness, knowledge, attitude and perception on microplastics pollution around lagos lagoon,” Ecol. Saf. Balanc. use Resour., vol. 2, no. 24, pp. 35–46, 2022.

[122] H. Okoye et al., “Low awareness of venous thromboembolism among the general population: a call for increased public enlightenment programs,” J. Prev. Med. Hyg., vol. 62, no. 3, p. E704, 2021.

[123] S. Rijal, “The importance of community involvement in public management planning and decision-making processes,” J. Contemp. Adm. Manag., vol. 1, no. 2, pp. 84–92, 2023.

[124] A. Acharya, ASEAN and regional order: Revisiting security community in Southeast Asia. Routledge, 2021.

[125] J. L. Darman, I. Harsono, and A. S. B. Putra, “Bibliometric Analysis of Human Resource Development: Trends, Research Focuses, and Recent Developments,” West Sci J Econ Entrep, vol. 1, pp. 525–534, 2023.

[126] S. Hamouche, “Human resource management and the COVID-19 crisis: Implications, challenges, opportunities, and future organizational directions,” J. Manag. Organ, vol. 29, no. 5, pp. 799–814, 2023.

[127] A. M. Votto, R. Valecha, P. Najafirad, and H. R. Rao, “Artificial intelligence in tactical human resource management: A systematic literature review,” Int. J. Inf. Manag. Data Insights, vol. 1, no. 2, p. 100047, 2021.

[128] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas, and N. Roig-Tierno, “Digital transformation: An overview of the current state of the art of research,” Sage Open, vol. 11, no. 3, p. 21582440211047576, 2021.

[129] J. Fernandez-Vidal, F. A. Perotti, R. Gonzalez, and J. Gasco, “Managing digital transformation: The view from the top,” J. Bus. Res., vol. 152, pp. 29–41, 2022.

[130] K. AL-Dosari, N. Fetais, and M. Kucukvar, “Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges,” Cybern. Syst., vol. 55, no. 2, pp. 302–330, 2024.

[131] M. Husák, V. Bartoš, P. Sokol, and A. Gajdoš, “Predictive methods in cyber defense: Current experience and research challenges,” Futur. Gener. Comput. Syst., vol. 115, pp. 517–530, 2021.

[132] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions,” Electronics, vol. 12, no. 6, p. 1333, 2023.

[133] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” Energy Reports, vol. 7, pp. 8176–8186, 2021.

[134] D.-W. Song and P. Panayides, Maritime logistics: a complete guide to effective shipping and port management. Kogan Page Publishers, 2012.

[135] I. Ashraf et al., “A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry,” IEEE Trans. Intell. Transp. Syst., vol. 24, no. 2, pp. 2677–2690, 2022, doi: 10.1109/TITS.2022.3164678.

[136] R. C. Neild, R. Balfanz, and L. Herzog, “An early warning system,” Educ. Leadersh., vol. 65, no. 2, pp. 28–33, 2007.

[137] J. H. Scherrer and W. C. Grund, “A cyberspace command and control model,” Maxwell Pap., no. 47, pp. 27–58, 2009.

[138] G. Nikolakakos, M. Amyot-Bourgeois, and B. Astles, “A state-of-the-art review and analysis of tactical-level ground-based air defence systems and airborne threats,” 2022.

[139] M. Simanjuntak, “Pembentukan Bintara Pembina Potensi Maritim (Babinpotmar) di Pos Angkatan Laut (Posal),” J. Marit. Indones. (Indonesian Marit. Journal), vol. 9, no. 2, pp. 147–158, 2021.

[140] A. Taufiqoerrochman, Konsep Operasi Maritim Indonesia. Pandiva Buku, 2018.

[141] H. Widisantoso, “Studi Komparatif Antara Pemeliharaan Terjadwal dan Pemeliharaan Prediktif pada Kapal Perang,” J. Knowl. Collab., vol. 1, no. 4, pp. 146–152, 2024.

[142] BNPB, “Definisi Bencana,” 2016.

[143] E. Norman and E. Pahlawati, “Pengembangan Kepemimpinan yang Adaptif dan Fleksibel: Meningkatkan Ketahanan Organisasi di Era Transformasi Digital,” MES Manag. J., vol. 3, no. 1, pp. 298–305, 2024.

[144] O. S. Suharyo, I. R. Rosyid, M. Daniel, C. O. Promotor, D. R. Armono, and D. Haryo, “Model Penentuan Lokasi Pangkalan Angkatan Laut Berbasis Sustainabilitas,” Surabaya Inst. Teknol. Sepuluh Nop., 2017.

[145] G. Santoso, A. A. Karim, and B. Maftuh, “Kajian Ketahanan Nasional melalui Geopolitik dan Geostrategi Indonesia Abad 21,” J. Pendidik. Transform., vol. 2, no. 1, pp. 184–196, 2023.

[146] C. A. Ford and D. A. Rosenberg, “The Naval Intelligence Underpinnings of Reagan’s Maritime Strategy,” J. Strateg. Stud., vol. 28, no. 2, pp. 379–409, 2005.

[147] P. C. Fiedler and L. D. Talley, “Hydrography of the eastern tropical Pacific: A review,” Prog. Oceanogr., vol. 69, no. 2–4, pp. 143–180, 2006.

[148] D. Stefanus and E. Adiyanto, Komando Pengendalian Keamanan dan Keselamatan Laut. Gramedia Pustaka Utama, 2015.

[149] I. A. Sarjito, E. P. Duarte, and S. Sos, Geopolitik dan Geostrategi Pertahanan: Tantangan Keamanan Global. Indonesia Emas Group, 2023.

[150] R. M. Buchter, “2020: faster than real-time tactical intelligence, surveillance, and reconnaissance (ISR) from the dismount, and faster than real-time strategic ISR to the dismount,” in Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR IX, SPIE, 2018, pp. 100–118.

[151] Y. M. Yani and I. Montratama, “Indonesia sebagai poros maritim dunia: suatu tinjauan geopolitik,” J. Pertahanan dan Bela Negara, vol. 5, no. 2, pp. 25–52, 2015.

[152] A. P. Tanjung, “Pengaruh Kemampuan Operasi Keamanan Laut Pangkalan TNI Angkatan Laut Terhadap Penegakan Hukum di Laut,” J. Marit. Indones. (Indonesian Marit. Journal), vol. 8, no. 1, 2020.

[153] F. Ye, Y. Mao, Y. Li, and X. Liu, “Target threat estimation based on discrete dynamic Bayesian networks with small samples,” J. Syst. Eng. Electron., vol. 33, no. 5, pp. 1135–1142, 2022.

[154] L. Kharish, I. Syahtaria, D. Sianturi, L. Y. Prakoso, H. J. R. Saragih, and E. Bangun, “Strategi Gelar Kekuatan TNI Angkatan Laut dalam Mengatasi Pelanggaran di Wilayah Alur Laut Kepulauan Indonesia II Guna Mewujudkan Stabilitas Keamanan Perairan dalam Rangka Mendukung Operasi Militer Selain Perang (Omsp),” J. Inov. Penelit., vol. 2, no. 8, pp. 2849–2858, 2022.

[155] A. Supandi, “Pembangunan Kekuatan TNI AL Dalam Rangka Mendukung Visi Indonesia Sebagai Poros Maritim Dunia,” J. Pertahanan dan Bela Negara, vol. 5, no. 2, pp. 1–24, 2015.

[156] I. A. Sarjito, Kebijakan dan Strategi Pertahanan. CV Jejak (Jejak Publisher), 2023.

[157] R. K. Syahferzi, “Konversi Kapal Induk Izumo Dalam Perkembangan Sistem Pertahanan Nasional Jepang Tahun 2018,” 2022, Program Studi Ilmu Hubungan Internasional Fakultas Ilmu Sosial Dan Ilmu

[158] L. Yustitianingtyas, “Pengamanan dan Penengakan Hukum di Perairan Indonesia sebagai Konsekuensi Penetapan Alur Laut Kepulauan Indonesia (ALKI),” Pandecta Res. Law J., vol. 10, no. 2, pp. 143–152, 2015.

[159] M. N. Al Syahrin, “Kebijakan Poros Maritim Jokowi dan Sinergitas Strategi Ekonomi dan Keamanan Laut Indonesia,” Indones. Perspect., vol. 3, no. 1, pp. 1–17, 2018.

[160] M. W. Zacher, “The territorial integrity norm: International boundaries and the use of force,” Int. Organ., vol. 55, no. 2, pp. 215–250, 2001.

[161] M. E. Brown, The international dimensions of internal conflict, no. 10. Mit Press, 1996.

[162] S. A. Purwantoro, Sistem Pertahanan Rakyat Semesta Menyongsong Indonesia Emas 2045. Indonesia Emas Group, 2023.

[163] C. Limas, O. Setyaningsih, and I. Fauzi, “Konsep Smart Port di Ibu Kota Negara (IKN) Indonesia,” J. Penelit. Transp. Laut, vol. 23, no. 2, pp. 77–94, 2021.

[164] S. E. Ginting, D. Sufianto, and D. Sukmapryandhika, “Kolaborasi pemerintah daerah dengan satuan komando kewilayahan melalui fungsi pembinaan teritorial dalam

pengembangan potensi ekonomi lokal di Kabupaten Sukoharjo," J. Prinsip J. Mhs. Magister Ilmu Pemerintah., vol. 1, no. 1, 2024.

[165] A. W. Kusuma, L. Y. Prakoso, and D. Sianturi, "Relevansi Strategi Pertahanan Laut Berdasarkan Doktrin Jalesveva Jayamahe Terhadap Globalisasi Dan Perkembangan Lingkungan Strategis," J. Strateg. Pertahanan Laut, vol. 6, no. 1, 2020.

[166] P. Maesza, G. E. Saputro, and P. Suwarno, "Pengaruh Anggaran Pertahanan, Pertumbuhan Ekonomi, Dan Investasi Terhadap Ketimpangan Pendapatan Di Indonesia Tahun 2000-2019," J. Cafe., vol. 3, no. 1, pp. 130–140, 2022.

[167] Y. Geng and B. Doberstein, "Greening government procurement in developing countries: Building capacity in China," J. Environ. Manage, vol. 88, no. 4, pp. 932–938, 2008.

[168] A. J. Hillman, M. C. Withers, and B. J. Collins, "Resource dependence theory: A review," J. Manage., vol. 35, no. 6, pp. 1404–1427, 2009.

[169] S. Sumarlin, A. Adriyanto, and I. W. Warka, "Pertahanan Maritim: Antisipasi Ancaman Militer Melalui Kolaborasi Sumber Daya Nasional," J. Ind. Eng. Manag. Res., vol. 4, no. 6, pp. 20–27, 2023.

[170] A. M. K. Palar, R. T. Yulyanti, and M. A. Parasasti, "Pemberdayaan masyarakat pesisir sebagai komponen cadangan matra laut dalam mendukung pertahanan maritim Indonesia," J. Strateg. Pertahanan Laut, vol. 8, no. 2, pp. 57–72, 2022.

[171] L. Tang and P. Zhang, Human resource management in shipping: Issues, challenges, and solutions. Routledge, 2021.

[172] J. Parung, S. Larissa, A. Santoso, and D. N. Prayogo, "Penggunaan Teknologi Blokchain, Internet of Things Dan Artifial Intelligence Untuk Mendukung Kota Cerdas. Studi Kasus: Supply Chain Industri Perikanan," 2021, Universitas Surabaya.

[173] I. Naseer, "Cyber Defense for Data Protection and Enhancing Cyber Security Networks for Military and Government Organizations," MZ Comput. J., vol. 1, no. 1, 2020.

[174] A. Subagyo, "Sinergi dalam menghadapi ancaman cyber warfare," J. Pertahanan dan Bela Negara, vol. 5, no. 1, pp. 89–108, 2015.

HYBRID THREATS: A SERIOUS CHALLENGE TO THE CRITICAL INFRASTRUCTURE OF NATO ALLIES

Tamás SOMOGYI*, Rudolf NAGY**

* Doctoral School on Safety and Security Sciences, Óbuda University,
Budapest, Hungary
** Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda
University, Budapest, Hungary

Hybrid warfare may incorporate a wide range of abilities, conventional capabilities, irregular tactics and formations, indiscriminate violence and criminal disorder. All of these undoubtedly can jeopardize the political stability, the economic growth and the availability of essential services. As hybrid warfare is found to be actively used by NATO's adversaries from 2022, the security challenge faced by the operators of essential services in the EU and NATO became much more significant. Therefore, defense capability, especially cyber security plays a crucial role within NATO member countries. This paper aims to i) show the main elements of NATO's answer to the hybrid threats, with a focus on cyber security; and ii) provide some recommendations in order to enhance the resilience of critical infrastructure in NATO member states. In this study publicly available documents were explored and relevant literature was examined. As a result, this paper proposes the involvement of operators of essential services in training and exercises in order to enhance the level of resilience against hybrid threats.

Key words: *Critical Infrastructure Protection, cyber security, hybrid warfare, NATO.*

1. INTRODUCTION

As there have always existed important infrastructure, defending them was an essential question in the history. Building walls is a well-known example of critical infrastructure protection (Besenyő, 2017). Nowadays we have even more infrastructure to defend, since due to the advance in technology our accustomed life depends on many kind of infrastructure. Some of them are undoubtedly "essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people", as 2008/114/EC Article 2 defines the critical infrastructure in the European Union. Generally speaking, the energy, transportation, water and food supply, banking services, public safety and health services are considered essential services, provided or supported by the critical infrastructure. Any disruption of the critical infrastructure may result in a much higher impact on society (Luiijf and Klaver, 2021) and development (Chehabeddine and Tvaronavičienė, 2020). The outage of the energy infrastructure may cause the outage of food transportation, heating or electricity services (Sanders et al., 2022) for instance, or the outage of healthcare services (Besenyő et al., 2023) might cause loss of lives and lead to political instability. Moreover, critical infrastructure is a target of wars, e.g., Russia is attacking it in Ukraine (Padányi and Földi, 2023). Recognizing the increased dependence on infrastructure has fostered the research in this field (Galbusera, 2022; Scholz et al., 2022) and the adoption of critical infrastructure protection models in Europe and North America (Jones, 2007). No doubt, protecting the infrastructure, especially the critical one is an increasingly important area nowadays.

The smooth operation of essential services is jeopardize d by many threats from the effects of climate change (Lewin et al., 2023) to man-made attacks (Yosipof et al., 2023). In the latter category non-state actors can be found, e.g., well organized terrorist groups aiming to undermine the legitimacy of democratic national or regional governments (Besenyő and Kovács, 2023). However, the activity of state actors also can cause serious disruption. As Burmaoglu and Sarıtas (2017) have demonstrated, the characteristics of war had been profoundly changed: the asymmetric or hybrid warfare is one of the key determinants of current and future war concepts and technologies. For instance, disrupting a communication network to block the communication of security authorities (Suomalainen et al. 2022), the command and control of military operations (Hruza et al., 2024) or damaging the essential energy infrastructure (Lambert et al., 2022) can be a target. Przybylak (2024) has showed that nuclear power plants could be used by military forces as a kind of shields.

From 2022 the security challenge faced by the operators of essential services (OES) in the EU and NATO became much more significant. As it has been demonstrated, the war in Ukraine clearly shows the effects of the Russian hybrid warfare targeting critical infrastructure in the cyber space (Aviv and Ferri, 2023). Therefore, there is an urgent need to address this challenge in the critical infrastructure protection, especially in NATO member states. Although hybrid warfare is a topic that has been studied a lot, especially in the last decade, activities in the cyber space that jeopardize the operation of critical infrastructure is a crucial concern. This paper investigates the characteristics of hybrid warfare, with a special focus on the cyber security challenges, and aims to provide some recommendations to enhance the cyber security resilience of this domain in the NATO member states.

2. HYBRID WARFARE

According to Libiseller, who has conducted a literature review in this field, the terms ‘hybrid warfare’, ‘hybrid war’, and ‘hybrid threats’ are basically synonyms (Libiseller, 2023). In 2010, Hoffman published his famous work in which he defined hybrid threats as any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the battle space to obtain their political objectives (Hoffman, 2010). This type of warfare may incorporate a wide range of abilities, conventional capabilities, irregular tactics and formations, indiscriminate violence and criminal disorder. All of these undoubtedly can seriously jeopardize the political stability, the economic growth and the availability of essential services. For instance, some countries can give up their sovereignty in the face of hybrid warfare being waged against them in order to protect their economy and economic stability (Iskandarov and Gawliczek, 2022). It can be an extremely serious issue: it has been found that Ukraine’s per capita GDP foregone due to the war amounts to 15.1% on average for 2013–2017 (Bluszcz and Valente, 2022). Regarding to the political stability, democracy itself can also be threatened. Fox in his study suggests that Serbian and Russian nationalists and paramilitaries led by a Russian officer plotted to assassinate the Montenegrin prime minister in 2015 when Montenegro sought to join the NATO (Fox, 2021). Hoyle et al. shown that political tension and economic pressure can undermine and frustrate state-level decision-making (they call it societal destabilization). Incentivizing mass migration (Ďurkech and Švarný, 2016) or exploiting human traffic (Nagy et al., 2023) in order to weaken the political and economic stability can be another notable example of hybrid threat. It should be mentioned here that some elements of hybrid warfare undertaken by a state cannot be always considered as legal acts of war (Sanz-Caballero, 2023). Thus, protecting the critical infrastructure against the activities in the grey zone is crucial.

Moreover, disinformation campaign can also occur in hybrid warfare (Costigan and Tagarev, 2021). Winning the engagement of some countries, regions, communities can be crucial for NATO. However, adversaries may run disinformation campaigns to advance their interests and harm NATO's (Nelson, 2022; Pardyak, 2022). Thus, diplomatic, informational, military or economic resources can depend on the belief in the competing narratives. Undoubtedly, the problem of hybrid threats is even greater in countries where stability and peace is fragile and extremists are present (Fluri, 2020).

Combining regular and irregular mode of war is not new (Boda, 2024). However, as it has been explained in the Introduction, this security challenge recently became greater. Therefore, the capability of defense must consist of two parts: conventional capabilities and expertise at counterinsurgency and irregular types of warfare (Gentile, 2009). As cyber space became a field of hybrid warfare, no doubt, cyber-attacks must be incorporated into the irregular types of warfare.

2.1. Hybrid warfare and cyber security challenges

Beside the constant threat of cyber terrorism (Kenney, 2015) and criminal activities, guided cyber-attacks are also threatening the critical infrastructure. Due to the technical development, the Internet and relevant technologies became essential, since support the essential services. Since there are no borders in cyber space, and it is a worldwide thing, achieving absolute hegemony is impossible (Valuch et al., 2017). Moreover, it is difficult to identify the source of a cyber-attack. Therefore, cyber space is an ideal field for the hybrid warfare. Especially some parts of the cyber space, e.g., command and control systems and the national and military critical infrastructures are considered priority targets in a hybrid war (Grigore, 2021). But is cyber space really used to obtain political objectives?

In 2009 an analysis of Russia's war in Georgia already foreseen the possible further diversification of Russian military capability among which is the increase of ability to perform information warfare operations (Pallin and Westerlund, 2009). The information warfare operations are found to be part of the Russian military doctrine (Nilsson, 2021). And it has already been demonstrated that Russia is conducting non-military operations as well in order to achieve its own political and strategical goals in line with the so-called Gerasimov doctrine (Strucl, 2022; Jagiello, 2021). The Russians employ a blend of cyber and physical attacks on digital infrastructures since 2022 (Aviv and Ferri, 2023). Cyberattacks as part of the hybrid warfare have already been experienced by the operators of essential services in Europe in 2022 (Somogyi and Nagy, 2023). It should be mentioned that the critical infrastructure may be attacked indirectly as well. A well-known example of this is the ransomware called 'notPetya' that had been aimed to harm the Ukrainian infrastructure, however, it also has caused damage to the critical infrastructure outside of Ukraine (Harknett and Smeets, 2022).

So, all of these underpin that hybrid warfare poses a serious challenge to NATO's interest and security, especially to the critical infrastructure within NATO member countries. To answer to this challenge, NATO has identified cyberspace as a domain of operations and makes effort to strengthen its resiliency (Reveron and Savage, 2020). This will be looked at in the next section.

3. NATO'S RESPONSE TO HYBRID THREAT AND CYBER SECURITY RISKS

As it has been shown above, hybrid threats pose an increasing security challenge to NATO. And according to Dobias, NATO's adversaries are aware of NATO thresholds for employment of lethal force (Dobias, 2022), thus the hybrid threat will be probably not ended nor decrease. In this section NATO's response to hybrid threat and cyber security challenges will be described.

Addressing hybrid threats is part of NATO's deterrence and defense policy. Moreover, according to its latest annual report, countering such threats was a top priority in 2022 (NATO, 2023a). NATO's strategy makes clear that the primary responsibility to respond to hybrid threats or attacks rests with the targeted country (NATO, 2023b). However, NATO helps member countries to strengthen their resilience and supports members as part of the collective defense. In order to understand the sophisticated hybrid warfare applied by the adversaries and improve the ability of countering it, a strategy has been developed in 2015 in line with the prepare, deter and defend strategy. NATO states, that will deter hybrid attacks on the Alliance and, if necessary, will defend Allies concerned. First, to be prepared, information is continuously gathered by Joint Intelligence and Security Division, especially on the operations of the Russian Federation and the People's Republic of China. Focus has been put on the field of critical infrastructure protection and cyber security. In 2018 a team has been formed to support member countries in countering hybrid threats. Second, in order to deter hybrid threats, readiness and preparedness are being improved together with the decision-making process. And finally, should deterrence fail, NATO is ready to defend its members. A so-called Counter Hybrid Support Team can be sent to a member country requesting NATO support, either in a crisis or to help improving counter-hybrid capacities (Rühle and Roberts, 2021). Moreover, in 2016 it has been publicly stated that hybrid actions against NATO members can lead to the invocation of Article 5 of the Treaty ("the parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all...").

Hybrid threats are changing continuously since the tools of hybrid warfare are many. Therefore, countering them should be an adaptive activity. Elements of countering hybrid threats has been described by Hagelstam as follows (Hagelstam, 2018). Passive elements and active elements are need to be used in a harmonious way. Resilience is considered the passive part. Resilience of the critical infrastructure, the essential services, but also important is the safe operation of the state and the civil preparedness. Active elements have to be added on in order to being prepared and able to protect the critical infrastructure and essential services that highly probably will be targeted. However, as it has been mentioned above, enormous is the number of possible targets: from the global positioning systems and energy infrastructure to the transportation and banking industry or even the electoral system, press and social media.

As explained above, cyber threats are an essential part of the hybrid threats, therefore a special focus has to be put on this field. In NATO's Strategic Concept (NATO, 2022a), point 15 states that: "Cyberspace is contested at all times. Malign actors seek to degrade our critical infrastructure, interfere with our government services, extract intelligence, steal intellectual property and impede our military activities." Moreover, the Russian Federation (point 8) and People's Republic of China (point 13) are named as those actors who use cyber operations as part of their hybrid operations in order to reach their political goals. Therefore, in point 24, the political leaders of NATO promise that they "will expedite our digital transformation, adapt the NATO Command Structure for the information age and enhance our cyber defense s, networks and infrastructure. [They] will promote innovation and increase our investments in emerging and disruptive technologies to retain our interoperability and military edge. [They] will work together to adopt and integrate new technologies, cooperate with the private sector, protect our innovation ecosystems, shape standards and commit to principles of responsible use that reflect our democratic values and human rights."

Thus, NATO members work on strengthening their cyber defense capabilities: in May, 2022 the new strategic environment has been discussed by national cyber coordinators, and in December, 2022 a cyber exercise focusing on the protection of critical infrastructure took place in Estonia. No doubt, the best way to test NATO's structure, capabilities and tools is to exercise them. In addition to these, research centres have been founded to support NATO with knowledge, training and consultation. The European Centre of Excellence for Countering Hybrid Threats located in Helsinki serves as a hub of expertise, assisting member countries in improving their civil-military capabilities, resilience and preparedness.

At the 2023 NATO Summit in Vilnius, Allies endorsed a new concept of cyber defense. The point 66 of the Summit Communiqué says the following about this new concept: "It will further integrate NATO's three cyber defense levels - political, military, and technical - ensuring civil-military cooperation at all times through peacetime, crisis, and conflict, as well as engagement with the private sector, as appropriate. Doing so will enhance our shared situational awareness. Strengthening our cyber resilience is key to making our Alliance more secure and better able to mitigate the potential for significant harm from cyber threats." (NATO, 2023c) Thus, NATO's cyber defense capability has reached a high level and consists the following key elements (NATO, 2023d).

NATO's own ICT networks are protected by NATO Cyber Security Centre that provides non-stop centralised cyber defense support.

A Cyberspace Operations Centre has been found to support military commanders with situational awareness and to coordinate NATO's operational activities in cyberspace.

In the Defense Planning Process, targets are defined to be implemented by member states to strengthen the national cyber defense capabilities.

Cyber defense exercises are conducted to develop expertise and defense capabilities. Best practices are shared, information is exchanged. Training on the field of cyber security is available in the NATO Communications and Information (NCI) Academy in

Oeiras; in the NATO School in Oberammergau; and in the NATO Defense College in Rome.

Cyber Rapid Reaction Teams are ready to provide help to any member state at any time.

To further strengthen the defense capabilities in the Euro-Atlantic area, it is essential to have a strategic partnership between NATO and the EU. At the 2023 NATO Summit in Vilnius, this cooperation has been emphasized. Point 73 of the Summit Communiqué says: "The European Union remains a unique and essential partner for NATO. Our strategic partnership is essential for the security and prosperity of our nations and of the Euro-Atlantic area." (NATO, 2023c) Answering to the evolving cyber threats, in July, 2022 senior officials of the EU and NATO explored the possibilities to enhance cyber resilience (NATO, 2022b). Beside the cooperation with the EU, NATO has a partnership with non-EU states as well. Over 3000 participants from 38 countries have participated in the exercise Locked Shields in April, 2023 (NATO, 2023e). This is thought to be the world's biggest cyber defense exercise. Simulating tactical and strategic decisions in critical situations can undoubtedly enhance the preparedness for any cyber-attack, which is part of the hybrid warfare applied more frequently by NATO's adversaries.

Security experts of NATO and EU cooperate regularly by participating in each other's cyber security exercises organized by NATO's Cooperative Cyber Defense Centre of Excellence in Tallin (NATO, 2024). Training and education are also part of this cooperation, thus exchanging knowledge between these powers is ensured. Realizing the importance of the smooth operation of critical infrastructure, common crisis management exercises have been introduced. The so-called Parallel and Coordinated Exercises (PACE) creates the platform for a strengthening the preparedness of NATO and EU by organizing yearly exercises on a rotational basis. Altogether, enhancing cyber security of the Euro-Atlantic area is key point of the EU - NATO partnership.

As Hamilton pointed out, NATO's tasks of defense and deterrence, crisis management, and common security should be improved to meet all the threats (Hamilton, 2022). In order to have the necessary level of resilience, further development may be needed, especially in the field of cyber security. The next part aims to suggest new possible ways of further work and to provide some recommendations that can enhance the cyber security of the essential services.

4. ENHANCING CYBER SECURITY – RECOMMENDATIONS

A connection between a country's internal and external security and the level of cyber security has already been established (Sipos, 2023), therefore cyber security can be considered essential. Especially if the political and economic stability and the critical infrastructure are jeopardize d by hybrid threats. Thus, effective and improved deterrence and defense capabilities against hybrid threats are crucial. Although NATO's leading power is unquestionable, exploring new ways to improve it is important. In the field of cyber security and preparing to hybrid threats, training and exercises play a significant role. Therefore, further research and work relating to training and exercises are required.

NATO's Industry Cyber Partnership has been found to share information on cyber threats and information security best practices with partners from NATO member countries (Rühle and Roberts, 2021). This initiative is undoubtedly important, however, this kind of program for the operators of essential services is missing. The significance of critical infrastructure has been explained in the Introduction, and examples of cyber-attacks from irregular sources have been provided above. Therefore, programs for cyber security training and exercises are essential for the OES. Exploring and sharing best practices can improve the level of cyber security and even may lead to creating a kind of standard within NATO member countries. Thus, information sharing, demonstrations, community building can be urged, together with training.

As we pointed out above, cyber security training is an essential part of NATO's cyber defense capability. However, the possibility of an improved training to OES is missing. A common understanding of and approach to cyber security is important to have an effective minimum level of security in NATO's critical infrastructure. Experts in those sectors that provide essential service for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, undoubtedly shall be involved in the cyber security training. The basics of such a model for training is already exist, e.g., in the banking industry regular compulsory training is required by the sector specific authority (Somogyi and Nagy, 2022). A new training model should be created in order to have a regular NATO cyber security training in line with NATO standards for the OES in NATO member countries. Future research could investigate the necessity an applicability of a new standard for OES within NATO.

Training for the OES in NATO member countries can serve as the basis for a common exercise. Cyber defense exercises are conducted in NATO, however, the involvement of OES in such exercises is very limited. Thus, a broader and more mature cooperation could be recommended. The exercise Locked Shields in April, 2023 may serve as the basis of such a model for common exercises performed together with OES within NATO member countries. It should emphasized here that the outage of a critical infrastructure may have a negative effect on and can cause damage to other member countries as well. Therefore, the cooperation and common exercises are essential to improve the level of security, to learn and practice the decision-making process, the reporting and escalation in crisis situation. Moreover, such exercises can demonstrate the engagement with shared values and common responsibility. Beside the cooperation of member countries, the so called public-private partnership can be suggested as a way to improve the resilience, as both parties could contribute knowledge and best practice to build resilience of critical infrastructure. Resilience contributes to peace and security, therefore improving it is the key issue for the North Atlantic Treaty Organization.

5. CONCLUSION

NATO allies face security challenges from state and non-state actors who use hybrid warfare to threat and to damage critical infrastructure, political institutions and undermine the stability and security of NATO. Combining regular and irregular mode of war is not new. However, from 2022 the security challenge faced by the OES within the EU and NATO became much more significant. So, hybrid warfare poses a serious challenge to NATO’s interest and security, especially to the critical infrastructure in NATO member countries. Thus, NATO works on strengthening its cyber defense capabilities. NATO’s cyber defense capability has reached a high level and consists the key elements of cyber security training and cyber defense exercises.

NATO’s power is unquestionable, however, exploring new ways to improve is important. Although cyber security training is an essential part of NATO’s cyber defense capability, such training to OES provided in line with NATO standards is missing. This kind of training for the OES in NATO member countries can serve as the basis for a common exercise. Cyber defense exercises are conducted in NATO, so, the involvement of OES in such exercises could be recommended. The so called public-private partnership can be urged as a way to improve the resilience, as both parties could contribute knowledge and best practice to build resilience of critical infrastructure.

REFERENCES

[1] Aviv, I., Ferri, U. (2023) Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem, International Journal of Critical Infrastructure Protection, Vol 43, https://doi.org/10.1016/j.ijcip.2023.100637

[2] Besenyő, J. (2017) Fences and Border Protection: The Question of Establishing Technical Barriers in Europe, AARMS – Academic and Applied Research in Military and Public Management Science, 16(1), pp. 77–87. https://doi.org/10.32565/aarms.2017.1.7

[3] Besenyő J, Barten DG, De Cauwer HG, Tin D, Gulyás A. (2023) A Review of Ambulance Terrorism on the African Continent, Prehospital and Disaster Medicine, 38(2) https://doi.org/10.1017/S1049023X23000213

[4] Besenyő, J., Kovács, A. (2023) Healthcare Cybersecurity Threat Context and Mitigation Opportunities, Security Science Journal, 4(1). https://doi.org/10.37458/ssj.4.1.6

[5] Bluszcz, J., Valente, M. (2022) The Economic Costs of Hybrid Wars: The Case of Ukraine, Defense and Peace Economics, 33(1) https://doi.org/10.1080/10242694.2020.1791616

[6] Boda, M. (2024) Hybrid war: theory and ethics, AARMS, 23(1), https://doi.org/10.32565/aarms.2024.1.1

[7] Burmaoglu, S., Sarıtas, O. (2017) Changing characteristics of warfare and the future of Military R&D, Technological Forecasting and Social Change, Vol 116 https://doi.org/10.1016/j.techfore.2016.10.062

[8] Chehabeddine, M., Tvaronavičienė, M. (2020) Securing regional development, Insights into Regional Development, 2(1) http://doi.org/10.9770/IRD.2020.2.1(3)

[9] Costigan, S.S., Tagarev, T. (2021) Countering Crime, Hate Speech, and Disinformation in Cyberspace, Connections QJ, 20(2) https://doi.org/10.11610/Connections.20.2.00

[10] Dobias, P. (2022) Hybrid Warfare and the Need for Intermediate Force Capabilities, Connections QJ, 21(2) https://doi.org/10.11610/Connections.21.2.00

[11] Ďurkech, B., Švarný, J. (2016) Migration as security threat to EU, Security Culture, 22, https://www.ceeol.com/search/article-detail?id=753635

[12] Fluri, P.H. (2020) Stabilization Missions – Lessons to Be Learned from Resilience-Based Peacebuilding, Connections QJ, 19(4) https://doi.org/10.11610/Connections.19.4.04

[13] Fox, A.C. (2021) Russian hybrid warfare: A framework, Journal of Military Studies, 10(1) https://doi.org/10.2478/jms-2021-0004

[14] Galbusera, L. et al. (2022) Game-based training in critical infrastructure

protection and resilience, International Journal of Disaster Risk Reduction, Vol 78 https://doi.org/10.1016/j.ijdrr.2022.103109

[15] Gentile, G.P. (2009) The Imperative for an American General Purpose Army That Can Fight, Orbis, 53(3) https://doi.org/10.1016/j.orbis.2009.04.005

[16] Grigore, L.M. (2021) Strategic Leadership in Hybrid Warfare, International conference KNOWLEDGE-BASED ORGANIZATION, 27(1) https://doi.org/10.2478/kbo-2021-0008

[17] Hagelstam, A. (2018) Cooperating to counter hybrid threats, available at: https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html

[18] Hamilton, D.S. (2022) One Plus Four: What NATO's New Strategic Concept Should Say and How to Achieve It, Orbis, 66(1) https://doi.org/10.1016/j.orbis.2021.11.004

[19] Harknett, R.J., Smeets, M. (2022) Cyber campaigns and strategic outcomes, Journal of Strategic Studies, 45(4) https://doi.org/10.1080/01402390.2020.1732354

[20] Hoffman, F.G. (2010) 'Hybrid Threats': Neither Omnipotent Nor Unbeatable, Orbis, 54(3) https://doi.org/10.1016/j.orbis.2010.04.009

[21] Hruza, P., et al. (2024) Use of Information Technology by the Army of the Czech Republic for Command and Control in Operations, Science & Military, 19(1), https://doi.org/10.52651/sam.a.2024.1.5-14

[22] Iskandarov, K., Gawliczek, P. (2022) Economic coercion as a means of hybrid warfare: The South Caucasus as a focal point, Security and Defense Quarterly, 40(4) http://doi.org/10.35467/sdq/151038

[23] Jagiello, B. (2021) The Balkan Kettle: Russia's policy towards the Balkans, Security and Defense Quarterly, 35(3) https://doi.org/10.35467/sdq/138674

[24] Jones, A. (2007) Critical infrastructure protection, Computer Fraud & Security, issue 4. https://doi.org/10.1016/S1361-3723(07)70059-3

[25] Kenney, M. (2015) Cyber-Terrorism in a Post-Stuxnet World, Orbis, 59(1) https://doi.org/10.1016/j.orbis.2014.11.009

[26] Lambert, L.A., et al. (2022) The EU's natural gas Cold War and diversification challenges, Energy Strategy Reviews, Vol 43 https://doi.org/10.1016/j.esr.2022.100934

[27] Lewin, C., Rossi, M., Soultani, E., Raj, K.S. (2023) Managing infrastructure resilience and adaptation, Sustainable and Resilient Infrastructure https://doi.org/10.1080/23789689.2023.2241728

[28] Libiseller, C. (2023) 'Hybrid warfare' as an academic fashion, Journal of Strategic Studies, 46(4) https://doi.org/10.1080/01402390.2023.2177987

[29] Luiijf, E., Klaver, M. (2021) Analysis and lessons identified on

critical infrastructures and dependencies from an empirical data set, International Journal of Critical Infrastructure Protection, 35. https://doi.org/10.1016/j.ijcip.2021.100471

[30] Nagy, R. et al. (2023) The Relationship of Environmental Migration and Human Trafficking Concerning Natural Hazards at the Affected Regions of Africa, Journal of Central and Eastern European African Studies, 3(1) https://jceeas.bdi.uni-obuda.hu/index.php/jceeas/article/view/209

[31] NATO (2022a) Strategic Concept, available at: https://www.nato.int/cps/en/natohq/topics_210907.htm

[32] NATO (2022b) NATO and the European Union work together to counter cyber threats, available at: https://www.nato.int/cps/en/natohq/news_197959.htm

[33] NATO (2023a) The Secretary General's annual report 2022. available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/sgar22-en.pdf

[34] NATO (2023b) Countering hybrid threats, available at: https://www.nato.int/cps/en/natohq/topics_156338.htm

[35] NATO (2023c) Vilnius Summit Communiqué, available at: https://www.nato.int/cps/en/natohq/official_texts_217320.htm

[36] NATO (2023d) Cyber defense , available at: https://www.nato.int/cps/en/natohq/topics_78170.htm

[37] NATO (2023e) NATO Allies and Partners take part in world's largest cyber defense exercise available at: https://www.nato.int/cps/en/natohq/news_214144.htm

[38] NATO (2024) Relations with the European Union, available at: https://www.nato.int/cps/en/natohq/topics_49217.htm?selectedLocale=en

[39] Nelson, J. (2022) Developing a NATO Intermediate Force Capabilities Concept, Connections QJ, 21(2) https://doi.org/10.11610/Connections.21.2.05

[40] Nilsson, N. (2021) Between Russia's 'Hybrid' strategy and Western Ambiguity: Assessing Georgia's Vulnerabilities, The Journal of Slavic Military Studies, 34(1), https://doi.org/10.1080/13518046.2021.1923992

[41] Padányi, J., Földi L. (2023) The Effects of Armed Conflicts on the Environment, Contemporary Military Challenges, 25(1) https://doi.org/10.2478/cmc-2023-0004

[42] Pallin, C.V., Westerlund, F. (2009) Russia's war in Georgia: lessons and consequences, Small Wars&Insurgencies, 20(2), https://doi.org/10.1080/09592310902975539

[43] Pardyak, M. (2022) Fighting for Africans' Hearts and Minds in the Context of the 2022 War in Ukraine, Journal of Central and Eastern European African Studies, 2(4) https://jceeas.bdi.uni-obuda.hu/index.php/jceeas/article/view/182

[44] Przybylak, J. (2024) Nuclear power plants in war zones: Lessons learned from the war in Ukraine, Security and Defense Quarterly, 46(2), https://doi.org/10.35467/sdq/174810

[45] Reveron, D.S., Savage, J.E. (2020) Cybersecurity Convergence: Digital Human and National Security, Orbis, 64(4) https://doi.org/10.1016/j.orbis.2020.08.005

[46] Rühle, M., Roberts, C. (2021) Enlarging NATO’s toolbox to counter hybrid threats, available at: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html

[47] Sanders, P., Bronk, C., Bazilian, M.D. (2022) Critical energy infrastructure and the evolution of cybersecurity, The Electricity Journal, 35(10), https://doi.org/10.1016/j.tej.2022.107224

[48] Sanz-Caballero, S. (2023) The concepts and laws applicable to hybrid threats, with a special focus on Europe, Humanit Soc Sci Commun, 10(360) https://doi.org/10.1057/s41599-023-01864-y

[49] Scholz, C., Schauer, S., Latzenhofer, M. (2022) The emergence of new critical infrastructures. Is the COVID-19 pandemic shifting our perspective on what critical infrastructures are?, International Journal of Disaster Risk Reduction, Vol 83 https://doi.org/10.1016/j.ijdrr.2022.103419

[50] Sipos, Z. (2023) Cybersecurity in Algeria. Journal of Security and Sustainability Issues, 13(1) https://doi.org/10.47459/jssi.2023.13.6

[51] Somogyi, T., Nagy, R. (2022) Cyber threats and security challenges in the Hungarian financial sector, Contemporary Military Challenges, 24(3) https://doi.org/10.33179/bsv.99.svi.11.cmc.24.3.1

[53] Somogyi, T., Nagy, R. (2023) The Impact of the War in Ukraine on the Information Security of the European Union’s Banking Industry – A Case Study of Hungary And Slovakia, Contemporary Military Challenges, 25(3-4) https://doi.org/10.2478/cmc-2023-0020

[54] Strucl, D. (2022) Russian aggression on Ukraine: cyber operations and the influence of cyber space on modern warfare, Contemporary Military Challenges, 24(2), https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.6

[55] Suomalainen, J., et al. (2022) Security-driven prioritization for tactical mobile networks, Journal of Information Security and Applications, Vol 67, https://doi.org/10.1016/j.jisa.2022.103198

[56] Valuch, J., Gábriš, T., Hamuľák, O. (2017) Cyber Attacks, Information Attacks, and Postmodern Warfare, Baltic Journal of Law & Politics, 10(1) https://doi.org/10.1515/bjlp-2017-0003

[57] Yosipof, A., Woo, G., Komendantova, N., (2023) Persistence of risk awareness: Manchester arena bombing on 22 May 2017, International Journal of Disaster Risk Reduction, 94, https://doi.org/10.1016/j.ijdrr.2023.103805

FRAMEWORK OF ASCOPE/PMESII FOR MILITARY CONFLICT ANALYSIS IN RUSSIA-UKRAINE WAR

H.I. YUDISTIRA, A. FAISOL, A.K. SUSILO

Command and Staff College, Indonesia Navy
Ciledug Raya Cipulir, Kebayoran Lama, Jakarta, Indonesia

The Russia-Ukraine conflict in 2022-2024 began because Russia considered Ukraine's joining NATO would cause NATO members to side with Russia's military, and this was considered a threat to Russia. This incident highlights the evolution of modern warfare, which includes a combination of conventional, asymmetric, cyber, and non-military warfare.

This study uses a qualitative approach with deductive reasoning, supported by a comprehensive literature review. The results show that Russia's strategy focuses on controlling strategic areas and destabilizing Ukraine's politics, while Ukraine adopts a defense strategy that utilizes international support and power asymmetry. The ASCOPE/PMESII analysis reveals how both parties use various aspects of the operational environment (Area), infrastructure (Structures), capabilities (Capabilities), organizations (Organizations), society (People), and events (Events), as well as political, military, economic, social, information, and infrastructure dimensions (PMESII) to achieve their respective goals.

This study offers theoretical contributions to understanding the complexity of resource-based warfare, provides practical implications for the Indonesian Navy in dealing with hybrid threats, and provides managerial recommendations for decision-makers in designing adaptive defense policies. The implications of the Russia-Ukraine war provide educational, inspiring, and instructive insights for the Indonesian Navy in facing future geopolitical challenges..

Key words: *Russia-Ukrainian war, ASCOPE/PMESII analysis, geopolitics, national security.*

1. INTRODUCTION

The development of technology and information has created new models in today's warfare. The use of military and non-military capabilities is carried out to combine forces to create a stronger force. The combination of conventional warfare, asymmetric warfare, modern warfare, cyber warfare, and other non-military warfare is practiced and carried out in the current Russia-Ukraine war conflict [1]. This conflict stems from the long history of the two countries that are intertwined, which continues to complicate their relationship. Ukraine, as one of the countries formed after the collapse of the Soviet Union in 1991, has struggled to build a stable government and strengthen relations with other countries in the world. However, in 2014, relations between Russia and Ukraine deteriorated when Ukraine decided to move closer to the Western Bloc and postponed the signing of a proposed partnership agreement with the European Union.

In September 2020, Ukrainian President Volodymyr Zelenskyy approved a new National Security Strategy that emphasized the importance of developing a special partnership with NATO. This strategic move reflects Ukraine's commitment to enhancing its security and defense capabilities through cooperation with the North Atlantic Treaty Organization [2]. By emphasizing the development of a special partnership with NATO, Ukraine aims to strengthen its defense capabilities, enhance interoperability with NATO forces, and deepen cooperation in various security areas. This strategic alignment with NATO is of particular importance to Ukraine as it faces complex regional security challenges and seeks to safeguard its sovereignty and territorial integrity.

The armed conflict between the Ukrainian government and pro-Russian separatists continues and has resulted in many casualties and hundreds of thousands of civilians forced to flee, until finally on February 24, 2022, Russian President Vladimir Putin declared war on Ukraine, and since then Russia's military operations against Ukraine have begun.

The war between Russia and Ukraine in 2022 is a very complex and multidimensional conflict. This military operation is referred to as Russia's step in criticizing Ukraine for not joining NATO. Russia considers that Ukraine's joining NATO will cause NATO members to side with the military in Russia, and this is considered a threat to Russia [3]. This Russian invasion did not make Ukraine silent, a strategy was carried out by Ukraine to defend its territory from Russian attacks.

The use of information technology in this war is also carried out by using cyberwar as one of the strategies of both parties. In the current war, the use of non-military forces is carried out as a strategy to achieve victory, the non-military forces used include the use of information systems, building alliances with friendly countries, and building defense force arguments to the global community [4]. The war between Russia and

Ukraine has provided several relevant lessons not only for those directly involved but also for the international community as a whole.

According Raţiu & Munteanu [5], the success of a mission depends on the level of understanding achieved by the leader by integrating techniques for analyzing various aspects of the human terrain into the military decision-making process. Research by Qureshi et al [6] entitled Russia-Ukraine war and systemic risk: Who is taking the heat? Warns against the accumulation of systemic risk because sanctions can harm countries other than their main target, namely Russia. The Ukraine-Russia war has a significant trade impact on Ukraine and Russia, but only a limited impact on other countries [7].

This study aims to gain an understanding and analysis of resource-based warfare strategies applied from the Russia-Ukraine war in 2022-2024 using Clausewitz's theory of war which emphasizes the relationship between politics and war, as well as strategy theory to understand a systematic approach to achieving military goals amidst uncertainty. The analytical method applied is ASCOPE/PMESII, which is an analytical framework that integrates aspects of *Area, Structures, Capabilities, Organizations, People, and Events* (ASCOPE) with *Political, Military, Economic, Social, Information, Infrastructure* (PMESII). This method is used to evaluate the Russia-Ukraine war strategy in 2022-2024 from various multidimensional perspectives so that educational, inspiring, and instructive benefits are obtained for the Indonesian Navy.

This study provides strategic insights for the Indonesian Navy regarding resource-based warfare patterns, which can be an important reference in facing geopolitical challenges and hybrid threats in the future, in addition to the complexity of modern conflicts involving conventional, cyber, and non-military warfare, as well as the use of information technology in military strategy offered in this study.

The gap in this study lies in the focus of the analysis which only uses the ASCOPE/PMESII method without integrating other approaches, which can provide a broader perspective. In addition, there is also a lack of discussion about the long-term implications of this war on global geopolitical stability and how resource-based war strategies can be applied outside the context of the Russia-Ukraine conflict. This indicates the need for further research to enrich multidimensional analysis and expand the scope of the study. In theory, this study contributes to the development of an understanding of the relationship between war strategy and contemporary geopolitical dynamics, especially in the context of the Russia-Ukraine conflict, which can enrich the military strategy literature. In practice, the results of this study provide applicable insights for the Indonesian Navy in formulating adaptive and responsive defense strategies to hybrid threats, as well as improving the ability to analyze situations in the field. Thus, this study not only contributes to the development of theory but also provides practical and strategic guidance for military institutions in facing future challenges.

2. LITERATURE REVIEW

2.1. Theory of War

Carl von Clausewitz, a Russian military thinker, developed a theory of war that emphasized its complex and multidimensional nature. In his view, war is not just a military action, but a social and political phenomenon that is closely related to the goals of the state. Clausewitz argued that war is a never-ending cycle, and Clausewitz famously wrote, 'To ensure peace is to prepare for war.' In what Clausewitz called his theoretical concept of war, he outlined three goals of war [8]. First, the enemy's armed forces must be destroyed. Second, the state must be occupied. Third, the enemy's will must be broken.

Furthermore, Clausewitz introduced the concept of the "trinity" of war, consisting of 1) primordial violence, hostility, and hatred 2) chance and probability, and 3) the element of war subordinate to rational policy. The trinity serves as a magnet to balance the three forces of war - the people, the military, and the statesmen. Clausewitz argued that the spirit that fuels war must be present in the people, the courage and talent of the commanders and soldiers play a role in possibility and opportunity, but political goals are only the business of the government. In fact, without all three branches working in harmony, there will be war [9]. Clausewitz's theory remains relevant today because it provides a comprehensive framework for understanding the dynamics of war and the relationship between politics and the military.

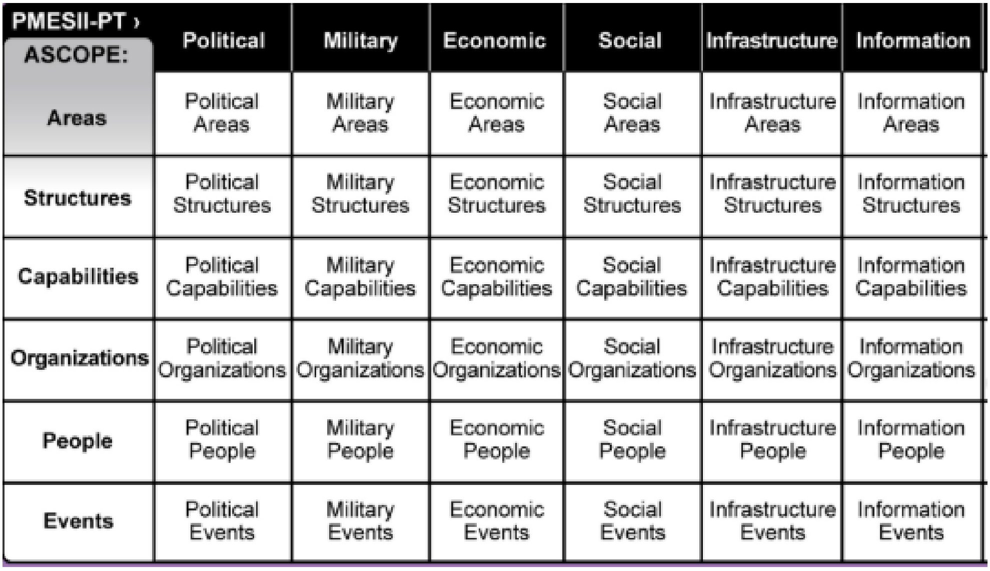
2.2. Human Resource Theory

Strategy theory is the study of how to achieve military objectives amid uncertainty and complexity. The strategy involves planning, organizing, and using resources to achieve competitive advantage and win conflicts. In the military context, "Strategy is the bridge that relates military power to political purpose. It is neither military power purpose nor political purpose. by strategy means the use that is made of force and the threat of force for the end of policy" [10]. It includes the selection of strategic objectives, the development of operational plans, and the management of available resources.

a. According to Von Clausewitz in his book entitled Vom Kriege or On War, Von Clausewitz argues "War is merely the continuation of policy by other means", War is an act of violence to force the opponent to submit to our will, the opponent must be made helpless by destroying his military strength, seizing his country and conquering the will to fight [11]. Regarding war strategy, Clausewitz stated "Strategy is The Art of The Employment of Battles, Mean to Gun The Object of War (Strategy is the art of fighting, as a means of achieving war goals). He also stated, "Strategy is the use of the engagement for war (strategy is the use of battles for war purposes)". In addition, context of war strategy, to grow national power, the term Diplomacy, Information, Military, and Economics DIME is known. DIME is used to determine the Course of Action in dealing with enemy actions or threats faced [12].
b. According to Hart's strategy is the art of distributing and applying military means to fulfill the ends of policy" (the art/skill of distributing and using (ways) military means (means) to achieve the ultimate goals of policy (ends)" [13]. From the definition, it is known that Strategy is the Science and art of determining goals (ends), formulating the methods taken (ways) and determining the infrastructure (means) used to achieve the goals. So the formulation of a strategy must contain goals (ends), the methods taken (ways), and the infrastructure (means) used. Russia and Ukraine use Strategy according to Liddell Hart in different ways, the interests of each country are different, where Russia has an interest in supporting the People of Donetsk and Luhansk, while Ukraine is interested in defending its territory.

2.3. ASCOPE/PMESII Analysis Theory

ASCOPE/PMESII is a comprehensive analytical framework used to understand and evaluate the operational environment in military and civilian contexts. This framework consists of five aspects, namely Areas, Structure, Capabilities, Organizations, People, and Events (ASCOPE) / Political, Military, Social, Economic, Infrastructure, and Information (PMESII). To form a structured approach to an action in the operational environment and analyze the external environment as a whole [15].



PMESII-PT › ASCOPE:	Political	Military	Economic	Social	Infrastructure	Information
Areas	Political Areas	Military Areas	Economic Areas	Social Areas	Infrastructure Areas	Information Areas
Structures	Political Structures	Military Structures	Economic Structures	Social Structures	Infrastructure Structures	Information Structures
Capabilities	Political Capabilities	Military Capabilities	Economic Capabilities	Social Capabilities	Infrastructure Capabilities	Information Capabilities
Organizations	Political Organizations	Military Organizations	Economic Organizations	Social Organizations	Infrastructure Organizations	Information Organizations
People	Political People	Military People	Economic People	Social People	Infrastructure People	Information People
Events	Political Events	Military Events	Economic Events	Social Events	Infrastructure Events	Information Events

Fig. 1. Matrices ASCOPE/PMESII.
Source: Tunning [14].

By combining these two components, ASCOPE/PMESII analysis allows for a holistic understanding of how various factors interact and influence the course of the conflict.

In the context of the Russo-Ukrainian War, ASCOPE/PMESII analysis is used to evaluate the strategies implemented by both parties. From a Russian perspective, this analysis highlights the importance of military and political factors in achieving its strategic goals, namely preventing Ukraine from joining NATO and maintaining geopolitical influence in the region. [16]. Russia uses conventional military superiority and information warfare to support its military operations. From a Ukrainian perspective, this analysis emphasizes the role of social and information factors in building civil resistance and rallying international support. Ukraine also uses asymmetric tactics and information technology to counter Russia’s larger military power.

Through ASCOPE/PMESII analysis, this study aims to identify relevant lessons for the Indonesian Navy in facing modern security challenges. Understanding the operational environment, the ability to adapt quickly to changing circumstances, and the use of information technology are increasingly important in today’s conflicts. In addition, the ability to build strategic alliances and partnerships, and mobilize public support, are also key factors in facing complex security threats. Thus, ASCOPE/PMESII analysis provides valuable insights for the Indonesian Navy in formulating an effective and adaptive defense strategy.

3. METHODOLOGY

In this case study, the 2022-2024 Russia-Ukraine conflict is the main focus of the analysis to understand the military strategies of both parties. This study uses a qualitative approach with a deductive method to explore in depth the complexities of modern warfare, including political, military, economic, social, informational, and infrastructure aspects. The ASCOPE/PMESII analytical framework is used to evaluate the multidimensional aspects of this conflict. Data collection was carried out through literature studies covering academic literature, official reports, strategic documents, and analysis from military experts. To strengthen the validity of data interpretation, internal brainstorming, and discussions with experts in the fields of military strategy, geopolitics, modern warfare, and military practitioners from the Indonesian Navy were also conducted. This research was conducted at the Navy Staff and Command School (Seskoal) by utilizing global data and literature studies relevant to the Russia-Ukraine conflict.

A deductive qualitative approach was applied in this study, the sequence of steps is as follows:

- First, the study begins by identifying relevant theories, namely Clausewitz's theory of warfare, strategy theory, and ASCOPE/PMESII analysis theory.
- Second, based on these theories, a conceptual framework is formulated that will be used to analyze the case study of the Russia-Ukraine conflict.
- Third, data is collected through a literature study that includes academic literature, official reports, and analysis by military experts.
- Fourth, the collected data is analyzed using the ASCOPE/PMESII framework to identify patterns and trends in military strategies implemented by both conflicting parties.
- Fifth, the results of the analysis are compared with previously formulated theories to confirm or reject the initial hypothesis.

4. RESULT

The results of the analysis show that Russia's strategy in the 2022-

2024 Ukrainian conflict focuses on achieving political goals through the use of measured military force, with the main goal of securing strategic areas and preventing Ukraine from joining NATO.

4.1. Analysis Based on Clausewitz's Theory of War

This study adapts Clausewitz's trinity concept to analyze the Russia-Ukraine war through three main elements: People, Military, and Statesman. This analysis aims to understand how these three elements interact and influence the course of the conflict, as well as their implications for the strategies implemented by both parties.

a. People

The "People" element reflects the emotional, cultural, and social aspects of the war. In the Russian context, the narrative constructed by the government about "special military operations" aimed at protecting ethnic Russians in Ukraine and preventing NATO expansion has succeeded in mobilizing domestic support. However, the escalation of the conflict and the economic impact of international sanctions have begun to raise doubts among the Russian public. In Ukraine, the “People” element manifested itself in high levels of patriotism and widespread civil resistance. Support from the Ukrainian diaspora around the world also provided an important resource for the Ukrainian government. Global public opinion, which largely supported Ukraine, exerted political and economic pressure on Russia.

b. Military

The “Military” element encompassed the operational and tactical aspects of the war. Russia initially relied on conventional military forces to achieve a quick victory, but stronger-than-expected Ukrainian resistance and logistical problems hampered Russian advances. Tactical adaptation became key, with Russia shifting to a more gradual strategy and focusing on consolidating territory in eastern and southern Ukraine. Ukraine, with limited resources, adopted a defensive strategy that utilized international support and asymmetric tactics. The use of information technology and cyber warfare also characterized the “Military” element of the conflict.

c. Statesman

The “Statesman” element reflects the high-level political, diplomatic, and strategic objectives that guide the course of the war. Russia’s political objective is to prevent Ukraine from joining NATO and maintain its geopolitical influence in the region. Russian statesmen use a combination of military pressure, diplomacy, and information warfare to achieve this objective. Ukraine’s political objective, on the other hand, is to maintain its sovereignty and territorial integrity and strengthen relations with Western countries. Ukrainian statesmen seek to build an international coalition to pressure Russia politically and economically. The role of international organizations, such as the UN and the European Union, is also an important part of the "Statesman" element in this conflict.

By analyzing the interactions between the People, Military, and Statesman elements, this study provides a more comprehensive understanding of the complexity of the Russia-Ukraine war. This conflict shows that strategic success depends not only on military power but also on the ability to mobilize popular support, exploit diplomatic opportunities, and adapt to changing operational environments.

4.2. Analysis Based on Strategy Theory

In the context of the 2022-2024 Russia-Ukraine war, strategy analysis can be conducted using the Ends, Ways, and Means framework, which helps identify goals, how to achieve those goals, and the resources used.

Table 1. Comparison of Russian and Ukrainian strategies in the 2022 war.

Strategy	Rusia	Ukraine
Ends	From a strategic perspective, Russia's primary goal in the Ukraine-Russia war is to maintain its influence over Ukraine and prevent the country from aligning with Western institutions such as NATO and the European Union	Ukraine's primary goal in the war is to expel Russian forces, protect its citizens, and maintain its independence as a sovereign state. It is important to note that Ukraine's goal is not only focused on defeating Russia but also on preserving its national identity, territorial integrity, and human rights
Ways	Military Intervention Information Warfare Diplomatic Maneuver Resource Leverage	Conventional Military Tactics Guerrilla Warfare Strategy Diplomatic Maneuver Cyberattacks
Means	Hybrid Warfare Proxy Warfare Military Economic Leverage	Military Economic Means Technological Means Diplomatic Means

a. Ends

Russia's Strategic Objectives. Your document states that Russia has political objectives, namely preventing Ukraine from joining NATO, protecting ethnic Russians in Ukraine, and maintaining Russian geopolitical influence in the region. These objectives translate into military objectives, such as securing strategic areas in eastern and southern Ukraine and destabilizing the pro-Western Ukrainian government. The document also states that these military operations are considered a Russian move to pressure Ukraine not to join NATO.

Ukraine's Strategic Objectives. Ukraine's strategic objectives are to maintain its sovereignty and territorial integrity, strengthen relations with Western countries, and secure military and financial assistance to counter Russian aggression. Ukraine's 2020 National Security Strategy, which emphasizes a special partnership with NATO, reflects these strategic objectives.

b. Ways

Russian Strategy. Russia initially used a conventional offensive strategy to achieve a quick victory (blitzkrieg). However, this strategy failed due to stronger-than-expected Ukrainian resistance and logistical problems. Russia then shifted to a more gradual strategy, focusing on consolidating controlled territory and using hybrid warfare tactics, including information warfare and economic pressure. Your document also mentions that this Military Operation was described as a Russian move to pressure Ukraine not to join NATO.

Ukraine Strategy. Ukraine adopted a defensive strategy that focused on the denial of objectives and imposing costs. This strategy included the use of international support, civil resistance, asymmetric tactics (such as the use of drones), and information warfare.

c. Means

Russian Resources. Russia relies on significant military power, including modern equipment and trained personnel. Russia also uses its energy reserves as a means to pressure Ukraine and European countries.

Ukraine Resources. Ukraine relies on military and financial assistance from Western countries, support from the local population, and a high level of patriotism. The use of information technology, such as social media, has also been an important tool for Ukraine to mobilize support and counter Russian disinformation.

Analysis based on the Ends, Ways, and Means framework shows that the success of both sides' strategies depends on their ability to balance their ends, means, and available means. Russia, with its resource advantage, seeks to achieve its political goals through military force. However, Ukraine has managed to hinder Russia’s progress by leveraging international support, asymmetric tactics, and high morale.

4.3. ASCOPE/PMESII Analysis

The ASCOPE/PMESII analysis provides a comprehensive understanding of the operational environment in Ukraine. From the Russian perspective, military (M) and political (P) factors are the most dominant, with a focus on the use of military force to achieve political goals. From the Ukrainian perspective, social (S) and information (I) factors are of great importance, with efforts to build public support and mobilize international opinion. Infrastructure (I) is also an important target for both sides, given its role in supporting military operations and civilian life. A review of the ASCOPE/PMESII analysis method from the Russian & Ukrainian perspectives can be seen in Table 2 and Table 3.

Overall, this study provides valuable insights for the Indonesian Navy in understanding the dynamics of modern conflict and its implications for national defense. The results of this study can be used as learning materials and input in formulating a more effective and adaptive defense strategy. In addition, this study also highlights the importance of understanding the operational environment (ASCOPE) and the political, military, economic, social, information, and infrastructure (PMESII) dimensions in planning and implementing military operations.

5. DISCUSSION

The 2022-2024 Russia-Ukraine War highlights the complexity of modern warfare that goes beyond conventional domains and includes asymmetric, cyber, and non-military dimensions. Analysis of the strategies of both parties reveals different approaches to utilizing resources and facing emerging challenges. Non-military forces are also used as strategies, including the use of information systems, building alliances with friendly countries, and building defense power arguments with the global community. Russia, with its conventional military advantage, initially adopted a blitzkrieg strategy aimed at achieving a quick victory and overthrowing the Ukrainian government. [17]. Ukraine, in defending its territory, carried out a strategy using modern warfare and utilizing information technology with cyberwar. This is in line with [18] In his book "Geodefense Future Defense Concept" he emphasizes the importance of adapting strategies in dealing with uncertainty on the modern battlefield.

Table 2. ASCOPE/PMESII Analysis Methodology - the Russian-Ukrainian War from a Russian perspective.

	P ***(Politic)***	**M** ***(Military)***	**E** ***(Economic)***	**S** ***(Social)***	**I*(Infrastructure)***	**I*(Information)***

A ***(Area)***	Historical Ties.
	Geopolitical Strategy
	Domestic Politics
		Donetsk and Luhansk;
		Crimea; Kharkiv and Chernihiv;
		Odessa and Mariupol;
		Lviv and Ivano-Frankivsk
			Trade;
			Energy;
			Infrastructure and Reconstruction
				National Identity;
				Media and Propaganda;
				Historical Narratives
					Transportation Infrastructure;
					NetworkASCOPE/ PMESII Analysis Methodology The Russian-Ukrainian War from a Russian perspective Communications;
					Energy Infrastructure;
					Military Bases and Installations;
					Border Security Infrastructure
						Propaganda and Disinformation;
						Media Coverage

S **(*Structures)***	Russian Government Leadership;
	State Institutions;
	Political Parties
		Russian Armed Forces;
		Central Command;
		Operational Command;
		Military Districts;
		Joint Task Forces;
		Special Operations Forces
			State Budget Structure;
			Domestic Economic Policy;
			Access to Capital Markets
				Historical Narrative;
				National Identity;
				Ethnic and Linguistic Affiliation;
					Transport Network;
					Border Infrastructure;
					Cyber Infrastructure;
					Humanitarian Infrastructure
						Official Government Statements;
						Media Coverage

	P ***(Politic)***	**M** ***(Military)***	**E** ***(Economic)***	**S** ***(Social)***	**I*(Infrastructure)***	**I*(Information)***

C ***(Capabilities)***	Leadership Authority;
	Government Institutions;
	Diplomatic Influence;
	Domestic Support and Stability
		Offensive maneuvers, defensive operations, and support for separatist groups;
		Nuclear capabilities;
		Missile capabilities;
		Advanced cyber warfare capabilities;
		Electronic Warfare;
		Asymmetric warfare and destabilizing enemy forces;
		Logistical capabilities.
			Energy Resources;
			Financial Reserves;
			Industrial Base;
			Trade Relations;
			Sanctions Resilience
				Historical Narrative;
				Media Influence;
				Cultural Diplomacy;
					Transportation Networks;
					Communication Systems;
					Energy Infrastructure;
					Cyber Infrastructure;
					Humanitarian Infrastructure
						Intelligence capabilities:
						Information propaganda capabilities;

O (Organization)	political organizations;
	Federal Assembly of the Russian Federation;
		Russian Armed Forces;
		Special Operations Forces (SOF);
		Information Warfare Units;
			Ministry of Finance;
			Eurasian Economic Union (EAEU);
				Russian Orthodox Church (ROC);
				State Agency for Culture;
					Ministry of Transport;
					Gazprom;
					Rosatom;
					Russian Railways (RZD);
					Roscosmos;
						RT (formerly Russia Today) and Sputnik;
						Federal Agency for Press and Mass Communications;

	P *(Politic)*	**M *(Military)***	**E *(Economic)***	**S *(Social)***	**I*(Infrastructure)***	**I*(Information)***

	United Russia party	Proxy Forces	Russian Direct Investment Fund (RDIF);
			Gazprom;
			Central Bank of Russia;
			Russian Chamber of Commerce and Industry
				Veterans Association;
				Youth Organizations;
				Media and Cultural Institutions;
				Public Opinion Research and Polling Institute
					Ministry of Energy;
					Regional and Municipal Authorities
						Internet Research Agency (IRA);
						Spokespersons and Government Officials

P *(People)*	Vladimir Putin;
	Russian Parliament
		Vladimir Putin;
		Sergey Shoigu;
		Valery Gerasimov;
		Alexander Dvornikov;
		Igor Konashenkov
			Vladimir Putin;
			Anton Siluanov;
			Mikhail Mishustin;
			Elvira Nabiullina;
			Dmitry Medvedev;
				Patriarch Kirill;
				Sergei Lavrov;
				Margarita Simonyan;
				Vladimir Soloviev
					Denis Manturov;
					Aleksandr Kozlov;
					Vitaly Markelov;
					Igor Sechin;
					Dmitry Rogozin
						Sergey Lavrov;
						Dmitry Kiselyov;
						Maria Zakharova

E *(Event)*	Russian Recognition of Donetsk and Luhansk;
	Deployment of Russian Peacekeepers
		Invasion of Eastern Ukraine;
		Siege of Mariupol;
		Battle of Kyiv;
		Occupation of Crimea;
			Investment Uncertainty;
			Impact of Sanctions;
			Ruble Devaluation;
				Public Demonstrations and Rallies;
				Cultural and Educational Exchanges;
					Military Development and Deployment;
					Cross-Border Infrastructure Projects;
						Propaganda Campaigns and Media Messaging;
						Disinformation Campaigns and Psychological Operations;

	P *(Politic)*	**M *(Military)***	**E *(Economic)***	**S *(Social)***	**I*(Infrastructure)***	**I*(Information)***

	to Eastern Ukraine;
	Bilateral Talks and Negotiations.
		Ceasefire Negotiations	Diversification of Economic Partnerships	*Memorialization and Commemoration;*
				Religious and Spiritual Engagement
					Energy Infrastructure Security;
					Information and Communication Networks;
					Transportation and Logistics;
					Critical Infrastructure Protection;
					Reconstruction and Rehabilitation
						Public Diplomacy and International Outreach;
						Social Media Influence Operations;
						Media Coverage;
						Diplomatic Initiatives and Peace Negotiations;
						Opinion Polls

Source: Data processed by the author

Table 3. ASCOPE/PMESII Analysis Methodology - the Russian-Ukrainian War from a Ukrainian perspective.

	P *(Politic)*	**M *(Military)***	**E *(Economic)***	**S *(Social)***	**I *(Infrastructure)***	**I *(Information)***

A *(Area)*	Territorial Integrity
	National Sovereignty
	Political Stability
		Eastern Ukraine;
		Kyiv;
		Southern Ukraine;
		Chernihiv and Sumy;
		Western Ukraine
			Trade and Investment;
			Energy;
			Infrastructure Damage;
			Foreign Aid and Assistance
				National Identity;
				Language;
				Religion;
				National Unity
					Transport Infrastructure;
					Energy Facilities;
					Communication Systems;
					Water and Sanitation Infrastructure
						Propaganda and Disinformation Campaigns;
						Public Opinion and National Unity

S *Structures*	Governmental Institutions;	Armed Forces of Ukraine;	Trade and Investment;	Historical Narrative;	Transportation Network;	Official Government Statements;

	P ***(Politic)***	**M** ***(Military)***	**E** ***(Economic)***	**S** ***(Social)***	**I** ***(Infrastructure)***	**I** ***(Information)***

	State Institutions;
	Ukrainian Parliament
		Special Operations Forces (SOF);
		Volunteer Battalions
			Government Expenditure and Budget Deficit;
			Inflation and Currency Devaluation
				National Identity;
				Cultural Resilience;
				Social Cohesion
					Communication Systems;
					Energy Infrastructure;
					Water Supply;
					Reconstruction Efforts
						Media Coverage

C ***(Capabilities)***	International Diplomacy;
	Strategic Communications ;
	Adaptability
		Mobilizing conventional forces;
		Air and Missile Defense;
		Cyber Warfare;
		Naval Capabilities
			Economic Challenges;
			Resilience and Adaptability;
			International Support
				Historical Narrative and National Identity;
				Cultural Heritage and Language;
				Education System and Societal Values
					Transportation Infrastructure;
					Energy Infrastructure;
					Communications Infrastructure;
					Water and Sanitation Infrastructure;
					Health Infrastructure
						Strategic Communications;
						Countering Disinformation;
						Cyber Defense and Resilience

O (Organization)	Zelensky and his government;
	political parties;
	Civil society organizations and volunteer groups
		Ukrainian Armed Forces;
		Special Operations Forces (SOF);
		Civil Support;
		International Assistance
			Central Bank of Ukraine;
			Ministry of Finance of Ukraine;
			Association of Ukrainian Entrepreneurs;
			Ukrainian Foreign
				Maidan SOS;
				Helsinki Initiative-XXI;
				Ukrainian Helsinki Human Rights Union (UHHRU);
					State Emergency Service of Ukraine (SESU);
					Ministry of Infrastructure of Ukraine;
					Ukrainian Railways (UZ);
					Naftogaz of Ukraine;
						Ukrainian Crisis Media Center (UCMC);
						UKRINFORM;
						UHHRU

	P ***(Politic)***	**M** ***(Military)***	**E** ***(Economic)***	**S** ***(Social)***	**I** ***(Infrastructure)***	**I** ***(Information)***
			Investment Board	International Renaissance Foundation (IRF)	National Guard of Ukraine	

P ***(People)***	Volodymyr Zelensky;
	Dmytro Kuleba;
	Andriy Yermak;
	Denys Shmyhal
		Volodymyr Zelensky;
		Valerii Zaluzhnyi;
		Sergei Shaptala;
		Andriy Taran;
		Oleksandr Syrskyi
			Oleksiy Markarov;
			Volodymyr Melnyk;
			Tymofiy Mylovanov;
			Aivaras Abromavicius
				Serhiy Zhadan;
				Oksana Zabuzhko;
				Andriy Kurkov
					Denis Manturov;
					Aleksandr Kozlov;
					Oleksandr Kubrakov;
					Volodymyr Omelyan
						Volodymyr Zelenskyy;
						Mykhailo Fedorov;
						Oleksandr Tkachenko;
						Dmytro Kuleba

E ***(Event)***	Martial Law and General Mobilization;
	Ukraine's EU Candidate Status;
	Liberation of Kherson
		Invasion of Eastern Ukraine;
		Siege of Mariupol;
		Battle of Kyiv;
		Battle of Donbas
			Energy Security;
			Currency Fluctuations;
			Infrastructure Reconstruction and Investment;
			Sanctions and Economic Pressure on Russia
				National Unity and Solidarity;
				Civil Society Activism;
				Cultural Resilience and Expression;
				International Solidarity
					Infrastructure Damage;
					Reconstruction Efforts;
					Strategic Importance of Infrastructure;
					Cyberattacks on Infrastructure
						Disinformation and Propaganda Campaigns;
						International Media Coverage;
						Social Media and Digital Activism;
						Official Communications and Public Diplomacy;
						Digital Security and Cyber Defense

Source: Data processed by the author

Besides that, Ukraine's strategy is based on denial of objectives and imposing costs against Russia [19]. Ukraine leveraged international support, high patriotism, and asymmetric tactics to slow Russian advances and increase costs. Based on strategic theory, Russia implemented a combination of offensive and defensive strategies tailored to achieve its geopolitical goals while countering the perceived threat of Western encroachment [20]. This is in line with Cordesman's (2017) study which highlighted the important role of innovation and adaptation in modern warfare, especially for states facing a larger military power.

ASCOPE/PMESII analysis provides a useful framework for understanding the complex operational environment of this conflict. From the Russian perspective, military and political factors are most dominant, using military force to achieve political goals. From the Ukrainian perspective, social and informational factors are of paramount importance, with efforts to build public support and mobilize international opinion. Infrastructure is also an important target for both sides, given its role in supporting military operations and civilian life. This is in line with Kofman et al. [21] who emphasize the importance of understanding the social and informational dimensions of modern warfare, and their implications for military strategy.

Implications

Theoretical Implications

Theoretically, this study contributes to the development of strategy theory and conflict studies by applying the ASCOPE/PMESII framework in analyzing the Russia-Ukraine war. This study enriches the understanding of how various factors (area, structure, capability, organization, society, and events) and dimensions (political, military, economic, social, information, and infrastructure) interact and influence the course of the conflict. In addition, this study also strengthens the relevance of Clausewitz's theory on the relationship between politics and war in the context of modern conflict. By integrating strategy theory and the ASCOPE/PMESII framework, this study offers a more comprehensive approach to analyzing conflict and formulating effective defense strategies.

Practical Implications

Practically, this study provides valuable insights for the Indonesian Navy in facing maritime security challenges in the regional area. The results of this study can be used as learning materials and input in formulating a more adaptive and responsive defense strategy to hybrid threats. This study also highlights the importance of understanding the operational environment and the dimensions of politics, military, economic, social, information, and infrastructure in planning and implementing military operations. The recommendations resulting from this study can help the Indonesian Navy in improving its situational analysis capabilities, developing new tactics and technologies, and strengthening cooperation with strategic partners. Thus, this study contributes to improving the readiness and effectiveness of the Indonesian Navy in maintaining Indonesia's maritime security and sovereignty

6. CONCLUSIONS

This study, which focuses on a case study of the 2022-2024 Russia-Ukraine war using ASCOPE/PMESII analysis, aims to understand resource-based warfare strategies and their benefits for the Indonesian Navy. The results of the analysis show that this conflict is a complex example of modern warfare involving a combination of conventional, asymmetric, cyber, and non-military warfare. Russia's strategy initially focused on achieving political goals through the use of measured military force, while Ukraine adopted a defensive strategy that utilized international support and asymmetric tactics.

ASCOPE/PMESII analysis reveals how both parties utilized various aspects of the operational environment (Area, Structures, Capabilities, Organizations, People, and Events) as well as political, military, economic, social, information, and infrastructure (PMESII) dimensions to achieve their respective goals. Russia utilized military superiority and information capabilities, while Ukraine relied on international support, asymmetric tactics, and civil resistance.

From the perspective of Clausewitz's theory of war, this conflict asserts that war is a continuation of politics by other means, where political goals guide military strategy. Strategy theory helps understand how both parties plan, organize, and use available resources to achieve their respective goals. The application of the ASCOPE/PMESII framework provides a more comprehensive understanding of the operational environment and the factors that influence the course of the conflict.

Overall, this study provides theoretical implications in enriching the understanding of modern war strategy and conflict studies. The practical implication is to provide valuable insights for the Indonesian Navy in facing maritime security challenges in the regional area. This study highlights the importance of understanding the operational environment, adapting to changing situations, and utilizing information technology in planning and implementing military operations. Thus, the results of this study can be used as learning materials and input in formulating a more effective and adaptive defense strategy for the Indonesian Navy.

Further research can also develop computer-based simulation models to predict the impact of various military and non-military strategies in conflict, or further explore the role of information technology and social media in influencing public opinion and conflict dynamics. Additionally, an in-depth analysis of the ethical and legal implications of the use of asymmetric tactics and cyber warfare is also a promising area for future research.

ACKNOWLEDGEMENT

This study was supported by Naval Staff and Command College. Appreciation and sincere thanks to all leaders of the Indonesian Navy. Researchers would like to thank all parties who have participated in completing and supporting the implementation of this research so that it can be completed smoothly.

REFERENCES

[1] M. Khudaykulova, H. Yuanqiong, and A. Khudaykulov, “Economic Consequences and Implications of the Ukraine-Russia War,” the International Journal of Management Science and Business Administration, vol. 8, no. 4, pp. 44–52, 2022, doi: 10.18775/ijmsba.1849-5664-5419.2014.84.1005.

[2] A. G. Kostyrev, “NATO-Ukraine strategic communications: theory and practice,” 2023.

[3] M. Saeri, A. Jamaan, M. F. Surez, P. Gayatri, H. I. Utami, and Z. Zarina, “Konflik Rusia-Ukraina Tahun 2014-2022,” Dinamika Global: Jurnal Ilmu Hubungan Internasional, vol. 8, no. 2, pp. 319–334, 2023.

[4] M. Y. Samad and P. D. Persadha, “Memahami Perang Siber dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman di Siber,” JURNAL IPTEKKOM Jurnal Ilmu Pengetahuan & Teknologi Informasi, vol. 24, no. 2, pp. 135–146, 2022.

[5] A. Raţiu and A. Munteanu, “Hybrid Warfare and the Russian Federation Informational Strategy to Influence Civilian Population in

Ukraine," Land Forces Academy Review, vol. 23, no. 3, pp. 192–200, 2018, doi: 10.2478/raft-2018-0023.

[6] A. Qureshi, M. S. Rizwan, G. Ahmad, and D. Ashraf, "Russia–Ukraine war and systemic risk: Who is taking the heat?," Finance Research Letters, vol. 48, no. May, p. 103036, 2022, doi: 10.1016/j.frl.2022.103036.

[7] S. Steinbach, "The Russia–Ukraine war and global trade reallocations," Economics Letters, vol. 226, no. August 2022, p. 111075, 2023, doi: 10.1016/j.econlet.2023.111075.

[8] J. Lindell, "Clausewitz : War, Peace and Politics", E-International Relations, pp. 1–7, 2017, [Online]. Available: https://www.e-ir.info/pdf/2735.

[9] T. Waldman, "Clausewitz and the study of war," Defence Studies, vol. 12, no. 3, pp. 345–374, 2012, doi: 10.1080/14702436.2012.703843.

[10] C. von Clausewitz, On War (Translate by M. Howard and P. Paret, Trans.). 1984.

[11] A. Setiawan, "Pengantar Hubungan Internasional," Repository UMJ, pp. 11–117, 2021.

[12] Craft Defense state, "Diplomatic political," Defensestatecraft, 2023.

[13] L. Milevski, "Liddell Hart's Impact on the Study of Grand Strategy," The Oxford Handbook of Grand Strategy, pp. 73–88, 2021.

[14] C. W. Tunning, "The Analytics Quotient: Retooling Civil Affairs for The Future Operating Environment," 2020.

[15] B. Janse, "PMESII-PT Analysis, an army Theory explained," ToolsHero, 2024. .

[16] A. N. Melania, "Nato Strategy in the Russia-Ukraine Conflict: Analysis Based on Defensive Realism Theory 2014-2022." Universitas Islam Indonesia, 2024.

[17] C. Ferruzzi, "Russian Airpower in Ukraine: Analyzing the Performance of Russia's Aerospace Forces and its Implications for the Theory of Airpower," 2023.

[18] I. A. Sarjito et al., Geodefense Konsep Pertahanan Masa Depan. Indonesia Emas Group, 2024.

[19] C. Pischedda and A. Cheon, "Does plausible deniability work? Assessing the effectiveness of unclaimed coercive acts in the Ukraine war," Contemporary Security Policy, vol. 44, no. 3, pp. 345–371, 2023.

[20] D. V Gioe, M. Miron, and M. Ozawa, "Reassessing NATO's deterrence and defence posture in the Baltics: rebalancing strategic

priorities to counter Russian hybrid aggression,” Defense & Security Analysis, vol. 41, no. 1, pp. 145–165, 2025.

[21] M. Kofman, A. Fink, D. Gorenburg, M. Chesnut, J. Edmonds, and J. Waller, Russian military strategy: core tenets and operational concepts, vol. 104. CNA Arlington, Virginia, USA, 2021.

THE REPUBLIC OF MOLDOVA IN THE CONTEXT OF THE RUSSIAN FEDERATION HYBRID WAR

Svetlana CEBOTARI *, Ion COROPCEAN **, Selena STEJARU***

* Department of International Relations, Faculty of International Relations, Political and Administrative Sciences, State University of Moldova;
"Alexandru cel Bun" Military Academy
** Agency for Science and Military Memory, Ministry of Defense of the Republic of Moldova;
*** Department of International Relations,, Faculty of International Relations, Political and Administrative Sciences,
State University of Moldova

Nearly 35 years after the conclusion of the Cold War and the collapse of the former Soviet Union, the Russian Federation, as its successor, strives to reclaim its status as a great power. More than three decades since the dissolution of USSR and Moldova's declaration of independence on August 27, 1991, the Republic of Moldova remains a state where the Russian Federation pursues its own geopolitical interests, employing a range of strategies from soft power to coercion in order to achieve its objectives. Since early 2000s, the Russian Federation has adopted a more assertive policy to reestablish its influence in the "near abroad," a region where it continues to advance its geostrategic interests. In this manner, the Russian hybrid warfare against the Republic of Moldova reflects its broader strategy of maintaining regional dominance. Since the end of the Cold War and the dissolution of USSR, the Russian Federation, as its successor, has persistently sought to regain its status as a global power. The purpose of this article is to highlight the main elements of the hybrid war used by the Russian Federation to maintain the Republic of Moldova within its sphere of influence.

Key words: *hybrid warfare, financing, disinformation, fake news, Russian Federation, Republic of Moldova*

1. INTRODUCTION

Interference in the internal affairs of states is not only a longstanding phenomenon but also a persistent feature of international relations. External interventions are far from being a recent development, as states have always found ways to justify even the most blatant violations of the sovereignty of the nations they target. The Republic of Moldova's close proximity to an active war has given rise to numerous national security threats. After the European Union granted Moldova candidate status in June 2022 and launched EU accession negotiations in June 2024, alongside the heightened political rhetoric surrounding the country's geopolitical orientation, Moldova has increasingly become a target of foreign interference. Since February 2022, in the wake of the Russian Federation invasion of Ukraine, political discourse surrounding the Republic of Moldova's geopolitical alignment has grown increasingly intense. The country is now the focus of a "hybrid war" orchestrated from abroad, particularly by Russia. Since the 2000s, in its pursuit of reclaiming "great power" status within the "near abroad", a region of critical geostrategic interest, the Russian Federation has adopted an assertive policy aimed at restoring its influence. In this context, the hybrid war waged by the Russian Federation in the Republic of Moldova represents a continuation of its policy to advance its dominance in the region. Since the end of the Cold War and the collapse of USSR, the Russian Federation, as its successor, has continuously strived to restore its standing as a great power.

2. CONCEPTUAL AND THEORETICAL IDENTIFICATIONS OF THE "HYBRID WAR" PHENOMENON

As a result of the crisis in Ukraine, the term "hybrid war" has increasingly appeared in specialized literature, as well as in the speeches of politicians, polemologists, and representatives of the academic community (Presa străină). Currently, Western experts use the term "hybrid war" to describe the conflict between the Russian Federation and Ukraine (Moldavie : courte victoire du «oui»). The "hybrid" component, derived from the Latin hibrida, meaning mixture or combination, refers to an organism or cell that, through genetic crossbreeding, acquires a new form (Evaluarea implicării Federației Ruse în procesele electorale din Republica Moldova).

Some polemologists believe that the origins of "hybrid war" date back to the 1920s (characterized by the methods and activities of special services). However, an analysis of Soviet-American relations during the final phase of the Cold War reveals early manifestations of the "hybrid war" concept (Presa străină). According to Zbigniew Brzezinski, "hybrid war" was employed during the Cold War by both the former USSR and the USA. Currently, the new world order is losing the structural and coordinating capacity it possessed during the bipolar era. In this context, it is worth noting the research on "hybrid war" conducted by E. Messner in the 1960s. Messner suggests that in the near future, warfare without the involvement of military troops—specifically involving partisans, saboteurs, terrorists, subversives, diversionists, and propagandists—will assume significant proportions. However, according to Messner, irregular actions that lack support from official forces (instructors, weapon supplies, combat equipment, medicines, gear, financial resources) are destined to fail. Such actions gain power, success, and results only through the material and moral support of primary forces: the success of primary forces enhances the activism of irregular forces and contributes to their numerical growth (Fiodorov, 2016).

Messner's theses were studied by the Russian General Staff and in Russian military academies. Many of the ideas Messner presented were integrated into the Russian concept of hybrid war, developed in 2012 by the Russian General Staff. This concept was first publicly presented by Chief of the General Staff Valery Gerasimov in early 2013, at a meeting of the Academy of Military Sciences. In his publication „The Value of Science in Foresight" based on the "Arab Spring" experience, Gerasimov outlined the Russian perspective on the Western approach to warfare and the nature of modern military conflicts:

In the 21st century, the distinction between war and peace is increasingly blurred. Wars are no longer declared, and once initiated, they do not follow the traditional patterns.

The focus of confrontation methods has shifted to the widespread use of political, economic, informational, humanitarian, and other non-military measures, often implemented through the protest potential of the opposing state's population.

These methods are complemented by covert military actions, including informational warfare and the operations of special forces. The open use of force, often under the guise of peacekeeping and crisis management, is employed primarily to achieve final success in the conflict.

Asymmetric actions are widely used to neutralize the enemy's superiority in armed combat. This includes leveraging special operations forces and internal opposition to create a persistent front throughout the opponent's territory, as well as conducting informational influence, with constantly evolving forms and methods.

Following the annexation of Crimea in 2014, where these outlined provisions were practically tested, this report was perceived as a policy document and an example of a warfare approach, becoming known as the "Gerasimov Doctrine" (Gherasimov). The discussions held in January 2013 at the General Assembly of the Academy of Military Sciences in Moscow also addressed issues related to new forms of contemporary warfare, conflict conditions, present elements, operational stages, and new methods of exerting pressure on the enemy through political, economic, and humanitarian means. Informational tools played a role in every stage of the conflict: initiation, development, and post-conflict phases. Special attention was given to "asymmetric methods" that enable internal opposition actions and psychological impact on the adversary. Many of the elements discussed in 2013 were applied by the Russian Federation during the annexation of Crimea and later in eastern Ukraine.

F. van Kappen, addressing the new war paradigm, stated: "Hybrid war represents a combination of classical warfare with the use of new elements. The state engaged in a 'hybrid war' makes agreements with non-state executors - fighters, local population groups, organizations, with which it fully denies any connection. These executors can perform actions that the state itself would not undertake. All dirty work is carried out by non-state formations." The Russian Federation, through classic scenarios of maintaining frozen conflicts, such as the Transnistrian conflict in Moldova or the South Ossetian and Abkhaz conflicts in Georgia, currently resorts to energy resource blackmail as elements of "hybrid war" (Bernhard). A definition of "hybrid war" was also proposed by NATO's Supreme Allied Commander in Europe, General F. Breedlove. He argues that "hybrid war" consists of several components, which were present in past military practices but not to the same extent. The first characteristic is diplomatic warfare, aimed at breaking agreements between states, dismantling alliances, and depriving states of international support. The second characteristic involves mobilizing media and other tools to influence public psychology, creating a false image of unfolding events. The third characteristic is the unchanged military component, but with innovation in how the state’s army is used covertly, with the state denying direct involvement. Economic warfare, including recognized forms like blackmail, embargoes, and fuel price hikes, is also part of this strategy (Géopolitique).

In geopolitical terms, "hybrid war" is a new concept, particularly relevant in the realm of special forces operations, combining robust resistance to international security threats with lessons learned from combating extremism by state and non-state actors. "Hybrid war" is conducted both by forces seeking to weaken or overthrow governance, acting from within a state or region, and by external forces. External actions involve supporting and converting sympathizers for operational support, impacting the economy and social sphere, coordinating diplomatic efforts, and conducting protest actions. At a general level, "hybrid war" today refers to the relationship between belligerent parties, addressing both international and regional security incidents, as well as the national security of individual states. Scholars attempt to frame this phenomenon within more or less theorized categories, using the "hybrid war" concept to describe actions in Crimea and southeastern Ukraine (Ingérence, droit d'ingérence).

Starting from the broadest definitions of hybrid warfare accepted by academic communities, "hybrid warfare" refers to a type of conflict in which one of the belligerent parties employs both conventional military methods and unconventional or non-military means simultaneously (Acuzații de cumpărare de voturi și interferență a Rusiei). The Russian Federation military aggression against Ukraine in 2014 led to a significant distortion of the international and regional security systems, as well as the international legal framework. Virtually all international security guarantees for Ukraine (including those outlined in the Budapest Memorandum) can be considered ineffective, given that the primary aggressor—the Russian Federation—acts as the principal guarantor. From a structural-functional perspective, "hybrid warfare" is unique: its form is "hybrid," while its content is "asymmetric." The novel characteristics of this new hybrid warfare were evident during the annexation of Crimea by the Russian Federation in the spring of 2014 and later in its support of separatist elements in eastern Ukraine. The innovative nature of this phenomenon lies in the interplay of its elements, the dynamic and skillful use of these elements, and the increasing importance of the informational factor. In some cases, the informational factor becomes independent and is as crucial as the military component. Although many researchers and polemologists emphasize the "hybrid" nature of this war, the conceptualization of the phenomenon remains incomplete.

The concept of hybrid warfare has little in common with the traditional rules governing classical warfare between belligerent parties. Instead, it is more akin to an asymmetric war with minimal use of military potential to achieve strategic objectives. In this conflict (specifically, by Moscow), all possible means are utilized to achieve geostrategic objectives and interests—ranging from partisan groups, information and cyber warfare, urban revolts, economic pressures, to conflicts instigated by diversionist groups. U.S. Army General B. Hodges stated that within a few years, Russia would have the capability to wage war in multiple directions (Presa străină scrie). F.G. Hoffman, a former U.S. Navy officer and current research fellow at the U.S. Department of Defense, specializing in armed conflicts and politico-military strategies, believes that conflicts will become multimodal, unfolding concurrently in several directions through various means. According to Hoffman, future threats may be characterized as hybrid, combining traditional tactics with new strategies. This approach involves planning and execution with the participation of non-state actors who use both simple and advanced technologies. Hoffman also argues that "hybrid warfare" can be multimodal (conducted by both states and various non-state actors).

To describe the ongoing conflict between Ukraine and the Russian Federation, terms such as "unconventional warfare," "irregular warfare," "compound warfare," or "state-sponsored hybrid warfare" are also used. Virtually all forms of warfare reference the presence of military conflict and the involvement of non-military means, which often bear little resemblance to classical military confrontations. However, the methods used by the Russian Federation against Ukraine have not been fully conceptualized by either domestic or Western researchers. The genesis of the "hybrid warfare" concept, its stages, components, and main directions remain under scrutiny and require further definition.

3. ELEMENTS OF RUSSIAN HYBRID WARFARE IN THE REPUBLIC OF MOLDOVA

Approximately 35 years after the end of the Cold War and the collapse of the former USSR, the Russian Federation, as its successor, seeks to reestablish its status as a great power. More than three decades since the Republic of Moldova’s declaration of independence on August 27, 1991, it remains a state in which the Russian Federation pursues its own geopolitical interests. To achieve these interests, Russia employs a spectrum of methods ranging from soft power to coercion. Since the early 2000s, Russia has relaunched an offensive policy aimed at restoring its influence in the "near abroad," a region it continues to view as a zone of geostrategic interest (Barnaud). In this context, for the Russian Federation, the hybrid war waged in the Republic of Moldova represents a continuation of its policy to assert dominance in this region, which is regarded as a "gray zone" of confrontation with the West (NATO Summit prokladîvat kurs).

The Russian Federation interest in maintaining the Republic of Moldova within its sphere of influence lies in "halting Moldova’s pro-European trajectory" (Geoană). Given that Moldova received EU candidate status on June 23, 2022 (Conțu, 2022), and continues to register processes and implement democratic reforms, Russia does not accept the Republic of Moldova drift away from its influence. Consequently, Moldova's democratic processes and reforms aimed at meeting European standards—including strengthening mutually beneficial relations with the USA, NATO, and the EU—conflict with Russian interests. In this regard, the Republic of Moldova becomes a target for Russia’s hybrid actions.

To better comprehend the created situation, it is necessary to examine the Russian hybrid actions agains the Republic of Moldova. Currently, to ensure its influence in the region, including in the Republic of Moldova, Russia employs a range of tools, such as gaining favorable public opinion; leveraging the separatist regime and its military potential, including the illegal stationing of Russian troops on the left bank of the Dniester; exploiting the Russian ammunition depot in Cobasna; manipulating the frozen Dniester conflict and the Peacekeeping Forces format; utilizing economic and energy levers; financing and supporting political forces, NGOs and mass-media structures; spreading propaganda, disinformation, and manipulation, etc.

Additionally, to achieve its geopolitical and geostrategic objectives, Russia exploits the vulnerabilities of the Republic of Moldova political, security, administrative, informational, and economic systems. Equally effective for the Russian federation strategy of maintaining influence in Moldova are vulnerabilities in the electoral system, regional issues, linguistic and legislative challenges, and problems on the energy sector and trade relations, particularly concerning the export of local products (Rusia va căuta vulnerabilități). More than 30 years after gaining independence, the Republic of Moldova continues to face constant threats. Although the military phase of the Dniester war ceased in 1992, the conflict persists in the region through other forms characteristic of hybrid warfare (M. Sandu).

Analyzing the specifics of hybrid warfare, L. Grigore argues that, to achieve its interests through hybrid threats, an aggressor state uses a wide range of methods. Typically, the aggressor seeks corrupt or corruptible individuals who, through blackmail and bribery, will advance its interests. These individuals receive material and financial support to attract new members, potentially leading to the creation of favorable political formations that, when needed, will serve the aggressor's interests. Importantly, not only are the parties and politicians of the target state affected, but also those in allied or potentially allied states. Corruption is often closely linked to the political class. The presence of corruption in a state makes it vulnerable and allows the adversary to intervene in the command system, political matters, and economic affairs. The goal of hybrid warfare is not only to infiltrate favorable individuals through corruption, capable of executing orders as situations evolve, but also to create significant governance issues that render the state incapable of responding effectively in the event of armed conflict. Therefore, maintaining corruption within state institutions and in related domains is a primary objective of aggressor states.

The population of the opposing state is the most important target in a hybrid war. It no longer needs to be conquered and administered; instead, it must become favorable to the adversary. To achieve this, through specific means and techniques of manipulation and mass control, the population is subjected to an intense and subtle process of influence aimed at: promoting new values that oppose national identity and traditions, aligning with those of the aggressor state; introducing a new culture (without it being perceived as an act of aggression) that advances the interests of the aggressor state; offering new interpretations of religious precepts that contradict those of the majority, leading to population division in such a way that allows manipulation from both directions; and implementing controlled deprivation of certain material and spiritual needs. The ultimate goal of these strategies is to divide and confuse the population while justifying Russia’s unacceptable behavior (Ambasadorul Regatului Unit).

Once the objective of total or partial control over the adversary's population is achieved, specific military actions can be planned. Military action in a hybrid war is carried out by a "covert" army. Such action is initiated when the objectives of other forms of influence have been or are close to being achieved, with the aim of neutralizing the adversary armed forces and consolidating the gains made up to that point. The covert army has the following characteristics: the soldiers within these forces belong to a military structure not recognized by the aggressor state or any other state in the world; the ideals for which this army fights align with those of the aggressor state, but the declared purpose is merely a facade; financial, material, and logistical support is provided by the aggressor state, albeit indirectly, through national, transnational, or international non-governmental organizations or secret societies; although militarily trained and organized, these armed forces do not bear the distinctive insignia of any state and generally do not adhere to agreements and treaties regulating the laws of war; terrorist actions, although not characteristic of this covert army, can be used, if necessary, in the form of sabotage on the land, air or naval communications system or to strike the command and control system of the opposing state's army; traditional forms of military action, such as defense and offense, manifest through specific operational methods that combine conventional and guerrilla tactics. The military actions of the covert army have a pulsating and discontinuous spatiotemporal character, seamlessly intertwined with cyber, diplomatic, and economic operations; covert armed forces can also engage in non-warfare activities, such as stability and support operations, without a mandate from an international peacekeeping organization, with the aim of gaining the sympathy and support of the population in the conflict zone. Conversely, if the majority of the population is hostile to the aggressor, this scenario cannot be considered a hybrid war but rather a conventional war (Grigore, 2015).

Therefore, all these actions analyzed by L. Grigore are also relevant to the case of the Republic of Moldova. The propaganda and disinformation narratives used by the Russian Federation in the information space have fragmented the population, fostered distrust in state institutions, and left the country vulnerable in pursuing its strategic objectives of development and European integration. In analyzing the hybrid threats facing the Republic of Moldova, we can identify both permanent, historical threats - dating back to the early steps of Moldova's independence - and variable threats that emerge in specific situations or periods. These variable threats aim to undermine or discredit certain political decisions of the state in its course of internal or external development, create a favorable environment for promoting or defending the aggressor interests and political forces representing those interests, and transform the local exchange or bargaining platform into aspects of geopolitical interest.

For the Russian Federation, the range of topics and mechanisms of hybrid warfare that can be exploited to promote threats and destabilize society is broad. For example, in March 2022, amid the war in Ukraine, the Russian Embassy in Chișinău once again resorted to the issues of language and ethnicity. It urged "Russian citizens and Russian compatriots" to seek assistance from the embassy regarding what it described as a "growing number of cases of discrimination based on national, linguistic, cultural, religious, and other grounds, as well as acts of violence or threats to life and health." According to the provisions of the Russian Federation Foreign Policy Concept of March 31, 2023 (Lebedeva & Bobrov, 2023), the primary objectives of Russia include ensuring the rights of Russian citizens and organizations abroad, supporting compatriots, combating Russophobia, strengthening the position of the Russian language globally, fighting for historical truth, and protecting Russian culture (Putin utverdil obnovlenuiu Conțepțiu vneșnei politiki RF). When comparing the reasons cited by the Russian leadership for initiating the war in Ukraine with the actions taken by Russia in March 2022 in the Republic of Moldova, certain similarities can be identified. When invading Ukraine, President Vladimir Putin justified his actions by arguing that "a modern Ukraine, aligned with the West, represents a constant threat, and Russia cannot feel 'safe, develop, and exist' under such conditions." Consequently, the Kremlin leader’s initial goal was to change the current government and halt its foreign policy orientation toward the Euro-Atlantic space. Additionally, another pretext invoked by the Kremlin leader concerned Russian intention to demilitarize and denazify Ukraine to "protect" the pro-Russian population from "eight years of aggression and genocide" (Crăișor – Constantin, 2023:21).

In response to the statements made by President Putin, as well as to the appeal from the Russian Federation embassy in March 2022, President Maia Sandu stated that “regardless of the language spoken, whether Romanian or Russian, all citizens of the Republic of Moldova are safe,” emphasizing that the leadership in Chișinău is making every effort to ensure the safety of the country’s citizens. Since the early days of the war, in order to maintain public order, the country’s leadership has called for unity and for the prohibition of hate speech that could have divided the nation (Președinta Maia Sandu).

In reply to the statements made by Russian diplomatic representatives, the Ministry of Foreign Affairs and European Integration (MFAEI) requested the Russian embassy to refrain from actions that could contribute to escalating tensions within Moldovan society and to demonstrate more appropriate conduct. Additionally, according to MFAEI officials, the Republic of Moldova guarantees the rights of all residents and serves as a model in the region for the peaceful and safe coexistence of citizens, regardless of their ethnic background. Chișinău officials also provided assurances that, under no circumstances, have there been recorded cases of discrimination, particularly on ethnic grounds, and that the Republic of Moldova, in its treatment of its citizens, adheres to international legislation on preventing discrimination (MAEIE despre mesajul Ambasadei ruse la Chișinău).

In this context, it is noteworthy that Russian-speaking citizens or those of other ethnicities did not respond to the provocative message of the Russian Federation Embassy in Chișinău, and Russia lacked legitimate reasons to resort to any hybrid destructive actions. Moreover, the topic of ethnic affiliation (specifically Russian) and the spoken language does not represent a significant advantage for Russia, as Russian-speaking citizens do not constitute a critical mass in the Republic of Moldova. At the same time, the fact that 14.5% of Moldovan citizens use Russian in daily communication (Recensămîntul populației din 2014), and that the majority of residents understand the language, makes Moldova vulnerable to propaganda, manipulation, and misinformation directly originating from Kremlin media sources or from official institutions, such as statements from the Information and Press Department of the Ministry of Foreign Affairs of the Russian Federation (Declarația purtătoarei de cuvînt a MAE Federației Ruse).

The invocation of the violation of the right to use the Russian language by Russian-speaking citizens in the Republic of Moldova (Ruskii iazîk v prițele mirovoi ghibridnoi voinî) can also be considered an element of hybrid warfare. A new attempt to use the language issue as a tool in the information war, this time on the left bank of the Dniester, involved the scenario of organizing a conference dedicated to the Russian language in Tiraspol in September 2023. Based on a risk analysis and information obtained from the Intelligence and Security Service, as well as from international partners, a group of individuals, alleged scholars from the Russian Federation and Central Asia, were denied entry to the Republic of Moldova (Precizările Poliției de Frontieră). Thus, in light of the failure of threats to use the language as a destabilizing factor, the Russian Federation is likely to shift its tactics to destabilize the situation in the Republic of Moldova by employing propaganda, disinformation, and manipulation strategies. To achieve its objectives, Russia will focus not only on ethnic Russians but also on all categories of citizens, particularly Moldovan citizens who either maintain pro-Russian doctrinal views due to the lingering effects of the past, are victims of hostile propaganda and manipulation, or are incentivized to promote Russia's interests in the Republic of Moldova. This tactic was notably employed during the protests organized by the opposition to overthrow the government and seize power.

Considering the Republic of Moldova high dependence on Russian gas, Moscow fully exploited this vulnerability by imposing prices four times higher than in the same period before the war in Ukraine. The resulting situation led to inflation rising by up to 35% and the risk of gas supply cuts during the winter in Moldova. To further destabilize the country, the Kremlin coordinated prolonged anti-government protests from October to November 2022. The goal of these actions was to remove the current leadership and replace the pro-Western President Maia Sandu with individuals loyal to Moscow (ibid., 51).

Additionally, to strengthen its forces, to organize and conduct psychological and informational operations against political elites and the population, the Russian Federation employs pro-Russian platforms, including media outlets, fake news dissemination tools (such as Telegram channels and TikTok accounts), political parties, civic movements, non-governmental organizations, politicians, propagandists, political and civic activists, journalists, and influencers. In this regard, the informational space remains the primary arena of hybrid warfare (Război hibrid).

In this context, the most widespread false narratives promoted on these platforms include: European democracy has failed; NATO and/or the European Union are weak and unable to effectively resist Russia; NATO is an aggressor organization, creating a pretext for a world war; NATO and Romania are "invading" the Republic of Moldova; Europe is a military and political colony of the

United States; NATO provoked Russia and triggered the war in Ukraine; Brussels has approved the annexation of the Republic of Moldova by Romania; neutrality is what protects us; we do not need the National Army, nor relations with NATO or other international organizations; a closer relationship between Chișinău and NATO would mean the loss of Moldova’s sovereignty; mobilization exercises, combat training, and the modernization of the National Army are preparations for a military attack on Transnistria; the Republic of Moldova is preparing to mobilize its population and attack Transnistria together with Romania; the rights of Russian-speaking citizens residing in Moldova are being violated; the United States is constructing military facilities in Moldova; NATO is building a military base in Moldova; the Republic of Moldova has allegedly decided to allow F-16 fighter jets to be stationed at Mărculești (Site de combatere a știrilor false).

In the practice of international relations, as well as in the realities we are currently witnessing, it is important to note that informational warfare exerts a complex influence (through the entirety of informational operations) on the political and military governance system of the adversary. This influence extends to the political-military leadership of the target state, enabling the adoption of decisions favorable to the aggressor even in peacetime and potentially paralyzing the leadership and resistance infrastructure of the adversary during a conflict (Kuzimovici). The primary objective of this warfare is not necessarily the physical destruction of the adversary but rather its demoralization and the reduction of its capacity to resist the initiating aggressor. The targets of attack and disruption in an informational war include: the consciousness, will, and emotions of the population in the enemy state, particularly during elections, referendums, and crises; decision-making systems in the political, economic, social, scientific, and technological spheres, as well as in security and defense domains; the informational infrastructure of the adversarial state; the ultimate goal of informational warfare is to influence the enemy's knowledge and value systems. Additionally, it is characterized by the conflicting parties desire to create panic in hostile states, fostering a continuous atmosphere of crisis and tension (Magda, 2017: 114-120).

Another manifestation of hybrid warfare involves supporting and financing criminal groups, including politicians with pro-Russian views. In this context, the presidential elections in the Republic of Moldova in October 2024 are particularly noteworthy. The first round of the presidential elections, held on October 20, 2024, coincided with the referendum on the Republic of Moldova accession to the European Union, while the second round took place on November 3, 2024. These elections represent a historic event that marked the country destiny, emerging as a decisive turning point for Moldova’s future, including its aspirations to join the European integration space. Furthermore, the 2024 presidential elections were marked by foreign interference in the Republic of Moldova internal affairs. The elections witnessed significant Russian interference in the electoral process. Despite the provisions of the United Nations Charter and the principles of international law, which affirm that every state has the right to determine its own destiny without external intervention, we are currently observing numerous international events where this principle is violated. The Republic of Moldova is no exception to this phenomenon, and the 2024 presidential elections serve as a clear example of such violations.

When correlating the principle of non-interference in the internal affairs of a state with the 2024 presidential elections in the Republic of Moldova, it is important to note that these elections took place within a highly tense geopolitical context. The proximity of an active war near Moldova's borders generated a multitude of threats to national security (Alegerile și Referendumul din Republica Moldova). Following the Republic of Moldova attainment of EU candidate status in June 2022 and the initiation of accession negotiations in June 2024, the political rhetoric regarding the country geopolitical orientation intensified, leading to increased foreign interference. Since February 2022, amid the war triggered by the Russian Federation invasion of Ukraine, political discourse surrounding Moldova’s geopolitical direction has become more pronounced. The government publicly announced that the Republic of Moldova is the target of a "hybrid war" orchestrated from abroad. Authorities warned that the country had been subjected to various forms of manipulative interference aimed at destabilization, including illicit financing of political actors, disinformation campaigns, and cyberattacks. Opposition voices criticized the countermeasures, including the suspension of several media outlets, as excessively restrictive (Misiunea de observare a alegerilor).

Despite the large-scale Russian aggression against Ukraine and the intense Kremlin interference in electoral processes, the 2024 presidential elections represented a pivotal moment for the Republic of Moldova, according to Petra Bayr, Head of the Delegation from the Parliamentary Assembly of the Council of Europe. The elections held on October 20, 2024, are emerging as a decisive turning point for the country's future. This vote was not merely about determining who would govern Moldova but had the potential to define the nation's European trajectory. However, this historic opportunity was threatened by a wave of Russian disinformation and other hybrid attacks that could have compromised the vote. Less than a month before the presidential elections, the Republic of Moldova national security adviser warned that Russia had launched an unprecedented hybrid attack aimed at obstructing any progress toward European integration.

Had the integrity of the electoral process not been preserved, the Republic of Moldova could have missed the opportunity to join the European Union (EU) due to Russian interference. One of the main misleading narratives promoted by pro-Russian media focused on the claim that Moldova's constitutional referendum was, in fact, a covert attempt to abolish the principle of the Republic of Moldova neutrality by replacing it in the Constitution with the objective of EU accession. This, in turn, would pave the way for NATO integration, thereby endangering the country security.

The Russian threat to Moldova's elections and state institutions, in general, should not be underestimated. The presence of pro-Russian oligarchs in the Republic of Moldova exerts considerable influence over the country, dominating its economic, political, and public life. Additionally, Moldova faces the challenge of the separatist Transnistrian region, closely linked to Russia, where Russian troops are stationed. Despite limited human and financial resources, Moldova has managed to implement several key reforms to strengthen its democratic institutions against external interference. However, the fight against corruption within the judiciary remains a significant challenge. To reform the judicial system—an essential condition for EU accession—the government established a vetting process in which judges and prosecutors are assessed based on their ethical and financial integrity. It is alleged that some judges, who are sympathetic to the Russian Federation, attempted to disrupt the electoral process, knowing that their backgrounds could disqualify them in this evaluation, stripping them of power and professional prospects in a reformed state.

The integrity of the electoral process also heavily depends on media regulation. Moldova's media landscape is characterized by a high concentration of ownership among a few groups, often affiliated with pro-Russian interests. The European Commission reported media concentration among groups associated with fugitive oligarchs and linked to the Russian state media group RTR. Consequently, between 2022 and 2023, following recommendations from Moldova intelligence services, television channels primarily broadcasting Russian content were suspended. These channels were allegedly controlled by internationally sanctioned individuals and provided inaccurate coverage of the war in Ukraine. The suspensions were enacted in light of evidence showing that Russia used these channels to undermine the democratic process through disinformation campaigns. In September 2024, Moldova took additional steps by banning five Russian state media outlets.

The Constitutional Court of the Republic of Moldova recently obstructed executive attempts to regulate the media and ensure impartial coverage of electoral campaigns. The contested provision limited candidates appearances on audiovisual programs not specifically related to elections, as explicitly defined in the media editorial policies. This measure aimed to restrict discussions of electoral issues to specific programs listed by the media and monitored by the Audiovisual Council. In July 2024, the court declared this provision unconstitutional, finding that it imposed an excessive restriction on press freedom (Maréchal).

Another instance indicating foreign involvement in the internal affairs of the Republic of Moldova, and highlighting the presence of hybrid warfare elements in the country, relates to the funding of pro-Russian criminal groups. It has been established that the highest concentration of illicit funds sent by Russia through the Șor criminal group to influence Moldova's elections is in the Gagauz Autonomous Region (in the south) and Bălți, according to estimates by Moldovan authorities. The effort to undermine Moldova referendum cost the Russian Federation over 100 million euros. These funds were allocated to disinformation and societal destabilization activities, as well as vote-buying through direct payments to voters. In early October 2024, Moldovan security forces dismantled a scheme involving the bribery of approximately 130,000 individuals (equivalent to 5% of Moldova population) via electronic cards to boycott the referendum on October 20, which coincided with the presidential elections. According to estimates by authorities in Chișinău, this financial operation cost the Russian Federation and the Șor group over 15 million euros.

Sentenced in 2023 for banking fraud after embezzling nearly one billion dollars from three national banks, Șor is considered a key figure in organizing Russia’s destabilization maneuvers. On the social media platform Telegram, he regularly criticizes the Moldovan “police state,” which he describes as a “subservient puppet” of the West. His political party, also bearing his name, was banned in 2023 (Barnaud).

The Intelligence and Security Service (SIS) of the Republic of Moldova has collected and analyzed data indicating an unprecedented intensity of actions undertaken by the Russian Federation aimed at anchoring Moldova within its sphere of influence. The hybrid mechanism employed primarily targets democratic processes and seeks to undermine the country’s European integration trajectory. Based on operational data collected, verified, and systematized by SIS, it has been demonstrated that the Russian Federation maintains the strategic objective of drawing Moldova into its influence zone. In this context, the tactical objectives pursued over the next two years are as follows:

For 2024 - undermining the referendum on European integration, interfering in the presidential elections, and discrediting political candidates associated with the pro-European agenda.

For 2025 - ensuring the entry of political parties under Russian influence into the Moldovan Parliament, with the goal of establishing a pro-Russian majority or, at the very least, moderating the country's stance toward European integration.

The data points to a strategy for 2024–2025 that includes three main, interrelated components: support for political actors under direct or indirect control of the Russian Federation; openly pro-Russian political actors. These individuals or groups maintain direct and verified connections with Russian special services, political consultants, organized criminal groups, the Kremlin presidential administration, and oligarchic networks.

In 2024, the Russian Federation influence operations focused on the following directions:

1) Discrediting the European Integration Referendum. The strategy involved creating conditions to reduce voter turnout and/or undermine the legitimacy of the referendum itself. According to assessments, the Russian side aimed to promote options such as a "boycott," "voting against," and/or introducing a referendum question, or disseminating information, that would associate European integration with joining military alliances and blocs. Additionally, plans were made to amplify narratives in the information space suggesting that "European integration for the Republic of

Moldova is equivalent to losing neutrality and reigniting the Transnistrian military conflict."

2) Undermining Pro-European Candidates in the 2024 Presidential and 2025 Parliamentary Elections. The objective was to diminish the prospects of pro-European candidates while promoting a more favorable candidate (either someone directly controlled by the Kremlin regime or an individual with moderately anti-Russian views, with whom "negotiations could later be possible").

Elements of hybrid influence from the Russian Federation are rooted in interference in the internal affairs of the Republic of Moldova through the involvement of political actors, associative structures/pro-Russian influence groups, information-analytical companies connected to Russian interests, as well as distinct groups of citizens clandestinely funded by external subversive centers. Given the current situation, the main driving force, inclined toward measures that could provoke radicalization and violence, is I. Șor group through its socio-political extensions. The primary objective assigned to this group for 2024 was to undermine the results of the referendum.

Furthermore, certain data indicate attempts by the Russian Federation to revive the "sovereignist/statist" doctrine in the Republic of Moldova. The so-called "statist" groups have focused their rhetoric on populist principles and purportedly patriotic-nationalist approaches—emphasizing sovereignty, neutrality, and the principle of "self-reliance." Additionally, some of the entities connected to this doctrine received direct and/or indirect financial support from the "ȘOR" group, with their members displaying overtly pro-Russian views. There is a high probability that these structures are guided by Russian intelligence services or influence centers linked to the Kremlin Presidential Administration, disseminating the strategic narratives promoted by the Russian Federation regarding the Republic of Moldova. In this context, evidence of Russian interference in Moldova’s internal affairs has been investigated, including through the lens of reviving "fifth column" elements, masked under the guise of "national sovereign interest." Moreover, in the context of the presidential elections, there emerged signs of potential coalition-building under the auspices of the Russian Federation. This coalition could involve the aforementioned forces alongside other statist groups, aiming to promote speculations regarding the "erosion of sovereignty through EU integration" (Evaluarea implicării Federației Ruse).

During the presidential election and the referendum on European Union membership in October 2024, attempts at interference were detected. On October 17, the police announced the identification of a network of approximately one hundred individuals suspected of being trained to incite unrest in the country during the elections scheduled for October 20. As a result of the police operational actions, several suspects were arrested - primarily young individuals around twenty years old, who were allegedly sent to Russia, Serbia, and Bosnia and Herzegovina for training aimed at disrupting the vote (Géopolitique). As highlighted by the European Parliament, authorities uncovered a "large-scale electoral fraud scheme, financed by the oligarch I. Shor, involving the transfer of 15 million dollars to 130,000 Moldovans" through bank accounts opened in the Russian Federation.

According to the police, as reported by Moldovan media, approximately 130 individuals were responsible for coordinating these corrupt activities, while another 2,000 were tasked with recruiting candidates to support a "no" vote in the referendum and a positive vote for the pro-Russian candidate. Over 50,000 members of the network were able to collect data from around 70,000 voters. All participants were allegedly paid for their actions, with compensation ranging from 200 lei to 11,000 lei (10 to 560 euros). The primary suspect in organizing this democratic process sabotage scheme is I. Shor, who, in September 2024, promised via his Telegram channel to pay remuneration to all those who would vote against the European referendum. A video cited by CNN illustrates this, with Shor stating, "If you do well and most people in your area vote against, the bonus you will personally receive from me on your card will be 5,000 lei," or approximately 260 euros, serving as evidence of these offenses.

Among the evidence seized by the police during the investigation were large sums of money as well as tens of thousands of leaflets promoting a "no" vote, as documented by Sky News in a live broadcast from a warehouse in Chișinău. "Here you can see huge piles of posters or leaflets that were allegedly distributed, bearing the message 'vote no in the referendum.' On one side are the Russians, on the other side the Moldovans," reported the channel. "Over 100 young people participated in such training sessions in June, under the pretext of attending a cultural and tourism program," authorities detailed, describing a series of trainings that included "tactics for destabilizing constitutional order." Further evidence of the Russian Federation interference in the 2024 Moldovan presidential elections includes the arrest, on June 11, 2024, by Moldovan police of passengers arriving by plane from Moscow.

Some of the instructors were reportedly linked to Wagner, the Russian paramilitary group that has been in decline since the death of its leader in a plane crash in August 2023. Other individuals, including Moldovan citizens, were trained in Bosnia and Herzegovina and Serbia, where they underwent more extensive preparation from early September until mid-October. The investigation revealed a massive vote-buying scheme, involving tens of thousands of Moldovans being paid to cast anti-Sandu and anti-EU ballots. According to police chief V. Cernăuteanu, the scale and complexity of this mechanism make these actions by the Russian Federation "an unprecedented phenomenon". An observation corroborated by a study from the New Strategy Center, based in Romania states that between disinformation campaigns and a massive vote-buying system, "Russian interference has reached an unprecedented level" (La présidente sortante). According to data from the Information and Security Service of Chișinău, among the coordinators of the group's actions in Moldova are foreign nationals Konstantin Goloskokov and Mikhail Potepkin - the latter being subject to international sanctions. Potepkin is known for his connections to "Wagner" and the Russian organization "Ferma," both involved in financing and organizing the 2023 destabilization actions in Moldova (Călugăreanu).

This is not the first time Moldova has been targeted by destabilization attempts from the East. During the local elections in December 2023, "disinformation narratives such as 'Russophobia imposed by the West' circulated throughout the country via Facebook," confirms the independent platform Open Global Rights. Fake pages were created as early as July through Facebook advertising network to promote pro-Russian interests and figures, such as Ilan Shor, according to data from the NGO Reset reported by Le Monde. Deepfake videos targeting President M. Sandu also circulated. According to Reset, the total cost of this operation was estimated at between 198,000 and 280,000 euros (Quevrain, 2024). The day after the October 20 referendum, the Kremlin immediately denounced "irregularities" in the vote-counting process, and Russian media quickly began reporting on the "manipulation" of the vote (ibidem).

Members of the European Parliament emphasize the role played by a multitude of malicious actors, including pro-Russian Moldovan oligarchs and the Russian-funded RT network, in executing electoral fraud, conducting cyber operations, and engaging in information warfare. They also call on the EU and its member states to ensure that all necessary assistance is provided to Moldova to strengthen its institutional mechanisms and capacity to respond to hybrid threats. Destabilizing actions orchestrated by Russia in Moldova continued. The second round of the presidential elections on November 3, 2024, took place amid allegations of foreign interference, vote-buying, and voter intimidation. Additionally, according to data from the Moldovan Police, "reasonable evidence" was found concerning the organized and illegal transportation of voters to polling stations both within the country and from abroad. According to official statements from Moldovan police officials, activities were also identified involving "air transport from Russia to Belarus, Azerbaijan, and Turkey" of individuals intended to destabilize the situation in the Republic of Moldova (Acuzații de cumpărare de voturi).

According to Moldova's Deputy Prime Minister for European Integration, Cristina Gherasimov, Moldova has become a testing ground for Russia new subversive methods, stating that "whatever works in Moldova will subsequently be used in other countries." She warned of unprecedented Kremlin attempts to undermine democratic institutions, including through the use of weapons, explosives, and drones. According to C. Gherasimov, the Russian Federation goal is to prevent the Republic of Moldova from joining the European Union. The spokesperson for the U.S. National Security Council, John Kirby also spoke out regarding Russian interference in Moldovan presidential elections. Kirby stated that "Russia is attempting to undermine the presidential elections in the Republic of Moldova and has spent millions of dollars to do so." This perspective is echoed by European Council President Charles Michel, who warned in a letter to the 27 European leaders that "the Republic of Moldova is facing crucial moments on its European path." On October 17, 2024, the EU Council condemned Russian interference in Moldovan electoral process. Peter Stano, spokesperson for the European Commission, similarly noted that the election took place amid "unprecedented interference and intimidation from Russia (...) aimed at destabilizing the democratic process in the Republic of Moldova" (Moldavie : l'UE).

NATO Secretary General Mark Rutte also reacted to Russian interference in Moldovan presidential elections. According to Rutte, Russia is trying to divert the European trajectory of the Republic of Moldova. He welcomed the leadership of Maia Sandu and stated that through her actions, she is striving to build a stable democracy in Moldova, capable of protecting itself, particularly against "Russian hybrid interference" (Călugăreanu). In this context, the statements made by Polish Prime Minister Donald Tusk also deserve attention, as he welcomed the Republic of Moldova positive vote on EU membership. “She angers Moscow, impresses Europe, and once again saves her country—that is Maia Sandu.” European Commission President Ursula von der Leyen similarly praised Moldova vote in favor of joining the EU, despite Russian “hybrid strategies.” “[…] Moldova is showing that it is independent, strong, and committed to a European future,” von der Leyen wrote on social media. She highlighted that “Maia Sandu, who turned her back on Moscow following the invasion of Ukraine and brought her country candidacy to Brussels, called the referendum to validate her strategy and to determine the destiny of this former Soviet republic of 2.6 million inhabitants.” (Moldavie: l’UE).

In light of the numerous accusations of the Russian Federation interference in Moldovan presidential elections, Russian presidential spokesperson Dmitry Peskov demanded "proof" regarding the "serious accusations" made by Moldova pro-European president. Peskov argued that "it is difficult to explain the increase in votes for M. Sandu and EU membership." He added, "Anyone familiar with electoral processes can detect anomalies in the rise of these votes." To defend his position, Peskov further criticized the elections in Moldova as an "unfree electoral campaign" and claimed that Moscow sees "how many people do not support the ideology of the incumbent president actions."

4. CONCLUSIONS

In the context of the war in Ukraine, as well as in the context of obtaining the status of a candidate country for joining the European integration space, the Republic of Moldova faces a multitude of hybrid threats from the Russian Federation. Approximately 35 years after the collapse of the Soviet Union, the Russian Federation continues to strive to maintain influence over former Soviet republics. To achieve its geostrategic and geopolitical objectives, Russia employs a range of hybrid warfare tactics, including disinformation, manipulation, the dissemination of fake news, the financing of criminal groups and political actors, as well as the sponsorship of political parties.

The Republic of Moldova is facing an avalanche of disinformation and fake news. The Kremlin utilizes various strategies, including disinformation and hybrid aggression, to undermine the credibility of Moldovan institutions. Throughout the year, narratives, falsehoods, and disinformation, directly or indirectly related to Moldova, have been disseminated in the public sphere. Moldova efforts toward European integration and its collaboration with NATO to enhance national defense and security have made Russian propaganda, as a component of hybrid warfare, a significant national security concern. The primary goals of Russian propaganda, disinformation, and manipulation are to alter Moldova foreign policy direction, maintain its economic and energy dependence on Russia, and replace the current government with political entities loyal to Moscow. Furthermore, as Moldova is in an election year (parliamentary elections), Russia is attempting to destabilize the country by promoting numerous false narratives regarding Chișinău actions and stance on the country eastern regions. To prevent cyberattacks and anticipate the spread of fake news in the public sphere and on social media, it is crucial to involve IT specialists who can develop programs to identify, block, and preempt the dissemination of misinformation. Additionally, Moldovan institutions must be equipped with modern IT technology. Despite the establishment of two new institutions - the National Cybersecurity Agency and the National Institute for Innovations in Cybersecurity, "Cybercor," tasked with identifying and preventing cyberattacks, Moldovan authorities must expedite the adoption of the Digital Security Law and create a national-level authority to counteract cyber threats.

To reduce the influence of the Russian Federation, particularly in addressing elements of Russian hybrid warfare and enhancing national security, the Republic of Moldova should strengthen its cooperation with European countries, including its neighbors, Romania and Ukraine.

REFERENCES

[1] Acuzații de cumpărare de voturi și interferență a Rusiei. https://romania.europalibera.org/a/maia-sandu-alegeri-moldova/33186376.html

[2] Alegerile și Referendumul din Republica Moldova, Considerate Eficiente și Competitive de către Observatorii Internaționali, în Ciuda Tentativelor de Subminare a Integrității. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.oscepa.org/en/documents/election-o

[3] Ambasadorul Regatului Unit: Susținem cu fermitate capabilitățile Republicii Moldova de a rezista la amenințările rusești. În: https://moldova1.md/p/23651/ambasadorul-regatului-unit-sustinem-cu-fermitate-capabilitatile-republicii-moldova-de-a-rezista-la-amenintarile-rusesti

[4] Timothée, B. Moldavie : ces ingérences russes "sans précédent" pour perturber des élections cruciales

Europe. Moscou a investi des millions de dollars dans des opérations de corruption et de désinformation en Moldavie, où se tient ce dimanche l'élection présidentielle et un référendum sur l'adhésion à l'UE. https://www.lexpress.fr/monde/moldavie-ces-ingerences-russes-sans-precedent-pour-perturber-des-elections-cruciales-PAH63HGS3RD4TGDYRV4GB2FCMQ/

[5] Graefrath, B.. Ingérence et droit international , p. 17-32. https://books.openedition.org/iheid/2927

[6] Bizeau, M. Le principe de non-ingérence en droit international. https://fiches-droit.com/principe-de-non-ingerence#:~:text=Un%20autre%20exemple%20de%20violation,secrets%20fran%C3%A7ais%20en%20Nouvelle%2DZ%C3%A9lande

[7] Carta Natiunilor Unite*) din 26 iunie 1945 Emitent: Organizatia Natiunilor Unite publicat in: Monitorul Oficial din 26 iunie 1945 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.anr.gov.ro/docs/legislatie/internationala/Carta_Organizatiei_Natiunilor_Unite_ONU_.pdf

[8] Călugăreanu, V. Alertă sporită în ajunul alegerilor din Moldova. https://www.dw.com/ro/alert%C4%83-sporit%C4%83-%C3%AEn-ajunul-alegerilor-din-moldova/a-70541679

[9] Conțu, M. *Una-i să obții statutul de candidat la aderare în UE, alta-i să-l și păstrezi*. Moldova Suverană, 19 iulie, 2022, p.1,3.

[10] Crăișor – Constantin, I. Convențional și hibrid în primul an al războiului Federației Ruse împotriva Ucrainei. Concluzii și lecții desprinse din război. Bucureşti : Editura Universităţii Naţionale de Apărare "Carol I", 2023, p.21

[11] Declarația purtătoarei de cuvînt a MAE Federației Ruse. https://stopfals.md/ro/article/fals-regimul-maia-sandu-impune-cetatenilor-republicii-moldova-unirea-cu-romania-180883

[12] Evaluarea implicării Federației Ruse în procesele electorale din Republica Moldova în 2024-2025. Serviciul de Informaţii şi Securitate al Republicii Moldova. *chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://sis.md/sites/default/files/comunicate/fisiere/Scenarii%20de%20influen%C8%9B%C4%83%202024-2025.pdf*

[13] Géopolitique. La Moldavie affirme avoir arrêté des perturbateurs prorusses juste avant les élections. https://www.courrierinternational.com/article/geopolitique-la-moldavie-affirme-avoir-arrete-des-perturbateurs-prorusses-juste-avant-les-elections_223571

[14] Gherasimov, V. Țennosti nauki v predvidenii. Валерий Герасимов, Ценность науки в предвидениии, https://aillarionov.livejournal.com/704238.html

[15] Grigore, L. Viitorul războiului – războiul hibrid, Buletinul Universității Naționale de Apărare „Carol I" Vol. 2 No. 2 (2015) . https://revista. unap.ro /index. php/ revista /article/ view/135/145

[16]Fiodorov Iu. „ Ghibridnaia voina po ruski", Kiev:TOV „Biznespoligraf", 2016, 176 p. . Фёдоров Ю. Гибридная

война по-русски. Киев: ТОВ «Бизнесполиграф», 2016. 176 с.

[17] Ingérence, droit d'ingérence. https://geoconfluences.ens-lyon.fr/glossaire/ingerence-et-securite

[18] La présidente sortante pro-UE remporte l'élection présidentielle moldave. https://www.rts.ch/info/monde/2024/article/la-presidente-sortante-pro-ue-remporte-l-election-presidentielle-moldave-28682777.html

[19] Moldavie : l’UE dénonce « l’interférence sans précédent » de la Russie, après la victoire étriquée du oui au référendum. https://www.lemonde.fr/international/article/2024/10/21/moldavie-le-non-a-l-adhesion-du-pays-a-l-ue-pointe-en-tete-la-presidente-sandu-denonce-une-attaque-sans-precedent-contre-la-democratie_6357047_3210.html

[20] MAEIE despre mesajul Ambasadei ruse la Chișinău. În: https://www.jurnal.md/ro/news/8c360395a6711b67/ maeie-despre-mesajul-ambasadei-rusiei-la-chisinau-in-rm-nu-au-fost-inregistrate-cazuri-de-discriminare.html

[21] Kuzimovici A. Evoliuția vzgleadov na teoriu sovremenoi voinî. (Кузьмович А, Эволюция взглядов на теорию современной войны), https://cyberleninka.ru/article/n/evolyutsiya-vzglyadov-na-teoriyu-sovremennoy-voyny

[22] Lebedeva O., Bobrov, A. (2023).Konțepția vneșnei politiki Rossii 2023: strateghia monopolearnogo mira. Лебедева Ольга Бобров Александр. Концепция внешней политики России 2023: стратегия многополярного мира. 2 мая 2023. https://russiancouncil.ru/analytics-and-comeents/analytics/kontseptsiya-vneshney-politiki-rossii-2023-strategiya-mnogopolyarnogo-mira/

[23] Magda E. Ghibridnaia agresia Rossii: urochi dlea Evropî. (Магда Евгений, Гибридная агрессия России: уроки для Европы, К.: „КАЛАМАР”, 2017, pp.114-120.

[24] Maréchal A. Elections en Moldavie : comment limiter l’influence russe ? https://prospective-innovation.org/moldavie-integrite-elections-2024-ingerence-russe-adhesion-ue/

[25] M. Geoană, Secretar general adjunct NATO, https://www.ziarulnational.md/geoana-despre-un-eventual-pericol-ca-rusia-sa-atace-r-moldova-militar-nu-are-motive-de-ingriorare-un-razboi-hibrid-total-este-de-interes-vital-pentru-rusia-care-prin-cozi-de-topor-din-r-moldova-vrea-sa-opreasca-drumul-proeuropean-al-chisinaul

[26] M. Sandu, despre decizia de creare a Centrului național de apărare informațională, https://presedinte.md/presa/mesajul-presedintei-maia-sandu-despre-initiativa-de-creare-a-centrului-national-de-aparare-informationala-si-combatere-a-propagandei-patriot

[27] Misiunea de observare a alegerilor. Republica Moldova – Alegerile Prezidențiale și Referendumul Constituțional, 20 octombrie 2024. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.osce.org/files/f/documents/c/b/578857.pdf

[28] Ben Raies, M. La non-ingérence dans les affaires internes de l’état :

Définition Et Fondements. https://www.leaders.com.tn/article/32302-la-non-ingerence-dans-les-affaires-internes-de-l-etat-definition-et-fondements

[29] Presa străină scrie despre miza alegerilor prezidențiale din Moldova. https://www.ipn.md/ro/presa-straina-scrie-despre-miza-alegerilor-prezidentiale-din-moldova-8013_1108691.html

[30] Președinta Maia Sandu dă replica Ambasadei Ruse, https://moldova.europalibera.org/a/pre%C8%99edinta-maia-sandu-d%C4%83-replica-ambasadei-ruse/31757868.html

[31] Putin utverdil obnovlenuiu Conțepțiu vneșnei politiki RF. (Путин утвердил обновлённую Концепцию внешней политики РФ,)https://russian.rt.com/world/article/1130448-putin-koncepciya-vneshnei-politiki-rossiya

[32] Quevrain Caroline. D'ingérences russes dans le référendum européen en Moldavie ? 2024. https://www.tf1info.fr/international/que-sait-on-des-accusations-d-ingerences-russes-dans-le-referendum-en-moldavie-sur-l-adhesion-a-l-union-europeenne-eu-2329747.html

[33] Război hibrid: Metode, tehnici, canale de propagandă și dezinformare ale Federației Ruse în Republica Moldova, https://realitatea.md/doc-razboi-hibrid-metode-tehnici-canale-de-propaganda-si-dezinformare-ale-federatiei-ruse-in-republica-moldova/

[34] Recensământul poulației din 2014. În: https://statistica.gov.md/files/files/Recensamint/Recensamint_pop_2014/Rezultate/Infografic_RPL2014_2.pdf

[35] Rusia va căuta vulnerabilități.https://tvrmoldova.md/article/9d0fc9d2a05f487e/expertul-militar-ucrainean-mykhailo-samus-rusia-va-cauta-vulnerabilitati-oriunde-in-sistemul-politic-si-de-securitate-de-la-chisinau.html?utm_source=RSS&utm_medium= MicroService &utm_campaign=google_analytics

[36] Ruskii iazîk v prițele mirovoi ghibridnoi voinî. (Русский язык в прицеле мировой гибридной войны), https://nvo.ng.ru/concepts/2023-12-21/1_4_5_1267_language.html

[37] Site de combatere a știrilor false. În: https://stopfals.md

[38] Summitul NATO prokladîvat kurs k kraiu bezdnî. (Саммит НАТО прокладывает курс к краю бездны). https://nvo.ng.ru/concepts/2023-06-15/1_1240_summit.html

[39] Ukaz Prezidenta Rossiskoi Federații ot 31.03.2023, nr. 229. Ob utverjdenii Konțepții vneșnei politiki Rossiiskoi Federații ot 31.03.2023. (Указ Президента Российской Федерации от 31.03.2023 г. № 229. Об утверждении Концепции внешней политики Российской Федерации). http://www.kremlin.ru/acts/bank/49090

ENHANCING OPERATIONAL LOGISTICS IN RESPONSE TO UKRAINE WAR IMPACTS: A RELATIONAL ANALYSIS

Gheorghe MINCULETE

Land Forces Academy, Sibiu, Romania

The armed conflict in Ukraine represented a significant test for the efficiency of operational logistics, highlighting both the strengths and vulnerabilities in resource management and the coordination of operations under conditions of uncertainty and instability. The challenges encountered by the forces involved provided valuable lessons about the need for a flexible, rapidly adaptable, and well-integrated logistics system, capable of responding efficiently and coherently to the requirements imposed by the dynamics of a protracted conflict.

The article proposes an analysis focused on improving the functioning of operational logistics in the context of inter-organizational and intra-organizational relations within an area or theater of operations in which NATO operational forces with national and multinational status are engaged. The study examines how logistics structures will have to respond to the challenges and difficulties that may arise in the future in a high-intensity conflict such as the one in Ukraine. In this regard, we have identified key aspects with an impact on operational efficiency. In addition, we have proposed some applicative solutions for optimizing logistics processes, including the implementation of advanced technologies, adaptability, and flexibility in the face of unpredictable situations. The conclusions emphasize the need to implement innovative concepts that would improve operational logistics integrated into the combat structures of NATO states in future conflicts, providing a framework for the development of more efficient and sustainable practices in managing resources in crisis conditions.

Key words: *armed conflict; combat forces; operational logistics; improvement; mobility; sufficient resources; logistics resilience.*

1. INTRODUCTION

The future security environment will be increasingly complex, driven by the impact of new military technologies on the battlefield. The most disruptive technologies are not always the most advanced. Artificial intelligence (AI) and machine learning (ML) are good examples of this lesson, as relatively simple models have enabled the proliferation of inexpensive unmanned weapons systems and improvements in military decision-making [1]. The ongoing challenges to the international regulatory order and the manifestation of long-term strategic competition between the main global actors. Therefore, the future operational environment will be characterized by a modernized infrastructure, complex and dynamic operating methods, integrating technologies, equipment, automated and robotic systems, artificial intelligence, as well as advanced planning and action procedures. Under these conditions, both for NATO and national forces, operational logistics will need to have the capability and protection necessary to provide adequate logistical support to multi-domain, non-linear, and/or expeditionary operations conducted at greater distances, due to the context and complexity of the threats specific to the future confrontation environment [2].

The complication of regional and international security, as a result of Russian aggression in Ukraine, has led NATO bodies to carry out successive decision-making processes to increase the response force, as well as the related operational logistics. The high-intensity armed conflict in the vicinity of NATO's eastern flank (southeastern area) led to the establishment and implementation of measures to deter the aggressor state. To this end, the new NATO force model (New Force Model - NFM) was adopted at the Madrid Summit in 2022. It allowed the Allies to: deploy more forces in Eastern Europe by building eight Battle Groups [3]; agreeing on the implementation of new military training and defense plans; conducting more exercises; significantly improving NATO capabilities in the High North and the Baltic Region, following the accession of Finland and Sweden in 2023 and 2024 respectively to the Alliance; increasing military readiness to increase deterrence and, if necessary, defeat further Russian aggression [4].

At the same time, the NFM has significantly expanded the number of highly trained forces, as well as the follow-up forces available to NATO commanders. Thus, if before 2022, the NATO Response Force had the capacity to deploy approximately 40,000 soldiers at the Allied level in less than 15 days, through the NFM the Alliance intends to achieve the strategic objective (through specific training actions) appropriate to the deployment of over 100,000 soldiers (Level 1 Forces) in a maximum period of ten days [5] (Figure 1).

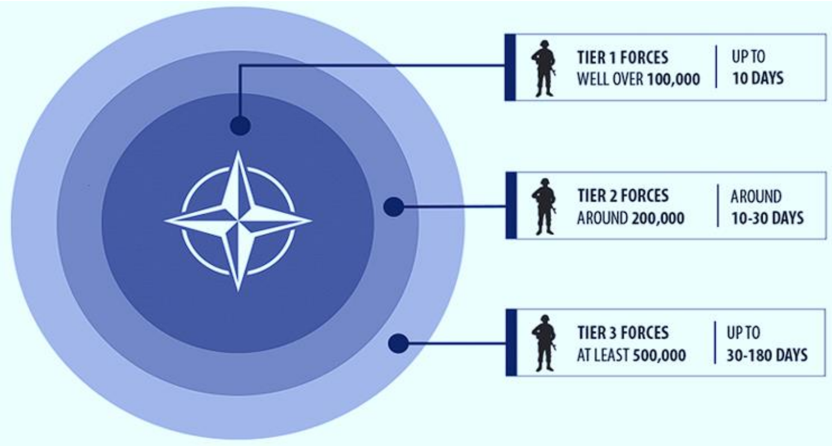


Fig. 1 An image on NATO's New Force Model [4]

The progress made by European NATO member states since February 2022 to date in adapting their forces to face a high-intensity war against Russia is significant. Military analysts believe that these countries need to redirect their efforts to support future actions, with a focus on the ability to fight and sustain operations over the long term. In this context, Alliance states need to intensify their preparation, improve mobility, and eliminate critical gaps in defense capabilities. Also, strengthening the defense industrial base and generating sustainable financial flows are key elements for future success [3].

In this sense, Figure 2 is suggestive, which reveals a conception of the "Iron Triangle" appropriate to NATO's specific deterrence and defense actions, involving the appropriate forces and means, as well as the necessary operational logistical support. We appreciate that, in a high-intensity conflict, for the success of NATO combat and support forces, it is necessary to increase the performance of operational logistics at the joint and tactical levels to provide continuous support for defensive or offensive operations within the allied framework. Moreover, modern operational logistics must adapt quickly to the requirements of a dynamic security environment, characterized by protracted conflicts, with increasing requirements for high mobility and viable and sufficient resources.

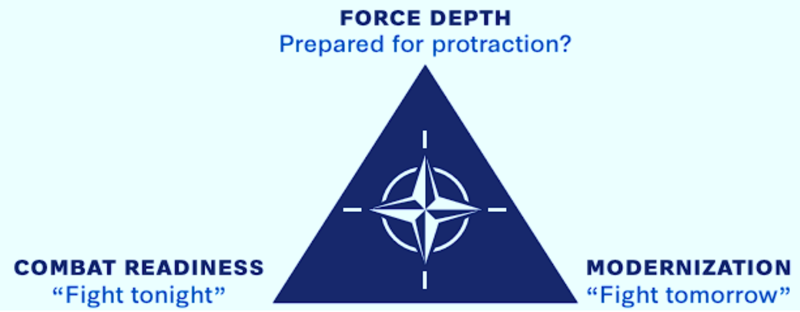


Fig. 2 A relevant concept of increasing resilience appropriate for deterring adversaries and defending the Alliance [3]

To meet current operational challenges, military experts believe that NATO member states must strengthen their supply chains, including transport and storage infrastructure, to ensure the rapid and efficient transfer of equipment and resources between areas or theaters of operations. In this regard, effective interoperability and coordination between the different forces of the Alliance are fundamental. It follows that the standardization of equipment, communications, and operational procedures between member states' forces will allow for their better integration into a common system, thus facilitating the rapid and efficient mobilization of personnel and logistical resources (of material, financial, and informational nature) [6].

Another critical point is, from our point of view, the development of cyber defence capabilities and the protection of logistical networks from external attacks or sabotage. With the rapid evolution of technologies, data protection, and communication security become vital to maintain a constant flow of information and materials. In addition, Member States need to invest in advanced technological solutions, including drones, satellite monitoring systems, and automation in logistics management, to improve efficiency and reduce reliance on human resources in a protracted conflict.

In parallel, the development of a robust defense industrial base is essential to sustain operations in the long term. This must not only meet immediate needs, but also ensure the continuous production of equipment, munitions, and technology, which is essential in a large-scale conflict. The creation of partnerships between the public and private sectors can stimulate innovation and flexibility in the defense industry, allowing rapid reactions to emerging operational needs. These partnerships can also include expanding collaboration with non-military industries to rapidly adapt production solutions to the requirements of a modern conflict [6].

Regarding the financial sustainability of long-term operations, according to the experts' assessment, NATO countries must review their budget structures and ensure constant and flexible financial flows to support defense efforts. This requires an efficient allocation of resources and greater transparency in the management of funds intended for the defense sector. Collaboration within the Alliance, in particular through common financing mechanisms, will contribute to a better distribution of costs and reduce the pressure on individual budgets of member states [3].

Thus, we believe that to meet the challenges of high-intensity warfare, NATO countries will need to combine advances in operational logistics with greater flexibility, coordination, and financial sustainability. This requires an integrated approach that ensures both the rapid mobilization of resources and the necessary long-term support for Alliance military forces, regardless of the duration and intensity of the conflict.

Starting from several directions that we propose, for the continuous improvement of operational logistics, we developed five subsequences within the second sequence, thus managing to appropriately develop in content all the elements in Figure 3. To this end, we used a combination of analytical, inductive, deductive and comparative methodological tools.

2.ELEMENTS OF INCREASING THE PERFORMANCE OF OPERATIONAL MILITARY LOGISTICS

The continuous and rapid development of military equipment that is and will be at the disposal of NATO national and multinational combat forces has a major impact on operational logistics. This determines that logistics managers and their subordinates, from the strategic level to the lower tactical level, to act in the direction of implementing logistics principles and functions according to the new operational requirements identified from the lessons learned resulting from the conduct of the armed conflict in the theater of violent confrontations in Ukraine.

The accumulation of modern equipment by operational structures and as a result of the aforementioned identified lessons, will determine new challenges for management and execution logisticians. In this sense, areas of logistical support will be involved, such as supply, maintenance, movement and transport, which will be correlatively and systemically engaged to ensure the consumption of materials necessary for operation, the provision of maintenance services, as well as for their timely movement to the area/theater of operations, but also within it.

In full agreement with the concept of transforming the Alliance's functions, operational logistics represents a system of systems, capable of anticipating and solving the requirements of the forces on which the evolution of joint and tactical situations will depend. In this sense, the support requirements (national and/or multinational) define even more precisely the role and importance of operational logistics (especially for the United States, Great Britain, and France), due to its expeditionary nature depending on the missions of the forces constituted by NATO states, also taking into account the experience of past campaigns in Iraq and Afghanistan [7]. Moreover, the destructive offensive actions, the challenges, and the consequences related to the Russian army's invasion of Ukraine have determined both on the part of the invaded state and on the part of the member countries of the North Atlantic Alliance, combined actions appropriate to the structural and functional reorganization and increase of the resilience of the combat forces, as well as of the specific operational logistics [8].

Therefore, the essential directions (objectives) revealed in Figure 3 aim at: *the organizational reconfiguration of logistics forces; the (overall) increase in operational logistics performance through the adequate modernization of its functional areas; the adequate planning of operational logistics with national and multinational status; the concretization in new conditions of resilience and risk management specific to operational logistics; the concretization of new requirements both in the field of training and in that of improving the training of officers who will perform leadership or execution duties of logistical support* [9]. All of these will be developed briefly, further, in a manner appropriate to the new requirements resulting from the lessons identified, as a result of the armed conflict in Ukraine.

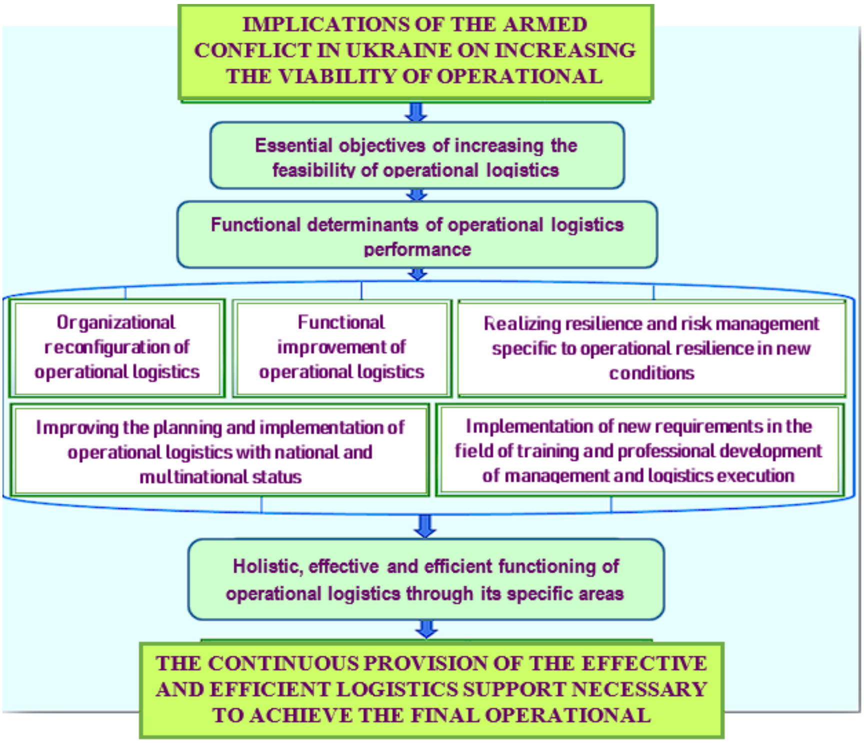

IMPLICATIONS OF THE ARMED CONFLICT IN UKRAINE ON INCREASING THE VIABILITY OF OPERATIONAL
Essential objectives of increasing the feasibility of operational logistics
Functional determinants of operational logistics performance
Organizational reconfiguration of operational logistics
Functional improvement of operational logistics
Realizing resilience and risk management specific to operational resilience in new conditions
Improving the planning and implementation of operational logistics with national and multinational status
Implementation of new requirements in the field of training and professional development of management and logistics execution
Holistic, effective and efficient functioning of operational logistics through its specific areas
THE CONTINUOUS PROVISION OF THE EFFECTIVE AND EFFICIENT LOGISTICS SUPPORT NECESSARY TO ACHIEVE THE FINAL OPERATIONAL

Fig. 3 Functional determinations regarding the increase of operational logistics performance [9]

The transformations and challenges determined by rapid technological and informational developments, specific to modern warfare, determine more and more conceptual and practical innovations for the continuous adaptation and modernization of operational logistics at all levels of military art (strategic, joint, and tactical), for achieving the overlap of the logistical support effort over the operational one to achieve success in the confrontation with the opposing forces and reach the final state in the area (theater) of joint operations in which national and/or multinational action and support forces are engaged. Therefore, the effect of increasing operational logistics performance is given, according to our assessment, by the relationship [9]:

$$\mathbf{E_{OLi} = (OLM\ x\ OLn/Lon) – MR_fC},$$

where:

- ✓ **E_{OLi}** = the effect of increasing operational logistics performance, expressed in value;
- ✓ **OLM** = the mission of operational logistics, represented and expressed in value - given by total capabilities;
- ✓ **OLi** = improving operational logistics (with increased resilience), with a determined value for total capabilities;
- ✓ **OLn** = non-modernized operational logistics, with a determined value for total capabilities;
- ✓ **MR_fC** = the consequences of the manifestation of risk factors, expressed in value.

The relational concretization of the aforementioned formula led us to highlight several objectives of maximum importance, according to Figure 3, which have the role of suggesting to specialists several ideas that can be exploited in the future for continuous modernization of operational logistics in the Romanian Army.

2.1.Organizational reconfiguration of logistics forces

Under the conditions of modern warfare, resulting from the confrontation between the aggressor and the defending forces in the joint theater of operations in Ukraine, there is a need for organizational reconfiguration of the logistics forces, especially at the tactical level, to increase their effectiveness and functional efficiency through improved structures, increased agility, resilience and robustness in the I, II, and III lines of operational logistics support. This requires structural and procedural improvement that allows ensuring a high level of sufficiency, flexibility, and modularity to ensure the optimal and timely provision of the resources and services necessary for the operational forces (at the tactical levels) și/sau joint), by the requirements, resources, the means, systems, and software available [10; 11], for the adequate fulfillment of the missions received and the achievement of the projected final state [12].

Regarding the structural organization, we consider that, at the level of the operational logistics modules (S4, G4, A4, N4, J4), organizational modeling is still necessary to increase functional performance to effectively manage, on a specialized basis, tactical logistic support units and subunits. To this end, for the logistic support execution structures, it is necessary, in addition to the appropriate transformation to achieve superior modularity and flexibility characteristics, to make and implement decisions to increase the level of protection by creating and allocating additional structures intended for: defense against ground and air actions of enemy forces using modern high-precision strike means, including cyber disruption; operation of identification, jamming and countermeasure systems for all drones operated by the enemy for attack and destruction; use of drones intended for the transport of materials in limited quantities (up to 1000 kg. or more) [13; 14], especially for combat, support and/or special operations subunits and units [15] which act in isolated directions that impose constraints on the normal implementation of logistical transport operations; the use of tiny ("pocket") drones for the purpose of directing and monitoring the movement of transport columns with materials requested by combat and combat support structures, etc.

In terms of procedural organization, from our point of view, new abilities and responsibilities are needed from the bodies of management and execution of operational logistics support, which must act by the new requirements determined by the use of modern technology, high-performance weapons systems and, especially, in terms of planning and ensuring timely material consumption and the continuous implementation of adequate transport, maintenance, medical support, protection and self-protection operations against the destructive actions of adverse forces. In this regard, we consider that a pertinent analysis and evaluation of the functional responsibilities of the bodies of management and execution of operational logistics, as well as of the inter-functional relations between them (regarding the chain of command and horizontal and vertical communication flows) is necessary.

2.2. Functional improvement of operational logistics

The need for the continuous achievement of operational objectives by joint combat forces, in dynamic conditions characterized by uncertainty and increased risk, determines, from our point of view, an increase (overall) in the performance of operational logistics through the appropriate modernization of its functional areas. Thus, the first area - ***supply*** or ***resupply*** - requires the existence of advanced technical forces and means, which allow for the rapid receipt, reception, and distribution of materials necessary for the combat and support structures within the organic structure of a combat force (national and/or multinational) operationally integrated in the area of joint operations, which implies the existence of viable supply chains. To achieve the projected success in achieving the necessary logistical support for combat and support structures, the management of the advanced military supply chain has the role of achieving important objectives necessary for logistical concentration, according to the operational effort, through: advanced, feasible, flexible and classified planning, which meets the requirements of resilience and risk management in the conduct of specific activities, for the delivery of the necessary logistical resources up to the fighter, equipment, fire system level [16], etc; the existence and employment of the forces, means and specialized infrastructure necessary for the rapid, efficient and resilient movement of goods between the components of the supply chain; the effective, protected, flexible and continuous implementation of distribution operations of equipment and other materials necessary for operational structures in any time, season and weather conditions ; the procurement and use of the RFID system based on GIS ("Geographic Information System"), necessary to increase the visibility of the movement of materials from the logistics support execution structures to military consumers and users (fighters, equipment, etc.) and for making real-time replenishment decisions [17].

In the perspective of 2035, the replenishment of the Alliance's operational forces focused on the on-demand (pull) process, will involve reducing the logistical footprint while ensuring timely and continuous provision at the tactical level (platoon, company, battalion, and similar) of all the resources necessary for the combatant forces to carry out their missions [18].

The existence of continuous flows of inputs and outputs of goods necessary to carry out planned operational combinations, in the integrated tactical operations areas of the joint (JOA), implies the existence of robust, versatile (lean and agile) supply chains [19], digitalized, flexible and resilient, allowing continuous flows (of information, goods, financial) [20] by integrating: *suppliers of goods; service providers; manufacturers; warehouses (belonging to existing logistics bases in the JOI); warehouses of economic operators (or belonging to branches of the body within the Alliance member state, specialized in the management and administration of state reserves); military warehouses (from the composition of the logistics support execution structures from the joint level up to, inclusively, the tactical level of the operational force); exoskeleton-type robotic devices to facilitate loading, unloading and handling operations in warehouses; consumers and end users (fighters, and equipment intended for the preparation and conduct of* *operations); civil and military transport entities; etc. We believe that each segment of the supply chain (mentioned) must be under the attention of responsible logistics commanders and managers, in terms of normal, effective and efficient functioning, corroborated with continuous protection from air strikes (with different means) and ground attacks (by surprise) by enemy forces.*

In Figure 4, I highlight (in our conception, less the integrated image: Military) [21] a variant of a supply-delivery chain for the staggered distribution of ammunition, through military ammunition depots integrated into the logistic support lines (belonging to the profile structures) to the combatants and the equipment served by them, necessary to replenish stocks to prepare and conduct operations at the joint and tactical levels. The design and management appropriate to the effective and efficient functioning of the military supply chain management - M.S.C.M., so that the contracting and resupply with ammunition of caliber over 20 mm and up to 20 mm (Battle Decisive Munitions - BDM and NON-BDM) of the national combatant structures, as well as of the allied ones participating in the joint operation conducted on the national territory or outside it, is the responsibility of the J4/GFI and JLSG/GFI logistic module. During the implementation of specific MSCM activities, for the resilient and timely support of troops with sufficient quantities of ammunition, the leadership and execution structures of logistical support will also be involved (upon order) in a staggered manner, down to the lower tactical level (battalion or similar).

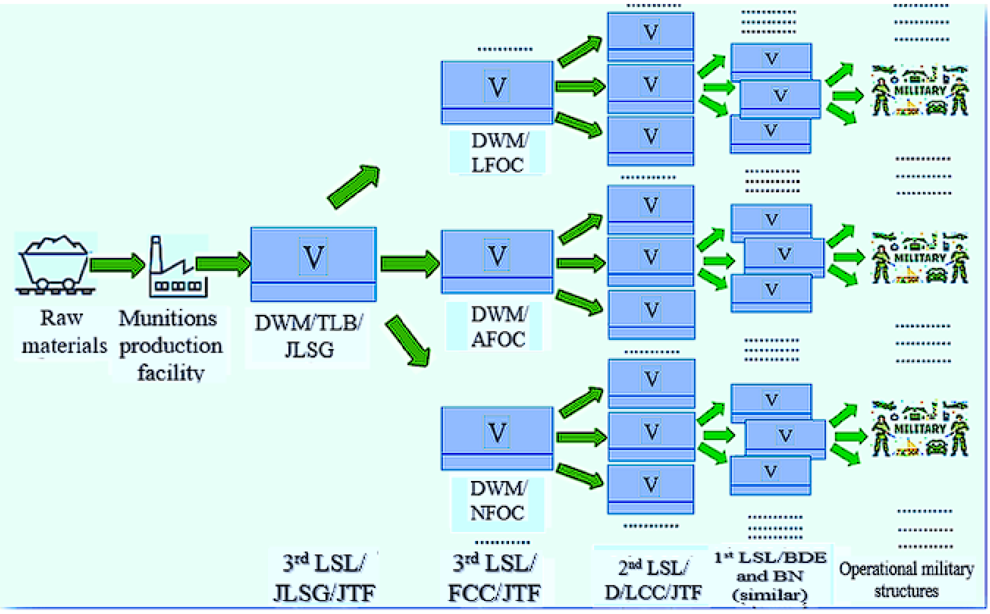


Fig. 4 Supply chain picture for supporting operational forces with munitions

Legend:

- ✓ DWM/TLB/JLSG = Depot of Weapons and Munitions/Theater Logistics Base/Joint
  Logistic Support Group;
- ✓ DWM/LFOC = Depot of Weapons and Munitions/Land Forces Operational Command;
- ✓ DWM/AFOC = Depot of Weapons and Munitions/Aer Forces Operational Command;
- ✓ DWM/NFOC = Depot of Weapons and Munitions/Naval Forces Operational
- ✓ Command/;
- ✓ 3rd LSL/JLSG/JTF = 3rd Logistics Support Line/Joint Logistics Support Group/Joint Task Force (Corp level);
- ✓ 3rdLSL/FCC/JLSG/JTF = 3rd Logistics Support Line/Forces Components Commands/Joint Task Force (Corp level);
- ✓ 2nd LSL/D/LCC/JTF = 2nd Logistics Support Line/Division/Land Component
- ✓ Command/Joint Task Force
- ✓ 1st LSL/BDE and BN (similar) = 1st Logistics Support Line/Brigade and Battalion

(similar).

To easily access real-time information and make appropriate decisions regarding acquisitions, requisitions, timely resupply, and/or timely provision of campaign services required by operational structures to properly fulfill the missions received, military logisticians (leadership and execution) can use rugged tablets. Entering the necessary data into the system of each tablet requires: either the use of several methods, including drones, 3D RealSense cameras, RFID scanners, and barcode readers; or their direct entry by user personnel [22].

The complexity of the destructive actions manifested in the theater of operations in Ukraine highlights lessons identified regarding the need for the survival of combat forces through planning and orders implemented by the command and execution structures of tactical-level operational logistics, which mainly aim to: establish the tasks of dispersing ammunition stocks necessary for conducting defensive and offensive tactical operations; identify possibilities for establishing places for performing maintenance operations on equipment that has become non-functional; continuous reconfiguration of command and control processes of essential logistical operations of supply, movement, transport, maintenance, medical support, for their effectiveness and efficiency [23].

At the same time, the conduct of high-intensity operations on the Ukrainian front reveals another lesson identified regarding the consumption rates of ammunition and spare parts, which are particularly high. This implies the development of the industrial infrastructure necessary for the sufficient production of the aforementioned materials, to ensure the normal functioning of the equipment (armored vehicles, motor vehicles, fire systems, etc.) and the necessary resilience both in the initial stages of the defensive operations against the enemy's offensive invasion actions and during their other phases [23].

Given Russia's clear intentions to annex its eastern neighbor, combined with the significant shortage of equipment and ammunition intended for the defense of sovereignty by the invaded Ukraine, at the beginning of March 2022, a multinational aid body was installed within the headquarters of the US European Command. It had and aims to ensure that the resources of each donor state (equipment of all types, ammunition, and other materials, which have been and will be worth billions of dollars) reach the Ukrainian state army, as the beneficiary, to successfully carry out operations to liberate the entire national territory [24].

To respond to Russian attacks in the occupied areas and gain the initiative to launch the offensive necessary to liberate the national territory, the Ukrainian combat forces consume large quantities of ammunition daily and as such have a significant deficit of projectiles necessary for the operation of artillery weapons. Under these conditions, at the NATO level, it was agreed to increase the production of ammunition by the allied countries to that level that would allow the rhythmic supply of the Ukrainian state army [25].

If from the very first days of the invasion of Ukraine until today, the logistics of the Russian attacking forces have revealed continuous failures, the Ukrainian army, benefiting from direct support with equipment and other stringent materials by the USA and a host of other NATO member and non-member states, has managed to increase its mobility, protection and, as such, successes on the battlefield. Since October 2022, the Ukrainian logistics and engineering structures have benefited from the aforementioned states with adequate equipment for the identification, elimination and crossing of fortified areas (reinforced with dense obstacles) by the Russian invading forces, to repel or limit the counteroffensives of the Ukrainian army. To this end, the defense structures of the invaded state requested and received "demolition munitions, obstacle destruction and remote demining equipment using detonating cord, mobile assault bridges, river and coastal patrol vessels, mine-resistant and ambush-protected armored vehicles (MRAP), as well as artillery-launched anti-tank mines" (according to the lists published by the Pentagon's authorized body for providing the necessary military assistance to Ukraine) [26].

At the same time, since February 2022, in addition to tanks, infantry fighting vehicles, armored personnel carriers, HIMARS, and precision ammunition, the US has also supplied the operational defense structures of Ukraine with: tactical towing vehicles; tactical vehicles for the evacuation of battle-damaged equipment (TEHEVAC); ammunition support vehicles; mobile assault bridge systems with Bradley support vehicles; trucks and trailers for transporting heavy equipment; logistics support vehicles; heavy tankers and fuel trailers; MRAP vehicles; armored utility trucks; mine clearance equipment; coastal and river patrol boats; C-4 explosives; demolition munitions and demolition equipment for overcoming obstacles; equipment for placing obstacles, etc. [26].

As part of the same joint effort to aid the Ukrainian army, the United Kingdom provided minefield clearance capabilities and mobile assault bridges. Germany, Canada, Finland, Slovakia, and Norway provided equipment such as engineering vehicles on Leopard chassis and the Netherlands provided mobile assault bridges and trucks [26].

●*Movement and transport* represent another operational logistics area that must allow both the planned deployment of tactical forces (national and multinational) in the JOA according to the increased requirements of military mobility in conditions of risk and uncertainty [27; 9], as well as continuous flows of materials (through transport) in the tactical field, for the immediate completion of the deficits resulting from consumption and/or destruction caused by the enemy. Regarding ⁕*transport***,** in order to achieve the interoperability requirements, it is necessary to plan and carry out with appropriate means specific multimodal transport operations at the joint level, with an emphasis on the tactical level. In this context, very important (to be implemented) are the evolved processes of palletization and containerization by the provisions of NATO standards (in the field). This allows, for example, at the tactical level (within the framework of the land transport mode) a rapid transshipment of materials (packed in containers and/or pallets), as follows: *from railway transport vehicles to road transport vehicles; from road transport vehicles to tracked armored transport vehicles (especially in mountainous forested terrain); from tracked armored vehicles on carriers (up to the firing positions of fighters, armored vehicles, and fire means/systems). All of the above could be beneficially realized if, in our opinion, objectives were proposed and achieved, such as: continuous monitoring of (modern) motor transport vehicles by procuring and equipping them with advanced technical systems, intended to determine the visibility in traffic at any time (including at night) of both the means and the quantities moved (by transport); the acquisition of evaluated vehicles (automated, robotic and equipped with artificial intelligence), which can be directed through stations in tactical transport networks, without pilots (mechanics; the acquisition and use of armored tracked vehicles (usable with or without driver mechanics) necessary for the transport of materials to the combat supply points of (similar) combat and/or combat support companies; advanced protection (against attacks: ground of any nature; anti-aircraft including against drones; with CBRN means; of an electronic and/or cyber nature)* [27; 9] , *sufficient and continuous support of transport structures and columns during the fulfillment of resupply missions both day and night,* etc.

The successes of the Ukrainian army in liberating the areas of the country occupied by the Russian invading forces were based on the continuous, effective, efficient, flexible, and resilient functioning of its logistics. To this end, on the territory of the Ukrainian state, there was and is a solid railway infrastructure of vital importance, with multiple branches from the railway junctions, which, regardless of damage, could be quickly reconfigured to carry out logistical transports, with the necessary transshipments on secondary routes, for the timely delivery of equipment and materials to the fighters. At the same time, the logistical structures of the Ukrainian combat forces have benefited and continue to benefit from a substantial contribution from civilian transport companies, as well as from assistance services in other areas of operational logistical support [28].

The need for rapid, timely, and on-site transport of materials, according to tactical and/or joint operational forces, has led to the increasing use of drones to provide logistical support to combat forces. In response to evolving operational requirements, since 1999, Lockheed Martin and Kaman Aerospace Corporation have developed the Kaman K MAX Unmanned Autonomous System (UAS), by adapting the Kaman K 1200 helicopter. Subsequently, after a decade of research, testing, and contract development with the Marine Corps, two Kaman K MAX models were delivered to support operational forces in Afghanistan. Later, from December 2011 to May 2012, these UAS (existing within a detachment, which operated until 2014) were used to move (in the aforementioned theater of operations) significant quantities of materials from the main operating bases to the advanced ones. A study on the UAS profile conducted in 2013 highlighted its usefulness and efficiency, as well as its fundamental role in reducing the loss of human lives during combat and logistical operations. In October 2016, at the Marine Corps level, two structures (in collaboration), namely the Marine Corps Warfighting Lab (MCWL) and the Marine Corps Installations and Logistics - I&L), organized and conducted a war game, to test and implement specific engagement and operating concepts for three recently developed ULS models (“Unmanned Logistics System” ULS), according to a scenario that included a maritime expeditionary force and the appropriate logistical support to support its missions. The final report of the aforementioned war game showed that ULS is particularly effective in carrying out emergency supplies (considering the easy loading, unloading, maintenance, and “Just in Time” transport operations) in a high-risk operational environment (due to enemy actions), generating a reduction in the use of land convoys, but also of manned air transport. At the same time, it was concluded that it is necessary to continue research on ULSs to develop their technological and functional evolution concomitantly with the use of manufactured models [28; 9].

The previously presented facilities in the use of drones in the field of operational logistics are materialized by the Israeli Self-Defense Forces, which already have the bulky drone “Heron TP” (manufactured by the Israeli state company “Israel Aerospace Industries Ltd”) with the effective capacity to transport a ton of ammunition [29]. On the other hand, in the UK, the delivery of logistical loads in hazardous environments, appropriate to the operational environment of combat forces, has become an achievable objective through the Autonomous Last Mile Resupply (ALMRS) project through which the “In View UAV” model was developed. This is an unmanned aircraft made of composite materials (with: two engines; dry weight under 20 kg.; wingspan of 5 m; minimum transport capacity worth 1200 dollars and maximum of up to 1000 kg.), with facilities suitable for vertical take-off and landing in rugged terrain [30; 9].

Within the tactical and/or joint operations of the future, the performance of operational logistics in achieving the profile support of combat forces with significantly reduced human losses, at the right times and in the right places, is dependent not only on ULSs, but also on a set of unmanned ground vehicles (drones) (Unmanned Ground Vehicles UGV), which can operate unarmed and in logistical transport missions, whose evolution is similar to that of UAVs, and their use is done in tandem with them [31]. Several years ago, the Estonian army tested (and later implemented) the unmanned ground vehicle "THEMIS" (a tracked infantry technical system with a modular design and robust components, produced according to the utility of choice in: armed version for combat; unarmed model for transport) through the "Milrem" company in a simulated operational exercise (three days), to carry out logistical missions of transporting equipment and materials [32; 33; 34]. The aforementioned model has been operational during several experimental exercises, as well as in counter-insurgency missions, such as Operation "Barkhane" in Mali. Therefore, for their operational and logistical facilities, THEMIS UGVs have been purchased by 16 countries, 8 of which are NATO members (i.e., Estonia, France, Germany, the Netherlands, Norway, Spain, the United Kingdom and the United States) [35; 9]. As I have already mentioned, these means are based on modern technologies and act complementary to robots and artificial intelligence, according to the objectives and logistical activities planned and programmed to be carried out in managing stocks and transporting materials to the combat structures [36].

Figure 5 shows a logistical mode of action of a maritime expeditionary unit supported by ULSs. The (logistic) support is initiated from the seashore (from the sea), developing inland to various maritime structures through several logistic platforms [37, 9].

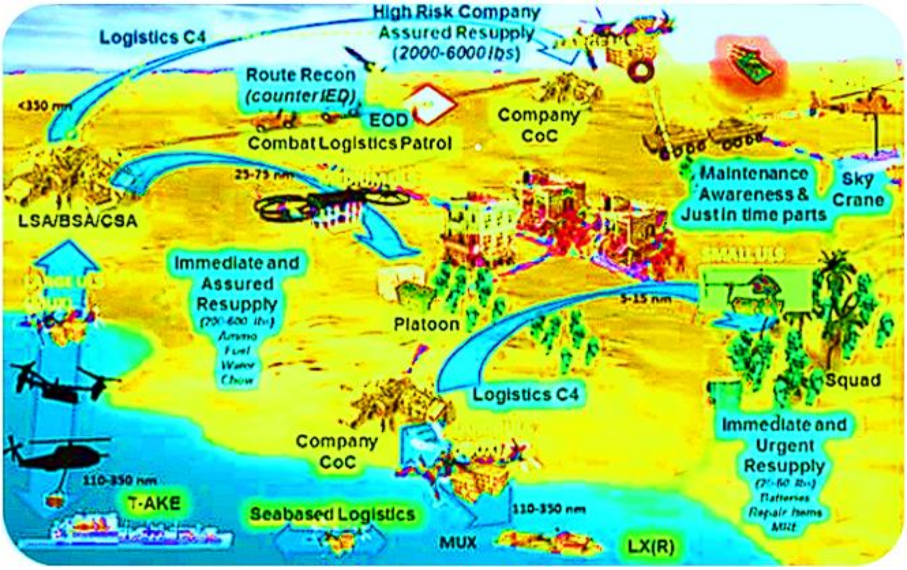


Fig. 5 Logistic drones (air and ground) are used to provide operational logistical support to a naval expeditionary structure (marine infantry) [37]

On 23.02.2023, the "Unmanned Systems Forum. Smart Approach, Fast Development" Forum took place, which was also attended by the Romanian Minister of Defense. There, new technologies were addressed, which will allow unmanned systems (through the development of multi-role capabilities) to have superior functional autonomy in modern warfare, focused mainly on those combat actions (with logistical implications and facilities) specific to reconnaissance, surveillance, target detection, electronic warfare, as well as for missions related to the protection of civilians or the precise identification of combatant and non-combatant structures [38].

For rapid monitoring of the transport and movement of materials (by supply class) intended for combat forces, in accordance with their requirements, both logistics managers and subordinate logisticians can use military tablets of the "rugged tablets" type, which include advanced security features (for example, CAC readers, i.e. "Common Access Card Reader") [39]. These contemporary operational resources can be deployed in command post facilities or directly in tactical environments, under severe and constraining working conditions. They incorporate appropriate durability requirements through design and manufacturing specifications and consequently necessitate only basic maintenance procedures, while simultaneously offering portability, lightweight construction, and ease of transportation during operational relocation. [40].

⁕*Movement* (as a subdomain of *movement and transport*) is the basis for the planned deployment of the operational force in the area or theater of operations combined with appropriate means (by moving: on national territory; strategic; at the operational or joint level) and includes the specific process of Reception, Staging, Onward Movement and Integration (RSOM&I) - as an important segment of operational logistics support [41]. The RSOM system is implemented as the 3rd line of logistic support of the joint multinational operation, which is prepared and carried out on the national territory or in an external theater of operations. Here, there are and operate, under protection conditions, a series of specific modern infrastructures, such as the air embarkation base (Aerial Port of Embarkation - APOE), the seaport port of embarkation (Seaport Port of Embarkation – SPOE), the rail port of embarkation (Rail Port of Embarkation - RPOE) - existing on the national territory in the area (territory) where the embarkation or embarkation of forces and means is carried out; Aerial Port of Debarkation (APOD), Seaport Port of Debarkation (SPOD), Rail Port of Debarkation (RPOD) - in the area (theater) of joint operations, where the forces necessary to be operationally engaged have been deployed; Holding Area (HA); Staging Area (SA); other elements [41;42]. A more complete picture of the RSOM&I mechanism, applicable by the US joint force in multi-domain operations, is presented in Figure 6.

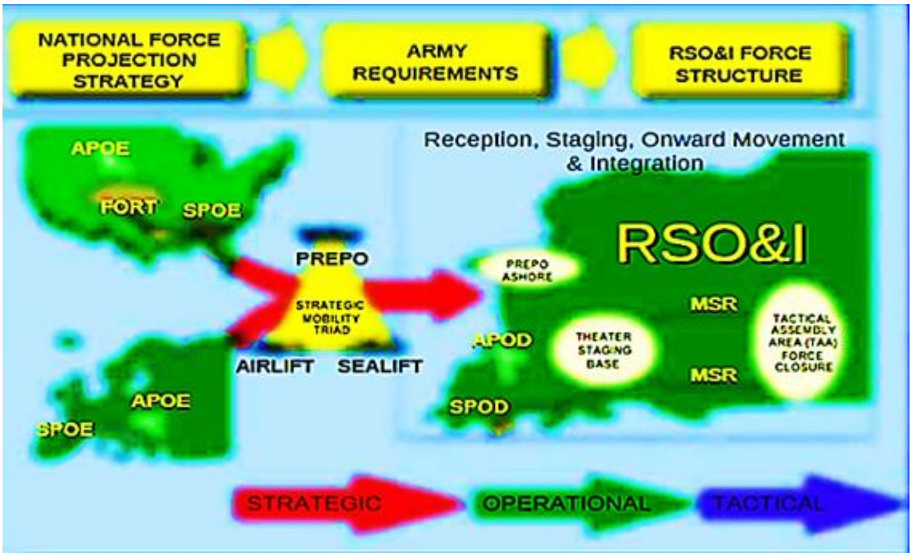


Fig. 6 RSO&I mechanism applicable by US joint forces [43; 44]

According to the requirements and exigencies of the specific mission, the Joint Logistic Support Group (JLSG), as an essential structure within the composition of the Joint Force, is directly involved and responsible for leading the deployment, support, and redeployment of operational forces in the area or theater of operations by accumulating and distributing the necessary logistical resources both with its forces and means and by carrying out operations specific to contracting and supporting the host nation (Host Nation Support - HNS) [45]. Therefore, the JLSG is responsible for the effective, efficient, and resilient organization and functioning of the RSOM in the area or theater of joint operations, which has specialized structures in its organization to support the combatant structures (of the operational commands: land; air; maritime; special operations, according to Figure 7) that act at this level [46], coordinating for this purpose - through its command and control authority (C2) - with the national support elements (NSEs) of the Alliance states participating with troops in the joint operation on national territory, with those responsible for the host nation's capabilities (operational request), as well as with contractors hired to provide materials and services by the requirements of the multinational combat forces [47].

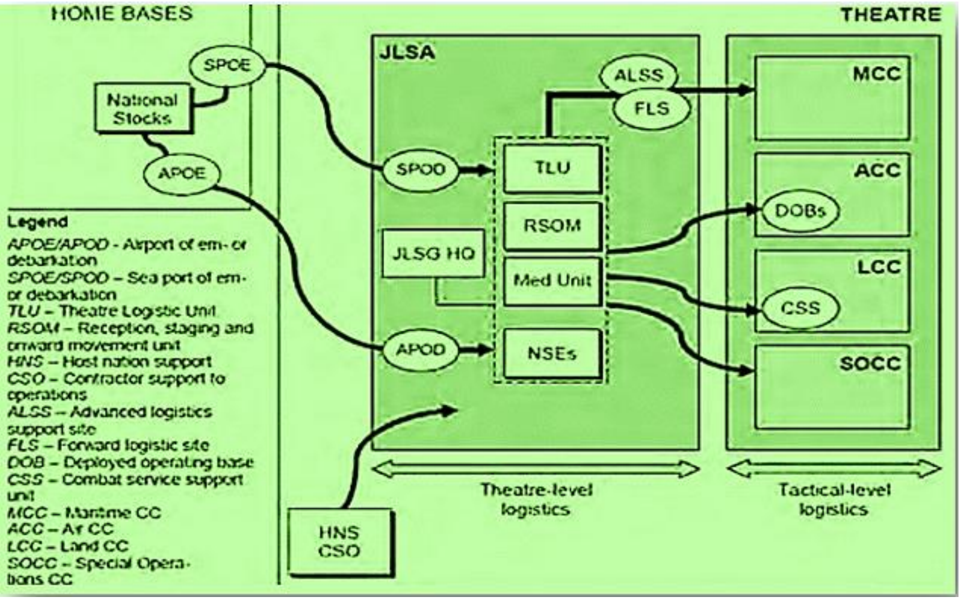

HOME BASES
THEATRE
SPOE
National Stocks
APOE
JLSA
ALSS
FLS
SPOD
TLU
RSOM
JLSG HQ
Med Unit
APOD
NSEs
HNS CSO
MCC
ACC
DOBs
LCC
CSS
SOCC
Theatre-level logistics
Tactical-level logistics
Legend
APOE/APOD - Airport of em- or debarkation
SPOE/SPOD – Sea port of em- or debarkation
TLU – Theatre Logistic Unit
RSOM – Reception, staging and onward movement unit
HNS – Host nation support
CSO – Contractor support to operations
ALSS – Advanced logistics support site
FLS – Forward logistic site
DOB – Deployed operating base
CSS – Combat service support unit
MCC – Maritime CC
ACC – Air CC
LCC – Land CC
SOCC – Special Operations CC

Fig. 7 Elements of the Joint Logistics Responsibility Area with JLSG and related functional relationships [47]

Given the lessons learned from the logistical failures of the Russian invading forces in Ukraine, we consider that, for the normal functioning of the RSOM mechanism in order to prepare and conduct a multinational operation assembled on the national territory, the following aspects could be taken into account: judicious planning of the activities specific to the 3rd line of logistical support by J4/JFC (Joint Force Command) and JLSG HQ (coordinated by J4) responsible for providing sufficient, flexible and resilient logistical support, according to the requirements received from the tactical operational forces (through their logistical management bodies) in the 2nd line of logistical support; the organization, coordination, command and control of the structures and facilities in the composition by JLSG HQ, for the effective, efficient and protected functioning of the RSOM; establishing viable, protected transport routes (Main Transport Route – MSR) with possibilities for variations in critical situations, which allow the safe movement of operational forces in order to integrate within the LRA (Logistics Responsability Area) within the tactical and/or joint device (according to the specifications in the OPORD received from the higher echelon); adequate replenishment of materials consumed from existing stocks at the combatant structures, during the movement (land, air, naval) in the area (theater) of joint operations, within the staging area (Staging Area); provision of additional quantities of materials (subsistence, ammunition, fuels-lubricants) for the combatant structures (combat and support) in the first echelon; other elements.

For the effective and continuous operation of the existing equipment in the combat structures, engaged in tactical and/or joint-level operations, it is necessary to improve the effective and efficient operation of the third important area of operational logistics, namely ***maintenance***. Very important here are the activities of planning and execution of maintenance activities in the preparation, conduct, and achievement of the final state of the operation concerning maintenance, evacuations, repairs, overhauls, and replacements of both combat vehicles and weapons systems. Particularly important here are maintenance materials, spare parts, aggregates, etc., which can be ensured through continuous resupply flows through single or combined push or pull processes, including through additive manufacturing ("Additive Manufacturing") of parts and components in the area of operations using printers 3D [48], 4D și 5D [49] or 6D [50].

Therefore, both combat vehicles (armored vehicles, trucks, etc.) and weapons systems (with increased performance) benefit (according to the requirements of opportunity and effectiveness) from simple or complex maintenance works involving fighters, crew chiefs, drivers, maintenance teams, management, and maintenance execution structures at the tactical and joint levels. The functional unavailability of some modern equipment (combat vehicles and weapons systems) may determine the taking of operational limitation decisions for some tactical combat structures, due to the non-existence of the guarantee of timely maintenance interventions (a fact also observed during the armed conflict in Ukraine). In this regard, experts believe that, in addition to the intervention of trained military personnel (who service combat equipment and technical systems) in carrying out repairs of reduced complexity, the modular structures of modern combat equipment could facilitate (allow) replacement of major components (modules), thus eliminating important maintenance work, which would involve the movement and continuous activity of specialized teams and equipment (with adequate protection), as well as the occurrence of immobilizations and blockages [51]. Figure 8 represents a process specific to *tactical-level maintenance intervention*.

The skills of logistics managers, the existence of specialists, and easy technical means of intervention at their disposal will allow the timely planning and execution of activities appropriate to the maintenance and repair of military or civilian equipment necessary for the conduct of operations in the tactical field. In carrying out these activities, advanced technology is needed, such as rugged tablets, which help to accurately capture data and increase the efficiency of operations. These tools (means) can help military and civilian specialists included in tactical maintenance structures and organized in teams, to: carry out preventive or corrective maintenance operations on time according to requirements; timely repair vehicles; management of spare parts and consumables; track, monitor, and report the performance of all actions regarding maintenance, repairs, and provision of consumables; carrying out related tasks assigned to those listed [53].

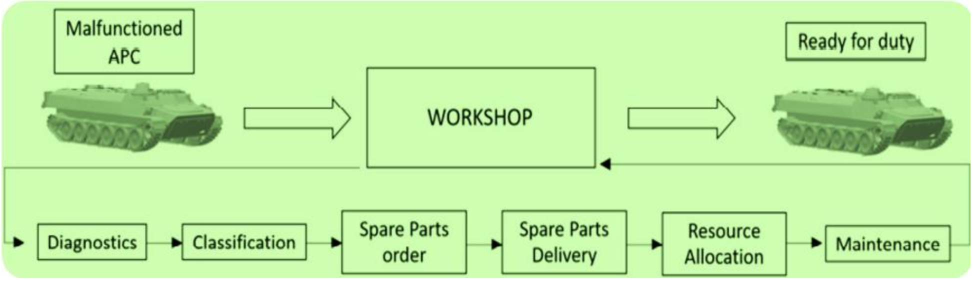


Fig. 8 Generic vision on maintenance intervention to a combat tactical structure [52]

The skills of logistics managers, the existence of specialists, and easy technical means of intervention at their disposal will allow the timely planning and execution of activities appropriate to the maintenance and repair of military or civilian equipment necessary for the conduct of operations in the tactical field. In carrying out these activities, advanced technology is needed, such as rugged tablets, which help to accurately capture data and increase the efficiency of operations. These tools (means) can help military and civilian specialists included in tactical maintenance structures and organized in teams, to: carry out preventive or corrective maintenance operations on time according to requirements; timely repair vehicles; management of spare parts and consumables; track, monitor, and reporting the performance of all actions regarding maintenance, repairs, and provision of consumables; carrying out related tasks assigned to

those listed [54; 55]. A facility for protecting the performance of maintenance activities through the appropriate structures (from the joint level to the last tactical level) would represent a procurement of armored means for equipping maintenance formations to reduce human losses (primarily), during the conduct of tactical operations.

Another area of major importance in the planning and conduct of logistical support of tactical combat actions is ●*operational medical support*. The normal functionality, through the effective conduct of all specific operations (at the tactical and joint levels), is determined by its direct leadership and execution by the chief physician and the subordinate medical treatment formations (from MTF ROL 1 to MTF ROL 3) [56]. The operational medical support missions are carried out by the specialized structures of the joint force through specific “MEDEVAC” operations. These must allow tactical medical evacuations (also called “TACEVAC”), for the adequate transport of the wounded from MTF ROL 2 (from the combatant structures) to MTF ROL 3 (from the JLSG). From here, depending on the complexity of the interventions to be made, the strategic medical evacuation (also called “STRATEVAC”) takes place from MTF ROL 3 at the joint level to MTF ROL 4 - located on the national territory or of another NATO state (depending on the situation, conditions, and urgency of the intervention) [41; 57; 9]. In Figure 9 we present the successive phases of medical evacuation, of the "MEDEVAC" type, from the tactical to the strategic level.

Given the current independent functioning at the tactical level of medical support compared to the areas of operational logistics [41] (following the practical reality in the Romanian Army), we consider that this will lead, to the situation of real tactical operations, to the emergence of syncopes regarding: the correlation of logistical supply flows (appropriate to the other areas of logistical support) with those related to medical support; collaboration in planning and executing logistical and medical transports and evacuations; coordination of actions specific to the deployment on the ground (within the logistical support lines) of the logistical and medical support execution structures (given that the tactical planners are different), etc. However, for functioning within the required parameters, we consider that the tactical and/or joint leaders (commanders) must pursue the achievement of adequate and continuous collaboration both between the logistical and medical support management bodies, as well as between their execution structures during the preparation and conduct of joint operations. We also consider that, at a tactical and/or joint level, it would be important to: acquire armored means – including drones – for evacuating the wounded (from established points), which would allow for greater protection against attacks by enemy forces; protection against the enemy's destructive actions with ground and air means, especially with kamikaze drones [59].

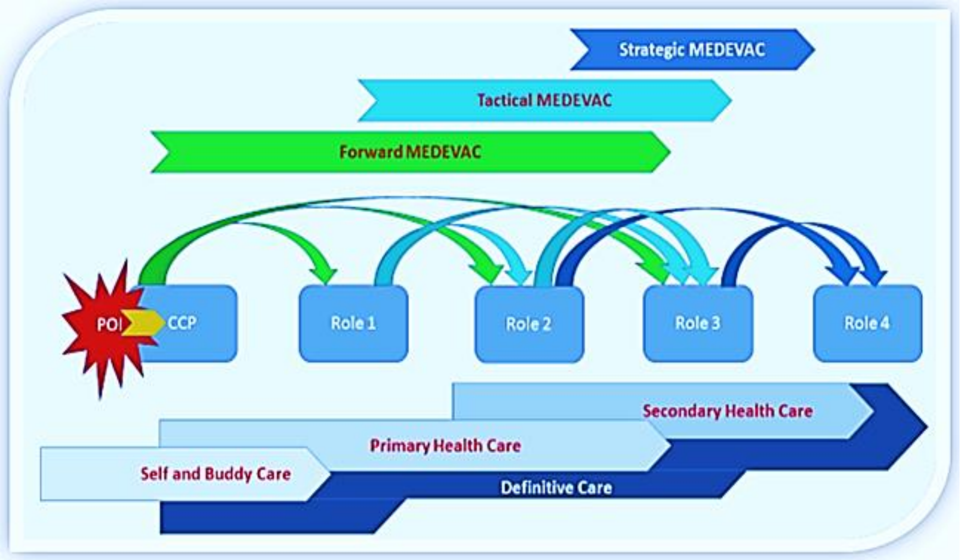


Fig. 9 Medical evacuation process within the NATO joint force [56]

The other areas (basic and related) of operational logistic support also require increased attention for modernization, taking into account the requirements and exigencies determined by the new military actions and challenges in the Ukrainian theater. In this regard, we would point out only one important requirement (related to campaign services), namely the acquisition of food preparation modules, which include mobile campaign kitchens and other technologically advanced food materials to replace the existing ones, to avoid deficiencies that appear during tactical exercises, due to the physical and moral wear and tear of the existing ones in the equipment of operational tactical structures.

2.3. Realizing resilience and risk management specific to operational logistics in new conditions

Providing logistical support according to the combat forces' operational situation requires the concretization of resilience and risk management specific to operational logistics in new conditions. This is based on analyses, assessments, and profile decisions, concretized in plans, orders, and documents, which will be implemented through activities appropriate to meet the identified organizational and individual requirements (consumption, use, and service provision) depending on the different capabilities that will be engaged and the established priorities. According to the operational context in the joint operations area, different logistical systems are integrated, within the combat devices of the combat and support forces, which must function effectively and efficiently without disruptions or turbulence. In this framework, the management and logistics execution bodies must act together to implement the necessary measures to increase the specific resilience of logistical support (provided to operational forces) in full correlation with the careful application of risk management at the tactical and joint levels [60].

Generically, the resilience of a military logistics system or a military supply chain (at tactical and/or joint level) represents the capacity to return to normal performance functionality within a favorable period, after it has been disrupted. At the same time, resilience reveals the capacity of the aforementioned systems to prepare to respond to the action of destabilizing impact factors (provocative of turbulence and uncertainty) that determine functional disruptions and interruptions (concerning the stopping of flows of goods and those adjacent to them, namely the flow of orders, the flow of production, the financial flow related to deliveries, etc.) to continue operations at an accepted level, as well as the levels of connection and control over the component structures [61; 62; 63]. Figure 10 presents a graph of possible disruptions to an operational logistics system or military supply chain until it returns to normal functionality; it includes eight phases, as follows: preparation; occurrence of the disruptive event; first response intervention; production of the initial impact; manifestation of the total impact; carrying out recovery preparations; achieving recovery; manifestation of the long-term impact [64].

Several risk factors with an immediate effect on the disruption of the normal functioning of an operational logistics system or a related supply chain mainly refer to: the manifestation of terrorist actions; obvious turbulence at a supplier's factory (interruption of incoming flows of raw materials due to unforeseen causes; strikes, bankruptcy, fires, explosions, etc.); various natural disasters (earthquakes, floods, epidemics, etc.); major cyber-attacks, etc. [65; 66].

According to the international authorized body (North American CRO Council), it results that in business the concept of operational resilience is used, which highlights the capacity to carry out specific operations, even critical ones. The result, therefore, is the action of effective, efficient, and continuous management of operational risks, corroborated with the commitment of appropriate financial means to materialize the aforementioned concept of resilience through appropriate actions to prepare, adapt, resist turbulence, and impact, recover and eliminate functional interruptions of the given business system. Specific resilience planning within an economic organization reveals and involves activities specific to business continuity, in simultaneous or different phases, such as adequate response to the consequences of the incident; carrying out crisis management; recovery after impact; adequate implementation of intervention options specific to Cyber Security, third-party relationship management, IT, etc. [67].

Following what has been stated previously, it results that in the process of functioning of a logistics system or of the management of a military supply chain (MLAM) at the tactical and/or joint levels, phases of specific correlation of risk management with the resilience involved take place. Thus, the prevention of risks (through necessary actions for identification, early warning, and preparation of the appropriate response to any logistical crisis) determines the design and implementation of a mechanism focused on avoiding and/or reducing as much as possible the disruptions, irregularities and as such the vulnerabilities. The consequence is the appropriate increase in the resilience of the logistics system or of the MLAM respectively based on proactive planning by phases and subphases of all specific actions, corroborated or common with those specific to risk management [77].

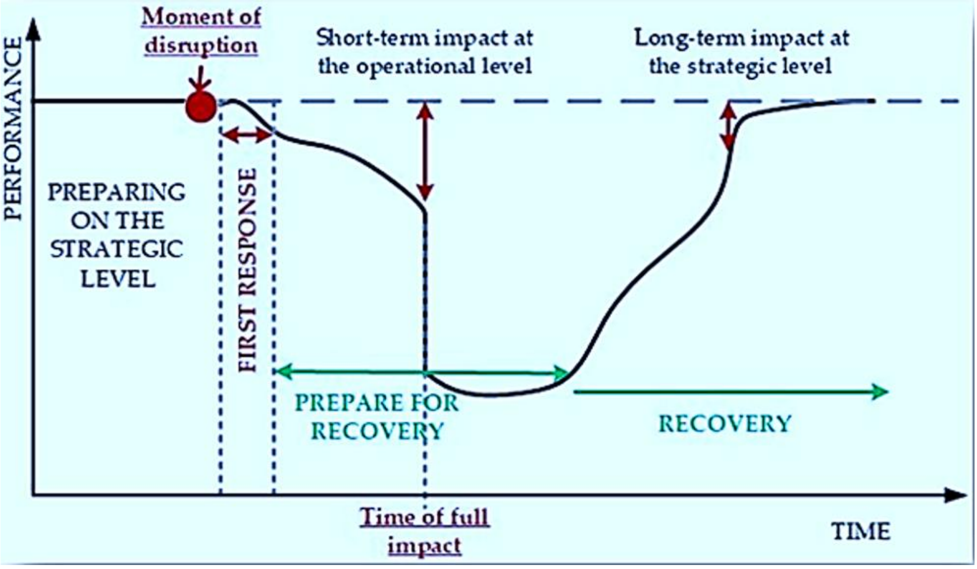

Moment of disruption
Short-term impact at the operational level
Long-term impact at the strategic level
PERFORMANCE
PREPARING ON THE STRATEGIC LEVEL
FIRST RESPONSE
PREPARE FOR RECOVERY
RECOVERY
Time of full impact
TIME

Fig. 10 Systemic vision on the resilience phases of an operational logistics system or related delivery supply chain [64]

By what has been stated previously, it results that in the process of functioning of a logistics system or of the management of a military supply chain (MLAM) at the tactical and/or joint levels, phases of specific correlation of risk management with the resilience involved takes place. Thus, the prevention of risks (through necessary actions for identification, early warning, and preparation of the appropriate response to any logistical crisis) determines the design and implementation of a mechanism focused on avoiding and/or reducing as much as possible the disruptions, irregularities and as such the vulnerabilities. The consequence is the appropriate increase in the resilience of the logistics system or of the MLAM respectively based on proactive planning by phases and subphases of all specific actions, corroborated or common with those specific to risk management) [68], continuity and functional protection; training of operational logistics management and execution personnel in the spirit of the appropriate applicability of both concepts, etc. Logistics managers and their subordinates are responsible, from our point of view, for the effective and efficient planning and operation of military supply chains. These involve complex processes carried out by specialized personnel and modern equipment for the purpose of procuring, transporting, storing, and delivering materials by supply classes to the combatant structures of the operational forces, in a timely manner and at the indicated time, according to their requirements. At the same time, the aforementioned specialists must act collaboratively and cooperatively to create the safety conditions related to the movement and provision of the necessary resources to the military beneficiaries by adequately implementing risk management and resilience measures. Therefore, according to the experts' assessment, it is necessary for logisticians to periodically analyze the risks that generate disruptions and functional disorders within the operational logistics system and/or the related supply chain, in order to avoid and/or mitigate them in time. Within this framework, emergency intervention scenarios could be built depending on the types of operations carried out and the missions received by the operational forces (tactical and/or joint) based on decisions substantiated in advance, which would allow the full or partial implementation of the phases of the resilience mechanism (mentioned above), for the continuation of logistical support (by support areas) at a certain pace depending on the existing potential and augmented by the higher echelon.

The complexity of the operations of tactical and/or joint combat forces (up to and including the G.F.Î. level), as well as the logistical support related to them, obviously determines a different daily operational rhythm. If in this rapid mechanism of operational evolution insurmountable discrepancies appear between the dynamic action of the combat forces and the logistical support necessary to be given to them, a specific crisis phenomenon will soon manifest itself (partial or total deficit of logistical resources and services), known in the economic field as the logistics culmination") [64], considered by us, at the operational level, as a logistics critical point or logistics critical deficit. Here, effective manifestations of adequate resilience in supply, transport, maintenance (as areas of operational logistics support) and medical support can be evident, because the avoidance of the manifestation of disruptive (risk) factors can no longer be prevented (at a given point) even though visible intervention measures have been taken (according to the requirements implied by the action effort) [69; 70] (Figure 11).

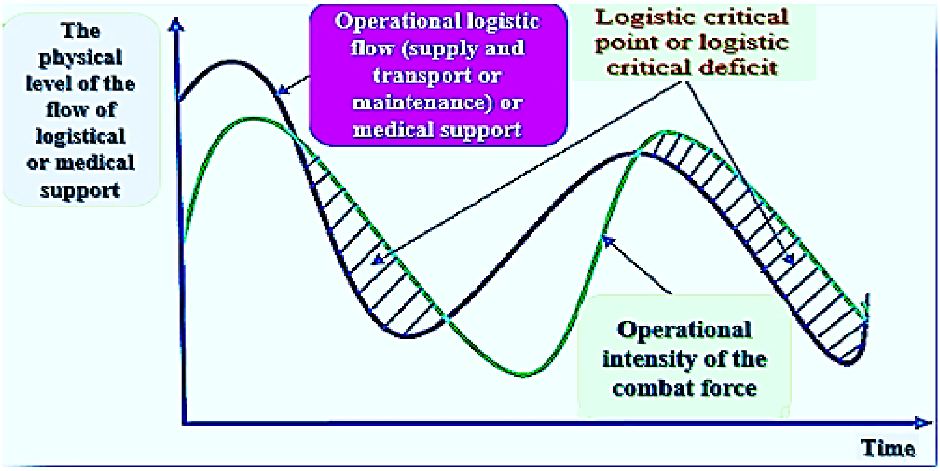

The physical level of the flow of logistical or medical support
Operational logistic flow (supply and transport or maintenance) or medical support
Logistic critical point or logistic critical deficit
Operational intensity of the combat force
Time

Fig. 11 A picture of the logistics critical point (deficit) [9]

In figure 12 we reveal the way in which the logistics critical point (deficit) manifests itself, which reveals a relationship and integration with the specific resilience graph presented previously. According to what has been revealed, we believe that it is possible to deduce the manifestation of the effect of possible risk-generating elements, such as: the insufficiency of logistical resources made available in the event of increased operational intensity, which would highlight the failure of logisticians to anticipate the situation in order to supplement the profile support; unpredictable actions of enemy forces on supply sources, transport columns or on logistic support subunits and units; ad hoc introduction of additional combat forces into the tactical and/or joint device, for the operational development necessary to reach the final state, not included in the logistical planning and execution processes, etc.

From our point of view, the critical logistical point (deficit) can appear during any tactical operation, with an immediate effect on the rapid decrease in the effectiveness and efficiency of the logistical support provided, taking into account the requirements highlighted below. For example, with the territorial (geographic) development of the area of operations, by the operational (tactical) forces conducting offensive operations, several requirements with increased risk (disruptive) potential appear in the provision (exhaustion) of the logistical resources necessary for resupply, such as: the increase in the need for material transport means (ammunition and lubricant fuels, in particular) for combat and support structures, to cover additional distances (under protection conditions); the need for increased protection of components of military supply chains (suppliers, manufacturers, logistics bases, material depots, logistics structures within the combatant tactical organizations, etc.) from the destructive actions of enemy forces; requesting prompt intervention with logistical resources by the higher echelon in critical situations, to avoid the emergence of a critical logistical point (deficit), etc. [70]

Consider the situation in which the enemy strikes, for example, a mixed territorial material depot, after implementing all risk management actions, the destructive and disruptive impact can determine the progressive and total destruction of the stored quantity of a product (ST), according to Figure 12, including the safety stock (Ss) and the current stock (Scr). For some time, the stock is non-existent, there is a stock shortage, and as such the storage infrastructure must be quickly rebuilt and then daily replenishment activities must be scheduled and carried out - until the initial level of the total stock (ST) is effectively reconstituted, with the two parts mentioned.

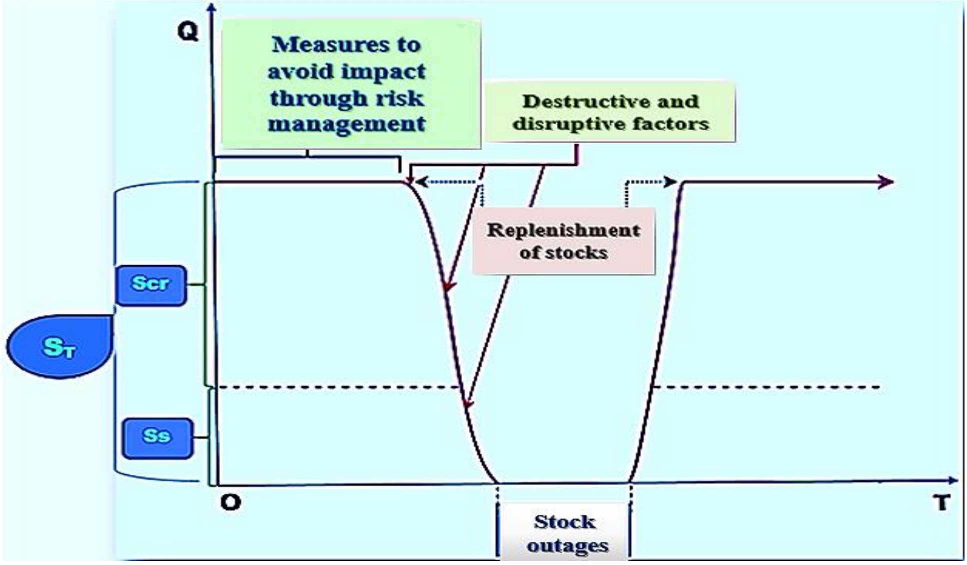

Q
Measures to avoid impact through risk management
Destructive and disruptive factors
Replenishment of stocks
Scr
S_T
Ss
O
T
Stock outages

Fig. 12 Briefly identifying the specific phases of resilience related to a mixed territorial material repository [9]

Legend:

Q = The quantity of product "X" stored;
Ts = Storage time;
S_T = Total stock in warehouse;
Ss = Safety stock in the warehouse;
Scr = Current stock in warehouse.

If we consider the way to highlight the resilience of the stock of a material (from classes I, III, V) existing (on combat structures and in warehouses) at a tactical and/or joint echelon, here, the safety stock (Ss) represents the troop stock or the operational stock (i.e. the planned stock – Sp), and the current stock (Scr) includes the amount of Combat Day of Supply (CDOS), which would be consumed in a day of combat. Of course, depending on the situation, the troops can be resupplied with the required materials from the safety stock (i.e. Sp), with the deficits to be filled 100% in the evening of the day of operation, upon request, by the higher echelon.

Based on what is presented, both logistics managers and their subordinates in the logistics modules can use three indicators to determine the level of resilience of operational logistics support [83], as can be noted further on.

2.3.Improving the planning and implementation of operational logistics with national and multinational status

All of the above-mentioned imply the improvement of the planning and implementation of operational logistics with national and multinational status (further details are provided in Annex 6), which must involve systemic and subsystem improvement in the planning of operations of combat forces (in their preparation and conduct) at all levels of military art, a process that needs to be carried out rigorously by evaluating the forces, resources employed, risks and elements (indicators) of progress in the accomplishment of missions. Within this laborious mechanism, commanders, staff, and logistics managers (together with their subordinates) will skillfully lead complex processes, appropriate for the development of specific effective, resilient, and integrative planning (for immediate or future application), in action situations and correlated operational stages, such as current operations, focused on the adaptation (modeling) and immediate application (execution) of existing OPLANs (implemented through related OPORDs and sometimes modified/added through FRAGOs, with specific evaluations and feedback), which influences the plans and orders that will be issued in the future; future operations, involving newly established objectives, actions and priorities (by the specifics of the new missions received by the subordinate forces) and materialized in very well-founded and modeled plans and orders of operations along the way, to successfully achieve the final operational state [72; 73].

Figure 13 presents an overview of operational logistics planning at tactical and/or joint levels. All elements in the figure are based on NATO specifications regarding the organization and conduct of this process (integrated into operational planning) in a national and multinational context, according to the level at which it is carried out, namely strategic, operational (joint), and tactical [72]. According to our approach, the macro component of operational logistics planning targets the entire mechanism specific to the tactical/or joint echelon at which it is carried out, integrating the micro side appropriate to the areas of logistical support to be provided to the respective combatant force.

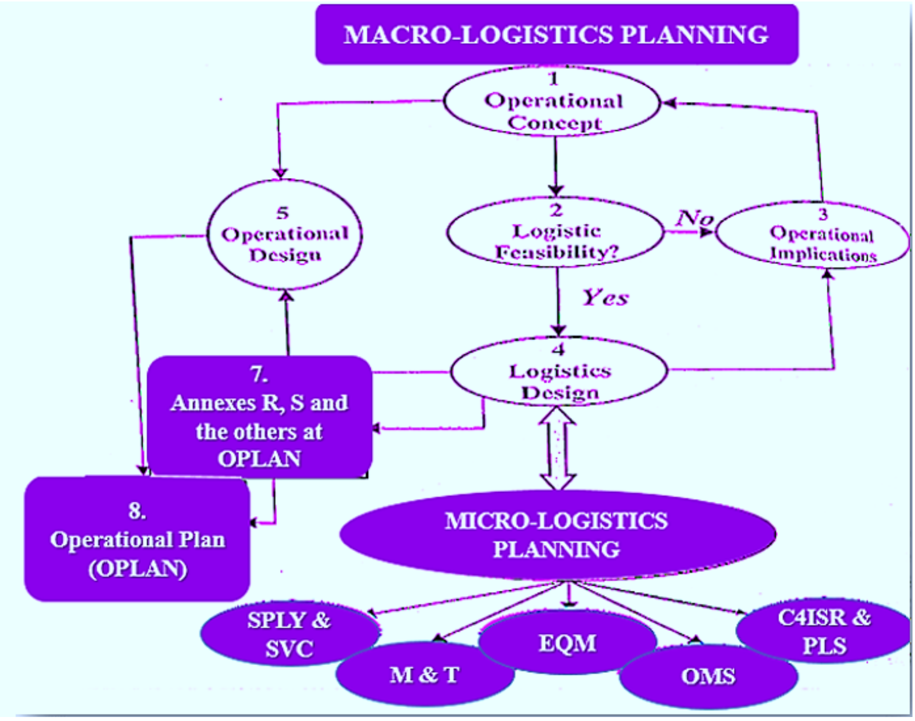


Fig. 13 The generic mechanism of operational logistics planning at tactical and/or joint level [9]

Legend:

- ✓ *SPLY* & SVC = Supply and Services;
- ✓ M & T = Movement and Transportation;
- ✓ EQM = Equipment maintenance;

- ✓ Operational Medical Support (OMS);
- ✓ C4ISR *& PLS = Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C^{4}ISR)* and Protection of the Logistics Structures (PLS).

Experience in the field reveals that, in the process of planning operational logistical support, integrated into the combat force mission planning mechanism, according to the analysis and evaluation of experts, the "Military Logistics Network Planning System" - MLNPS system can be used, through which, based on effectively simulated events, supply requests are processed according to the dynamic demands of fighters and equipment. This action will continue, so that following the interactive simulation and adjustment of the MLNPS network, the effective, appropriate, sufficient, and resilient logistics footprint can be identified in a short time, per the requirements resulting from the operational scenarios, staged [74].

Therefore, logistics planning in its known fields involves military logisticians who are perfected and experienced through proactive, anticipatory, and flexible thinking, vision, and action, who possess advanced capabilities for correlating and harmonizing the requirements for supporting operational forces with the availability and visibility of the resources that must be provided, depending on the particularities of the missions received, the specificity of the operational environment, the time available and the constraints that may arise as a result of the emergence and manifestation of risk and uncertainty factors. To this end, the judicious planning of operations specific to operational logistics requires a continuous exchange of adequate information (some even classified), necessary primarily for conducting transactions of goods and services between economic operators in the area of military actions and the beneficiary combatant structures [75].

The limitations that may arise, from our point of view, in planning the provision of the requested logistical support (during the preparation of the operation and/or during its conduct) are based on constraints concerning: the insufficiency of the resources necessary to fully cover the deficits reported by the tactical and/or joint-level operational structures, reduced sources of supply and/or service provision; significant losses predicted, as a result of the possibility of the enemy striking their own operational, incompletely protected logistical capabilities, etc. Under these conditions, the skill of logistics managers and subordinate specialists (logistics) consists in allocating the available resources by: the priorities of each operational force, according to the mission received; its place and role in the tactical and/or joint device; the deficits found, reported to the higher echelon and the sources (facilities) made available; the protection measures that must be implemented during supply-distribution operations (reception, transportation, storage, handling, delivery, specific information flows), etc.

Future functional development efforts in the face of an increasing diversity of threats oblige command and execution logisticians to flexibly manage the capabilities available to adequately support operational forces engaged in defense and/or expeditionary operations. Plans and orders for the preparation and conduct of tactical and/or joint operations are based on the projection (planning) of the related logistical potential, which can undoubtedly impose certain action (operational) limits. However, here the skills of logistics managers would also come into play, who through proactive, anticipatory, creative, and adaptable actions could determine the supplementation of the facilities (capabilities) to support combat forces by using other military and civilian sources in the area of operations (established by the higher echelon or identified and exploited with its agreement). At the same time, logistics specialists could act complementary (implementing planning procedures and tools or suggesting future operational actions), to balance and adjust the sufficiency of resources, by: *using high-performance equipment and fire systems; accumulating and pre-positioning protected support stocks for tactical expeditionary structures; operational restructuring of forces or groups of tactical forces while maintaining operational objectives (by virtue of the strike potential given by modern weapons systems in the equipment), to reduce the volume of logistical support granted to them [76] (for example, in the French army, in the immediate future, there will be a partial reduction of tank and infantry regiments in favor of expanding those profiled in long-range artillery, cyber actions or the use of drones; delaying offensive and/or expeditionary operations (tactical and/or joint) until the effective and sufficient procurement and provision of the resources and logistical services necessary for achieving operational success by the combat forces engaged,* etc. [77]. In line with what has been presented, experts believe that in the planning processes at the tactical and/or joint levels, it is necessary to identify military and non-military structures (such as economic operators, suppliers of goods or service providers, etc.) that can be engaged in complementary logistical support activities for multi-domain operations, even in less accessible areas [78].

Operational experience demonstrates that, even when a commander's strategy and tactics are sound, adequate combatant force logistics systems can quickly degrade, becoming unavailable shortly after a major operation has begun. Common problems, such as the intensification of inadequate use of strategic, operational (joint), and tactical reserves, disruption of specific supply chains, and insufficient information management, can reduce operational logistics availability by about 70% in the first 30 days of high-intensity armed conflict (as happened with the Russian invading forces in Ukraine) [79]. It follows, therefore, that proactive and anticipatory actions for planning logistical support, carried out by logistics management officers and their subordinates, by the (relevant) data and information received from the intelligence and operations structures (of tactical and/or joint commands) can determine in advance the augmentation of stocks and equipment in conditions of increased resilience so that the combatant structures benefit from an overwhelming operational advantage (with an even double combat potential) over the attacking forces of an adversary [80]. Figure 14 presents a variant of the gradual diminution of the operational logistical capabilities of one's own forces, as a result of enemy actions in a high-intensity conflict.

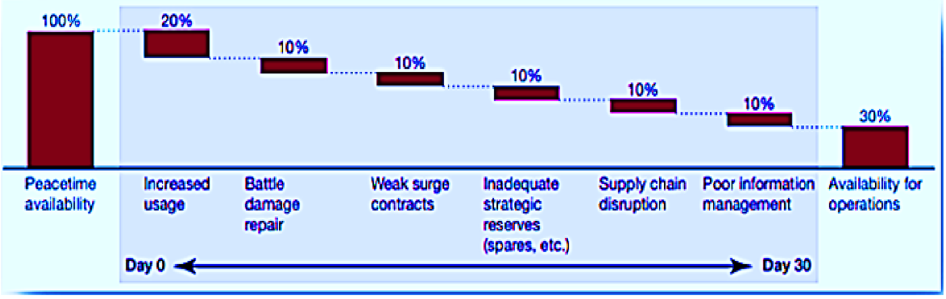


Fig. 14 A picture of the continuous diminution of the operational logistics potential of the (own) combat forces in a high-intensity conflict [80]

2.4. Implementation of new requirements in the field of training and professional development of logistics management and execution officers

The efficient functioning of operational logistics obviously requires the implementation of *new requirements both in the field of training and in the field of improving the training of officers who will perform leadership or execution duties of the necessary logistical support to combatant structures.* To this end, the lessons identified from the conduct of the armed conflict in Ukraine highlight the need for both the commanders of the combatant forces and the logistic personnel (leadership and execution under their command) to proceed with setting objectives, developing concepts and carrying out future actions to obtain organizational (logistical) performance by the missions received, especially in situations of crisis and armed conflict. For example, the essential elements of influence that have changed operational and logistical perceptions, as a result of the war waged on the territory of the Ukrainian state, are: *the intensive use of artificial intelligence; the predominance of air defense to the detriment of combat aviation (with invisible, reconnaissance surveillance aircraft, bombers, etc.); the establishment of stockpiles of materials sized at a higher level, due to increased operational requirements; the sharp development of the planning and conduct of operations (offensive and defensive) with combat and material transport drones (of various types; with the immediate prospect that drones for operational use will be programmed to select targets and act autonomously, without the intervention of operators); obtaining important data and information, adequate to the performance of missions (such as: maps, satellite photos, etc.) necessary for the geolocation of targets and the execution of reconnaissance (including logistics for the movement, disposition and resilient operation of logistical support structures) from open sources (Open source; OSINT) such as: internet; social networks; available Google applications; video clips; dialogue groups, etc.; decentralization of command of each combat and/or logistical support structure (noted beneficially in the Ukrainian defense forces, compared to the invading Russian ones)* [81].

Based on the above, we believe that a balanced combination of theory and logistics practice is necessary, according to the new requirements, taking into account (especially) the mistakes and deficiencies manifested in the Ukrainian theater of operations. From this, important lessons emerge, which must be implemented in the logistics educational process to train and develop the skills necessary for future logistics officers to understand and apply everything that logistical support to operational forces (at the tactical and/or joint levels) represents and will mean, engaged in complex (future) armed confrontations. All of these are based on the projection of the soldier of the future, correlated with the rapid progress of the modernization (primarily) of combat equipment and ammunition (which include unimaginable technological developments in the fields of automation, robotization, digitalization, and artificial intelligence), considered as determinants of the continuous transformation and change of methods and procedures of action, specific to operations carried out at all levels of military art (strategic, joint and tactical). Therefore, in these conditions, the advanced and continuous training of military logisticians (at all hierarchical levels) is very important, because the logistical support that will have to be provided to operational forces (with national and/or multinational status) will involve adequate modernism and as such, new ways of thinking and managerial action and/or execution (collaborative and cooperative) will be necessary, involving high-performance capabilities (in terms of logistics), which must be effectively and efficiently used, as well as very well protected (during their operation) from complex and continuous attacks by enemy forces, so that the missions of the combatant structures can be accomplished whenever and wherever they act offensively or defensively.

It would be important that shortly, each tactical combat structure in the Romanian Army goes through, in our opinion, a professional development process that, like in the armies of some advanced Western NATO states (USA, Great Britain, France), includes several stages with activities specific to modernization, preparation, training and the fulfillment of operational missions (offensive and defensive). Such a process will require both operational aspects and related logistical support: *specialized military personnel (leadership and execution) with enhanced skills; high-performance equipment and weapons systems; automated, robotic, digitalized, and sufficiently protected means for transport, storage, camping, maintenance, medical support; advanced means and systems for protection against attacks of any kind, including cyber attacks, etc. Some of these resources exist, and others are to be acquired (through: training and education of human resources; acquisitions and/or modernization of technical and material resources; procurement of advanced systems for visibility and protection,* etc.).

3. CONCLUSIONS

Modern operational logistics is a continuous cyclical process, which is carried out from the moment of receiving the mission until the moment of making the decision and, thereafter, during combat actions until the cessation of all activities and even for a period thereafter, during the transition phase. The characteristics of conflicts and situations of instability highlight risks and threats of a military and economic nature with an impact on the infrastructure of the areas and/or theaters of operations and other implications, which requires the provision of adequate and timely logistical support for the successful accomplishment of the missions received by the combat forces engaged in tactical and/or multi-domain operations. In this context, it is easy to explain why it is necessary to use operational logistics management to achieve the optimal direction of logistical resources appropriate to achieving operational objectives and the success of military actions. Logistics managers and their subordinates have extremely complex missions in the preparation and conduct of operations of the combat forces of the future.

Current changes, actions, and transformations in the military domain bring to light new challenges and dilemmas, involving ensuring an optimal balance between the need to have well-trained and modern troops, the significant number of missions, and increasingly limited resources. Thus, in the resulting situation, logistics stocks must be reduced, the quantities to be transported must be reduced, and the reaction time must be significantly shortened. Consequently, the transformation of military operational logistics is perceived not only as a central point in the future of logistical support but also as a lever for the effort of combat forces to ensure the appropriate balance between the state of readiness and their continuous functional modernization. The reaction of logistics decision-makers must respond to these challenges, which leads to the need to examine how military logistics transformation and decision-making can best respond to current circumstances and demands, dominated by the continuous adaptation of capabilities to new sustainability requirements.

In order to achieve their tactical operational goals of a logistical nature, the aforementioned specialists need solid training, competence, responsibility, a lot of initiative, and perseverance. Consequently, particularly important in the economy of military actions, shortly, is the reduction of the “volume” of operational logistics by reducing the duration of supply/resupply flows appropriate to the areas and/or theaters of operations. This is relatively easy to define, but much more difficult to achieve. The greatest challenge for logisticians of the future will be to ensure a versatile, interactive logistics system, capable of effectively and efficiently supporting military operations, prepared and deployed in increasingly complex operating environments.

Therefore, the increase in operational logistics performance is and will be given by the magnitude of technological advances that will take place in the future, such as: *the realization of 3D 6D printing; the use of alternative energy sources; the use of robotic systems intended for the evacuation of the wounded; production-delivery of modern combat equipment, as well as of developed unmanned technical systems (air and ground) necessary for a tactical and/or joint force to increase the facilities related to resupply operations (of materials), maintenance, repairs and medical support. It follows, therefore, that the use of these technologies will determine the improvement of logistical functions, concomitantly with the reduction of risks in the processes of providing operational logistical support.*

Under these conditions, it is obvious that the operational forces of the future will benefit, in addition to options for decentralizing tactical and/or joint maneuvers, from modularly organized, flexible and adequately protected tactical logistical entities (structures), which have transportation, storage, warehousing, maintenance facilities and apply effective, efficient and resilient logistical support procedures. To achieve these goals, very well-trained logistical leaders will be involved, who will plan and carry out advanced and complex logistical support operations, given the limited resources in the areas of operations within the theater of joint operations.

The transformation of operational logistics of combat forces will also depend in the future on: *logistics based on real-time distribution, considered to be the most important product of the revolution in the field of operational logistics; elimination of intermediate links in the supply chain, which will determine the creation of a flexible logistics system and the reduction of financial pressures, as well as other facilities (such as: elimination of excess stocks; a much faster response to the requirements of military beneficiaries; identification and application of the best solutions to reduce the impact of possible failures, before they occur); modernization of equipment, which involves their proactive monitoring and diagnosis, as well as adequate preparation of maintenance structures for interventions and evacuations*. Achieving these objectives requires rethinking logistics processes, organizational restructuring of the profile, development of new sensor systems and diagnostics of modern equipment, implementation of an advanced information, support, command and control system, but also the existence of very well-trained (logistics) personnel, capable of operating with the expected performance.

As stated, future operations imply that, at the tactical and/or joint level logistics systems, specific decisions regarding the allocation of limited resources should be based on the size of the requests, the availability of resources, the time available to execute effective and resilient support actions depending on the robustness of each existing and possibly augmented logistics organization. This implies optimal planning of the logistical support of future military operations to reduce risk and uncertainty as much as possible, which requires creativity, organizational skills, and innovation on the part of the logistics personnel (management and execution) involved.

Current and future military challenges are causing state and Alliance decision-makers at various levels to place increasing emphasis on future national and multinational defense requirements. This requires highly trained operational military leaders and (subordinate) logistics managers with the skills necessary to adapt immediately to the evolving and changing needs of the future joint theater of operations. The logisticians of the future army will be the leaders of the command and execution structures of major importance on the battlefield. They must delegate, adapt, take risks, and invest energy and effort to accomplish the complex missions assigned to them. As heads of the J4, G4, A4, N4, S 4 logistics modules (or their components), as well as commanders (deputies or chiefs of staff) of the logistics support execution structures (from the joint to the lower tactical level), they must be experts in understanding, hierarchically transmitting the real logistical situation in the field, proceeding further to carry out the planning processes and providing the logistical support requested by the combat forces.

The further development and modernization of operational logistics, according to the new requirements revealed by the war of the future, will be able to allow the combat and support structures, at the tactical and joint levels, to become more prepared, mobile, flexible, effective and efficient under the objectives and requirements of the future missions received.

For a prospective analysis, it results that operational military logistics will be modernized by reconfiguring the integrated logistics systems of the combat forces at the tactical and joint levels, as a result of the evolution of equipment, information technology, and the functional optimization of combat and support structures, for a greater and more precise reaction capacity in any circumstances, according to the missions received within the framework of multinational operations carried out on national territory or outside it within and under the aegis of NATO.

REFERENCES

[1] Strategic Studies Institute, US Army College (2024), *Annual Estimate of the Strategic Security Environment*, Strategic Research and Analysis Department, 58

[2] International Institute for Strategic Studies (IISS), *Building Defense Capacity in Europe: An Assessment Introduction: How Ready?,* Washington Office, USA, 8th November 2024, https://www.iiss.org/publications/strategic-dossiers/introduction-how-ready/, accessed on 10.01.2025

[3] Monaghan S. et al., *Is NATO Ready for War? An Assessment of Allies' Eorts to Strengthen Defense and Deterrence since the 2022 Madrid Summi,* Center for Strategic and International Studies, June 2024, 5-6; 8-12; 12-17

[4] The International Institute for Strategic Studies-IISS (2024), *Building Defence Capacity in Europe: An Assessment,* Arundel House, London, UK, 5-7

[5] International Institute for Strategic Studies-IISS (2024), *Building Defense Capacity in Europe: An Assessment Introduction: How Ready?,* Washington Office, USA, 8th November, https://www.iiss.org/publications/strategic-dossiers/introduction-how-ready/, accessed on 10.01.2025

[6] Sollfrank A. & Boeke S. (2024), *Enablement and Logistics as Critical Success Factors for Military Operations: Comparing Russian and NATO Approaches,* in The RUSI Journal Volume 169, Issue 7, 19-22

[7] Lieutenant Colonel Riga H. (2018), French Army Transformation Delivery Division, *Towards an Integrated and Expeditionary Operational Level Logistics,* Joint Warfare Centre, The Three Swords Magazine 33/2018, 27, https://www.jwc.nato.int/images/stories/threeswords/Operational_Level_Logistics.pdf, accessed on 27.12.2024

[8] Cuadernos de Estrategia 211-B (2022), *The future of NATO after the Madrid 2022 summit,* Spanish Institute for Strategic Studies. Layout and Printing: Ministry of Defense, 15-17

[9] Minculete G, *Determinări relaționale privind modeernizarea logisticii operaționale* (2023), Editura Techno Media: Sibiu, 109-165; 109-110; 111; 144; 146; 150

[10] US Army, Department of Defense (2021), *Software Modernization Strategy*, November, Version 1.0, 6-9

[11] Medley M. (2022), *The critical data thread tying together the military supply chain, logistics, and equipment support,* July 26, https://militaryembedded.com/ai/big-data/the-critical-data-thread-tying-together-the-military-supply-chain-logistics-and-equipment-support, accessed on 04.12.2024

[12] North Atlantic Treaty Organization (2020), *Models and Tools for Logistics Analysis,* STO-TR-SAS-132, 1-24

[13] Michalska A. & Karpinska K. (2018), *Capabilities of the Unmanned Aerial Vehicles in Logistic Support,* Scientific and Technical Journal Safety & Defense 4 (1), 22-26; https://sd-magazine.eu/en/publications/2018-2/, accessed on 29.12.2024

[14] Congressional Research Service (2022), *Unmanned Aircraft Systems: Roles, Missions, and Future Concepts,* USA, July 18, 7, https://sgp.fas.org/crs/weapons/R47188.pdf, accessed on 06.12.2024

[15]Fenema C. P., Kampen T., Gooijer G., Faber N., Hendriks H., Hoogstrate A. and Schlicher L. (2021), *Sustaining Relevance: Repositioning Strategic Logistics Innovation in the Military,* Joint Force Quarterly 101, NDU Press, March 31, 3-7

[16] ATP 4-42, *Materiel Management, Supply, and Field Services Operations* (2020), Headquarters Department of the Army, USA, Washington, D.C., 02 November, 1-6 – 1-13

[17] Centre for Land Warfare Studies New Delhi (2018), *Revolution in Military Logistics: Lean, Sustainable, Reliable Supply and Maintenance Chain (S&MC).* Seminar Report. KW Publishers Pvt Ltd New Delhi, March 17, 23-27

[18] Italian Army Headquarters (2019), *Future Operating Environment Post 2035 – Implications for Land Forces,* General Plans Department Plans Office, 33-34

[19] Llopis-Albert, C., Rubio, F. & Valero, F. (2021). *Impact of digital transformation on the automotive industry. Technological Forecasting and Social Change*, 162

[20] Lee, R. (2021) *The Effect of Supply Chain Management Strategy on Operational and Financial Performance*. Sustainability, 5138, 1-19

[21] “MILITARY”: https://www.vectorstock.com/royalty-free-vector/military-army-forces-featuring-soldiers-weapons-vector-51580502, accessed on 06.01.2024

[22] DTResearch (2021), *Digitization Improves Logistics for the Military,* https://dtresearch.com/blog/2021/09/23/digitization-improves-logistics-for-the-military/, accessed on 09.01.2025

[23] Zabrodskyi M., Watling J., Danylyuk V.O. and Reynolds N., *Preliminary Lessons in Conventional Warfighting from Russia’s Invasion of Ukraine: February-July 2022,* Royal United Services Institute for Defence and Security Studies Whitehall:

London SW1A 2ET United Kingdom, 1-3; 64-66

[24] Machi V. (2022), *Inside the multinational logistics cell, coordinating military aid for Ukraine,* https://www.defensenews.com/global/ europe/2022/07/21/ inside-the-multinational-logistics-cell-coordinating-military-aid-for-ukraine/, accessed on 07.01.2025

[25] Britzky H. and Liebermann O. (2023), *Ukraine is burning through ammunition faster than the US and NATO can produce it. Inside the Pentagon's plan to close the gap,* CNN, February 17, 2023, https://edition.cnn.com/2023/ 02/17/politics/us-weapons-factories-ukraine-ammunition/index.html, accessed on 08.012.2025

[26] Defense România, *Cu toți ochii pe HIMARS, succesul contraofensivei Ucrainei va depinde de logistică: Blindate TEHEVAC, cisterne de combustibil și camioane,* 21 aprilie 2023, https://m.defenseromania.ro/ cu-toti-ochii-pe-himars-succesul-contraofensivei-ucrainei-va-depinde-de-logistica-blindate-tehevac-cisterne-de-combustibil-si-camioane_622296.html, accessed on 02.12.2024

[27] Council of the European Union (2019), *Military Requirements for Military Mobility within and beyond the EU,* Brussels, 19 July, 9-11

[28] Lange N. (2023), *How to beat Russia What armed forces in NATO should learn from Ukraine's homeland defense,* Globsec. Ideas Shaping the World: Bratislava, Slovakia, February, 27-29

[29] *Nimeni nu poate auzi sau vedea atacul apropiindu-se". Israelul are drone cu bombe ce nu fac zgomot sau fum. Pot căra o tonă de muniție,* 02.02.2023, https://www.digi24.ro/stiri/externe/nimeni-nu-poate-auzi-sau-vedea-apropiindu-se-un-atac-israelul-are-drone-cu-bombe-ce-nu-fac-zgomot-sau-fum-si-pot-cara-o-ona-2237117, accessed on 09.01.2025

[30] Turner J. (2018), *How autonomous delivery drones could revolutionize military logistics*, Army Technology, October 8, https://www.army-technology.com/features/autonomous-delivery-drones-military-logistics/, accessed on 08.01.2025

[31] Finabel, *The Use Of Military Drones: The Impact On Land Forces And Legal Implications,* 14 January 2021, https://finabel.org/the-use-of-military-drones-the-impact-on-land-forces-and-legal-implications/, accessed on 09.01.2025

[32] Tomkins R. (2016), *Estonian military tests unmanned ground vehicle. A modular unmanned ground logistics vehicle has completed three days of testing on a simulated battlefield,* Tallinn, Estonia, 26 mai, https://www.upi.com/ Defense-News/2016/05/26/Estonian-military-tests-unmanned-ground-vehicle/2191464281640/, accessed on 10.01.2025

[33] Barnard S. (2022), *Politics • Armed Forces • Procurement •*

Technology • French Army Acquisition Programmes • European Artillery Requirements • Dismounted Situational Awareness, 2022 European Security & Defence, https://www.academia.edu/82175365/Politics_Armed_Forces_Procurement_Technology_French_Army_Acquisition_Programmes_European_Artillery_Requirements_Dismounted_Situational_Awareness, accessed on 12.01.2025

[34] Borchert H., Schütz T., Verbovszky J. (2024), Editors, *The Very Long Game 25 Case Studies on the Global State of Defense AI*, Springer, Switzerland, 54-55

[35] Milrem Robotics (2024), *The THEMIS UGV*, https://milremrobotics.com/, accessed on 30.12.2024

[36] Aitoro J. (2019), *US logistics boss talks risks to the supply chain and protective measure,* https://www.defensenews.com/interviews/2019/10/28/us-logis tics-boss-talks-risks-to-the-supply-chain-and-protective-measures/, accessed on 28.12.2024

[37] Ekman, Elle M. (2017), *Simulating sustainment for an Unmanned Logistics System concept of operation in support of distributed operations,* Monterey, California: Naval Postgraduate School, 6 -18

[38] Adrian Gabor (2023), *Ministrul Apararii Confirma o Decizie de ultimă oră legata de Armata Română, Razboiul din Ucraina,* Feb. 23.

[39] USB Common Access Card Reader (Non-TAA) (2015), *Smart Card Reader for CAC, PIV and Secure Access*, 1-2

[40] DTResearch (2021), *Digitization Improves Logistics for the Military,* September 23, https://dtresearch.com/blog/2021/09/23/digitization-improves-logistics-for-the-military/, accessed on 09.01.2025

[41] NATO Standard AJP-4 (2018), *Allied Joint Doctrine for Logistics*, Edition B, Version 1, December 2018, pp. 2-15 – 2-18; 5-3 – 5-4

[42] NATO Standard AJP-3.13 (2021), *Allied Joint Doctrine for The Deployment and Redeployment of Forces*, Edition A, Version 1 May , 3-1 – 3-11; 4-1 – 4-13

[43] ATP 3-35 (FM 3-35) (2018), C2, *Army Deployment, and Redeployment*, Headquarters Department of the Army Washington, DC, 10 October, 1-1 – 4-11

[44] Shaw Myra (2016), *Reception, Staging, Onward Movement & Integration (RSO&I) ppt,* Slide No 4, https://slideplayer.com/slide/ 4882996/, accessed on 05.01.2025

[45] Lieutenant Colonel Rengel V., Lieutenant Colonel Ortega Humelsine E. (2022), *Logistic challenges and Lessons Learned throughout the WFC Training and Certification exercise,* HQ NRDC-ESP, Journal I #Twelve Nations One Team, 36-38

[46] NATO Standard AJP-4.6 (2018), *Allied Joint Doctrine for The Joint Logistic Support Group,* Edition C Version 1, December, 2-3 – 2-5; p. 4-1

[47] Lt.col. Cornett A. (2020), Multinational Operations. *Joint*

Logistics Support Group offers effective role with allies, partners, Army Sustainment, January-March, 45-52

[48] Rautio S. & Valtonen I. (2022), *Supporting military maintenance and repair with additive manufacturing,* Sciendo, Journal of Military Studies-Sciendo, 1(1), 1-14

[49] Reddy Ravinder P. & Devi Anjani P. (2018), *Review on the Advancements to Additive Manufacturing-4D and 5D Printing, International Journal of Mechanical and Production Engineering Research and Development* (IJMPERD), Vol. 8, Issue 4, Aug, 397-402

[50] Vasiliadis, A.V, Koukoulias, N. & Katakalos K. (2022), *From Three-Dimensional (3D)-to-6D-Printing Technology in Orthopedics: Science Fiction or Scientific Reality?* J. Funct. Biomater, 13, 1-6

[51] Kress M. (2016), *Operational Logistics: The Art and Science of Sustaining Military Operations.* Second Edition. Springer. 2nd ed. 2016 edition. Best Sellers Rank. USA, New York, 12-17

[52] Rautio S., Valtonen I. (2022), *Supporting military maintenance and repair with additive manufacturing,* Sciendo, Journal of Military Studies-Sciendo, 1(1), 6

[53] DTResearch (2021), *Digitization Improves Logistics for the Military,* September 23, https://dtresearch.com/blog/2021/09/23/digitization-improves-logistics-for-the-military/, accessed on 08.01.2025

[54] Council of the European Union (2019), *Military Requirements for Military Mobility within and beyond the EU,* Brussels, 19 July, pp.11-13

[55] Coe J., Dunbar C., Epps K., Hagensee J. & Moore A.L. (2019), *A low-altitude unmanned aerial vehicle (UAV) created using 3D-printed bioplastic*. Journal of Unmanned Vehicle Systems, Vol. 7, 118-128

[56] NATO Standard AJP-4.10 (2019), *Allied Joint Doctrine for Medical Support,* Edition C, Version 1, September, 1-7 – 1-13; 3-17

[57] Colonel Ibañez Ruiz Jacinto T. (2022), Lieutenant Colonel Moreno Santatecla Juan O., *Tactical and strategic medical evacuation in a warfighting corps scenario,* HQ NRDC-ESP, Journal I #Twelve Nations One Team, 43-45

[58] ATP 4-02.13 (2021), *Casualty Evacuation,* Headquarters Department of the Army Washington, DC, 30 June, 1-3 – 1-8

[59] Christian P.van Fenema, Kampen T., Gooijer G., Faber N., Hendriks H., Hoogstrate A., and Schlicher L. (2021), *Sustaining Relevance: Repositioning Strategic Logistics Innovation in the Military,* Joint Force Quarterly 101, NDU Press, March 31

[60] Ashurst T. and Beaumont D. (2020), *Logistics Interoperability, Deterrence and Resilience - Why Working as Allies Matters now More than Ever,* https://logisticsinwar.com/2020/06/21/logistics-interoperability-deterrence-and-resilience-why-working-as-allies-

matters-now-more-than-ever-2/, accessed on 13. 01.2023

[61] Brandon-Jones E., Squire B., Autry C.W. & Petersen K.J. (2014), *A contingent resource-based perspective of supply chain resilience and robustness.* Journal Supply Chain Management, 50, 60-70;

[62] Christopher M. & Peck H. (2004), *Building the resilient supply chain*. Journal Logistic Management, 15, 5-12

[63] Ponomorov S. & Holcomb M. (2009), *Understanding the concept of supply chain resilience*. Journal Logistic Management, 20, 135-140

[64] Ryczynski, J. & Tubis, A.A. (2021) *Tactical Risk Assessment Method for Resilient Fuel Supply Chains for a Military Peacekeeping Operation*. Energies MDPI, 14, 4679, 3; 16-22

[65] Ivanov D. & Schönberger J. (2019), *Supply Chain Risk Management and Resilience: A Decision-Oriented Introduction to the Creation of Value,* In book: *Global Supply Chain and Operations Management,* 7, 455-479

[66] Singhal P., Agarwal G. & Lal Mittal M. (2021), *Supply chain risk management: Review, classification and future research directions*. Int. J. Bus. Sci. Appl. Manag. 2011, 6, 32-39

[67] North American CRO Council (2021), *Resiliency and Risk Management*, December, 1-6

[68] USA, Department of Defense (2022), *Securing Defense-Critical Supply Chains An action plan developed in response to President Biden's Executive Order 14017,* February, 6-7

[69] NATO Standard APP-28 (2019), *Tactical Planning for Land Forces,* Edition A, Version 1, November, 2-19

[70] Skoglund P., Listou, T. & Ekström T. (2022), *Russian Logistics in the Ukrainian War: Can Operational Failures be Attributed to logistics*? Scandinavian Journal of Military Studies, 5(1), 103; 99-110

[71] Minculete G. (2020), *Relation approaches to the resilience of operational logistics,* International Scientific Conference Proceedings 2nd Edition Military 24 Strategy Coordinates Under The Circumstances Of A Synergistic Approach To Resilience In The Security Field, Romanian Military Thinking International Scientific Conference, Military Theory and Art, 262-273

[72] NATO Standard AJP-5 (2019), *Allied Joint Doctrine for The Planning of Operations,* Edition A, Version 2, May, 1-5 – 1-6

[73] NATO Standard APP-28 (2019), *Tactical Planning for Land Forces,* Edition A, Version 1, November, 1-4 – 5-2

[74] Rogers B.M., McConnell M.B., Hodgson J.T., Kay G.M., King E.R., Parlier G. and Thoney-Barletta K. (2018), *A Military Logistics Network Planning System,* Military Operations Research, Published By: Military Operations Research Society, 5-24

[75] Council of the European Union (2019), *Military Requirements for Military Mobility within and beyond the EU,* Brussels, 19 July, 13-14

[76] United States Army War College (2020), *How the Army Runs. A Senior Leader Reference Handbook,* January 29, 3-35 – 3-39

[77] United States Army War College (2020), *How the Army Runs. A Senior Leader Reference Handbook,* January 29, 3-5 – 3-28

[78] Italian Army Headquarters (2020), *Future Operating Environment Post 2035 - Implications for Land Forces,* General Plans Department Plans Office, 33-34

[79] Dalsjö R., Jonsson M. & Norberg J. (2022), *A Brutal Examination: Russian Military Capability in Light of the Ukraine War,* Survival Global Politics and Strategy, Vol 64, no 3, June-July, 10-17

[80] Partner S., H., Mark B. & Dagher S. (2016), *Resilient and agile Making logistics a combat multiplier for GCC armed forces,* Strategy&, PwC. Disclaimer, 4-5

[81] News.Ro (2023), *Lecțiile războiului din Ucraina pentru orice conflict viitor,* 20.02, https://spotmedia.ro/stiri/eveniment/lectiile-razboiului-din-ucraina-pentru-orice-conflict-viitor, accessed on 13.-14.01.2025

NATO-EU COOPERATION IN RESPONSE TO THE CHALLENGES OF EMERGING AND DISRUPTIVE DEFENSE TECHNOLOGIES

Daniel DOICARIU, Alexandru-Iulian ACSINTE

"Carol I" National Defence University, Bucharest, Romania

The lessons learned in the Ukraine-Russia conflict, the security relations between the EU-NATO states and the U.S., the appearance of incisive emerging and disruptive technologies in China are some of the elements that determined a strong cooperation between NATO and the EU. In this scientific research, we aimed to gain an overview of NATO-EU cooperation on responding to the challenges of emerging and disruptive technologies in the defense field. There are two directions of analysis, on the one hand countering the effects of emerging and disruptive technologies against NATO and EU states to ensure sustainable security, and on the other hand, catching up with states such as China and Russia, especially in the field of defense.

Key words: *emerging technologies, disruptive technologies, defense and security, research, cooperation, budgets.*

1. CONCEPTUAL CLARIFICATIONS

The concept of *"disruptive technologies"*, recognized in the majority of specialized papers (National Research Council: 2010, p.xv) as having been launched in 1995 (Chrystensen, Bowell: 1995, p.4) and further developed in 1997 (Chrystensen: 1997) by Clayton M. Chrystensen, has over time become the main subject of numerous publications and specialized articles. These more or less scientific analyses have brought to the foreground the parallels with another association of terms, at least as common in the last decade, namely *emerging technologies* (Klasa, Trump, Linkov, Lambert: 2020, p.26).

In Chrystensen's view disruptive technologies are those technologies that *"introduce a very different package of attributes from the one mainstream customers historically value"* (Chrystensen, Bowell: 1995, p.45), but the timeliness of the theory has often been contested (Markides: 2006), as the author himself admitted in an article in the Harward Business Review

(Christensen, Raynor, McDonald: 2015, p.50).

On the other hand, emerging technologies are technologies *"whose development and application are not completely realised or finished"* (Rotolo, Hicks, Martin: 2015) and whose potential for use is not completely determined at present.

Since both at the NATO level, through the *"NATO 2022 Strategic Concept"* (NATO:2022, p 5) and at the EU level, in *"A Strategic Compass for security and defence"* (Council of the EU: 2022, p 11) document also approved in 2022, Emerging and Disruptive Technologies (EDT) are addressed as a unitary issue, but in this article we will not discuss the interdependence between them.

In our opinion, the approval of the above mentioned documents by the two major international organizations is not a direct consequence of the start of the war between Russia and Ukraine, but the adoption of doctrinal level measures is part of the broader context of the necessary reaction to Russian aggression.

As we shall see, the lessons learned from the Ukrainian War have determined the leaders of European and North American nations to prioritize technological development in general, and EDT in particular, with an emphasis on their applicability to the military domain.

At the same time, in order to delimit the conceptual framework characterized by different meanings of the terms *"disruptive"* and *"emerging"*, in this article we adopt the definitions used by the *NATO Science&Technology Organisation*, as follows (NATO STO: 2020, p 13):

- ***emerging technologies***: represent those technologies or scientific developments which are expected to mature in the period 2020-2040 and which are not currently widely used or whose effects on the North Atlantic Alliance (Alliance) are not fully known;
- ***disruptive technologies***: these are those technologies or scientific discoveries that are expected to have a major, perhaps even revolutionary, effect on NATO's defense posture and the way the Alliance will perform its missions in the period 2020-2040;
- ***converging technologies:*** a mix of technologies that are combined in an innovative way to create a disruptive effect.

NATO's official website lists three examples of emerging and disruptive technologies of interest, namely *"artificial intelligence (AI), autonomous systems and quantum technologies"* (NATO: 2024), and the Strategic Compass completes the list with *"advanced propulsion, bio- and nano-technology and new materials and industrial capacities"* (Council of the EU: 2022, p 34).

Who will lead the next wave of strategically important technologies is the question that creates uncertainty about future security. Figure 1 illustrates the evolution and prediction of emerging and disruptive technologies on a time axis, based on data from OMPI, MIT, WEF, OCDE, etc.

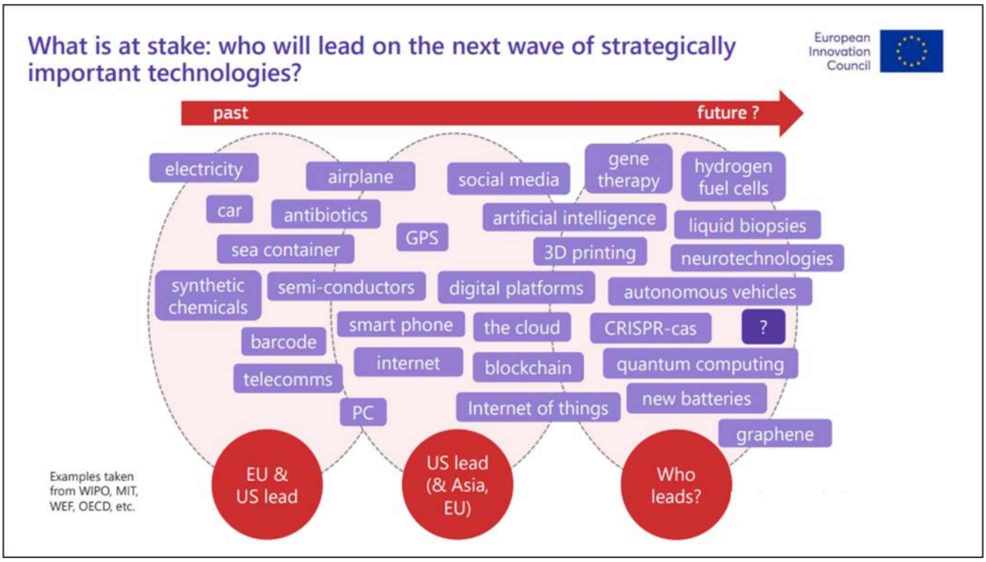

What is at stake: who will lead on the next wave of strategically important technologies?

Fig. 1. Temporal evolution of emerging and disruptive technologies. (Sequeira: 2021, p 4)

Head of the European Defense Agency's (EDA) Technology and Innovation Division, Panagiotis Kikiras, points out, *"in the end no matter how you define EDTs, you end up with a pretty similar list of technologies"* (EDA: 2024) and these provide a solid basis for cooperation between different institutional actors in NATO and the EU.

2. NATO - EU COOPERATION ON EMERGING AND DISRUPTIVE DEFENSE TECHNOLOGIES

Obviously, **NATO**'s interest in holding the technological advantage over adversaries has been a permanent preoccupation, but concrete steps to develop and adapt the Alliance to a new paradigm of

EDT use have been taken since 2019, by:

- adoption of a *"roadmap"* for EDT at the NATO Summit in London 2019 (NATO: 2019);
- the approval of *NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies* in February 2021, which lists 7 key areas for innovation activities: *"artificial intelligence (AI), data and computing, autonomy, computing systems, biotechnology and biological augmentation systems, hypersonic technologies and space"* (MCID: 2022, p 2). In addition to the technologies listed above, NATO currently attaches equal importance to *"energy and propulsion, and next-generation communication"* (NATO:2024);
- the launch *Defence Innovation Accelerator for the North Atlantic* (DIANA) at the NATO Summit in Brussels – 2021 (NATO: 2021), through which, to consolidate NATO's technological advance, the allied countries collaborate with the private sector to adopt and integrate new technologies and to form standards (DIANA:2025);
- the establishment of the *NATO Innovation Fund,* on a voluntary basis, to support investment in emerging and disruptive technologies start-ups in areas critical to Allied security (NATO:2024), with a capitalization of €1 billion. Currently, 24 countries are partners in this investment fund, but not including the US, France and Canada.

In order to lead and coordinate the broad field of EDT, a number of organizational entities with specific tasks operate at NATO level, such as the NATO Innovation Board, NATO Advisory Group on Emerging and Disruptive Technologies, NATO's Data and Artificial Intelligence Review Board, NATO-Ukraine Innovation Cooperation Roadmap or the NATO Communications and Information Agency (NCIA), etc.

In the case of the EU, we observe the establishment and implementation of mechanisms and bodies with similar responsibilities:

- the EDA acts as a *"European defence cooperation 'hub' "* (EDA:2025), supporting all member states to develop their military assets;
- The European Defence Fund (EDF), operating under the auspices of the European Defence Agency (EDA) was set up to support investment in joint research and

development of defense-related products and technologies (Official Journal of the European Union: 2021/697), with a budget of € 7.953 billion for the period 2021-2027 (EDF:2025);

- other institutions with a determined role for EDT are the *European Institute of Innovation&Technology* (EIT) and the *European Innovation Council* (EIC);
- the *Digital Europe Program* (DIGITAL), approved by the European Parliament to *"support the digital transformation of industry and to foster better exploitation of the industrial potential of policies on innovation, research and technological development"* (Official Journal of the European Union: 2021/694) has a planning horizon of 2021 - 2027 and a budget of €7,558 million, reflecting the main policy areas of *"High Performance Computing; Artificial Intelligence; Cybersecurity and Trust; Advanced Digital Skills; and Deployment and Best Use of Digital Capacities and Interoperability"* (Official Journal of the European Union: 2021/694).
- beginning in March 2024, the *Strategic Technologies for Europe Platform* (STEP) will become operational, aiming to boost investment in strategic technology start-ups. The platform is set to receive a budget of €300 million in 2025, with projected funding reaching approximately €900 million over the following three years (UEFISCDI: 2025).

This reflects the shared interest of the two major international organizations in the advancement of EDTs, 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.

Intensified cooperation between NATO and the EU is a critical objectives highlighted in official documents at the highest level, while the NATO-EU Strategic Partnership is considered *"crucial to maintaining security and stability in the Euro-Atlantic area, and to protecting citizens in Europe and beyond"* (Council of the EU:2024). According to the Strategic Compass, although *"a stronger and more capable EU in the field of security and defence will contribute positively to global and transatlantic* *security"* (Council of the EU: 2022, p 5), NATO is the main pillar, being *"the foundation of collective defence for its members"* (Council of the EU: 2022, p 5).

On the other hand, the *NATO 2022 Strategic Concept* states that *"the European Union is a unique and essential partner for NATO"* (NATO:2022, 10), and in the chapter on common areas of collaboration, *"military mobility [...] emerging and disruptive technologies [...] countering cyber and hybrid threats"* (NATO:2022, 5) are mentioned.

Furthermore, the latest *Joint Declaration on EU-NATO Cooperation* stipulates the extension and intensification of cooperation *"to address in particular the growing geostrategic competition [...] emerging and disruptive technologies"* (Council of the EU: 2023, 12).

3. REVIEW OF DEFENSE BUDGETS IN NATO AND EU

In *"Innovation as Adaptation: NATO and Emerging Technologies"*, arguments are made for a new legislative framework, where large-scale innovations lead to greater adaptability, efficiency and solidarity, but gradual adaptation is too slow and rigid (Soare: 2021, p 1). The outbreak of war in Ukraine in 2022 has prompted an acceleration of these measures, at both political and military levels.

The decisions of NATO and EU leaders to support Ukraine have translated into financial efforts, support with military technology and equipment, humanitarian assistance, etc.

According to the *International Institute for Strategic Studies,* global defense spending increased to 7.4% in 2024 from 6.5% in 2023 and totals $2.46 trillion, maintaining the trend of growth from previous years (IISS: 2025). Relevant to this equation is the position of the USA, which accumulates a budget as large as the top 15 countries in the ranking, as shown in Figure 2.

Out of the total of 27 EU member states, four countries are not members of NATO (Austria, Cyprus, Ireland and Malta), and of the 32 NATO member states, two are located outside the European continent (USA and Canada).

Based on the assumption that the priorities of an organization and/or a state are directly proportional to the way in which financial resources are distributed, we have analysed the defence budgets for the period 2022 to 2024 at the North Atlantic Alliance and EU level.

Annual Reports on the NATO Common Funding level show a significant increase in defense spending, with a total of €2.6 billion in 2022 (NATO: 2022, p 2) and €3.18 billion in 2023 (NATO: 2023, p 2).

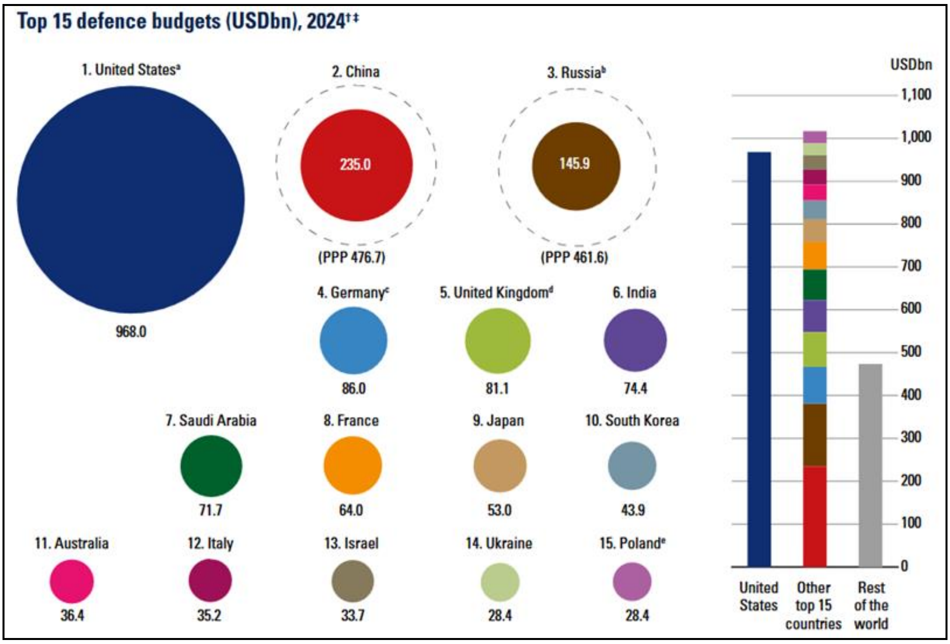


Fig. 2. Top 15 countries in the world by defense budget.
(IISS: 2025)

According to the NATO Secretary General's annual reports for 2022 and 2023, the fact that more and more member states have allocated at least 2% of GDP to defense is also reflected in the overall NATO budget: from 3 states in 2014, to 7 states in 2022 (Stoltenberg: 2022, p. 48), 11 states in 2023 (Stoltenberg: 2023, p. 50) and 23 states in 2024 (NATO:2024, p. 4).

Figure 3 shows that the economic and military strength of the US is also reflected in the significant contribution it makes to the annual defense budget allocation. The amounts allocated to defense by the US are almost double the total budgets of the other NATO states.

Detailed information on the distribution of financial resources by purpose (personnel, equipment, infrastructure, and others), as well as on activities directly related to emerging and disruptive technologies, is also available in the official reports (Figure 4).

NATO’s budgetary expansion has, almost inevitably, been mirrored by a similar trend of consolidation in EU spending and investment. Between 2021 and 2024, total defense spending by EU member states increased by more than 30%. More than 80% of total defense investments were allocated to new equipment and technology. In 2024, spending is estimated to have amounted to around €326 billion, representing about 1.9% of the EU GDP (Council of the EU: 2025) which shows that the EU is also getting closer to the 2% of GDP target set by the leaders of the North Atlantic Alliance (Figure 5).

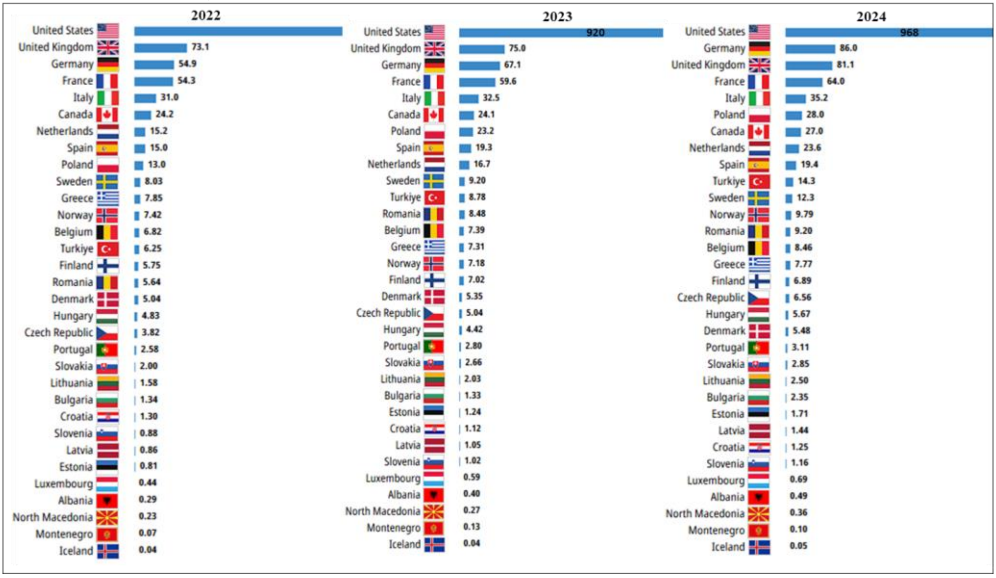


Fig. 3. Annual NATO defense budgets (USD billion)
(IISS: 2025)

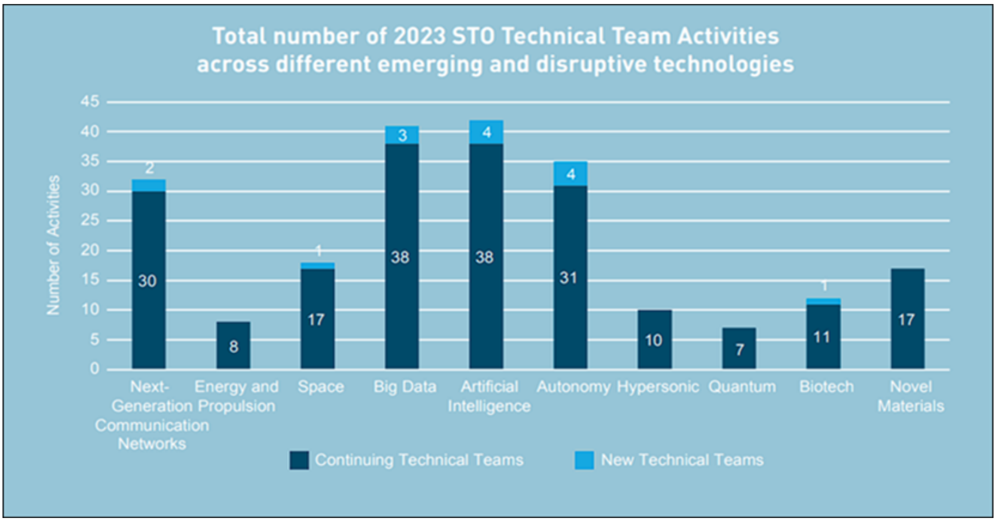


Fig. 4. NATO STO activities in 2023 for some of the EDTs
(Stoltenberg: 2023, p. 89)

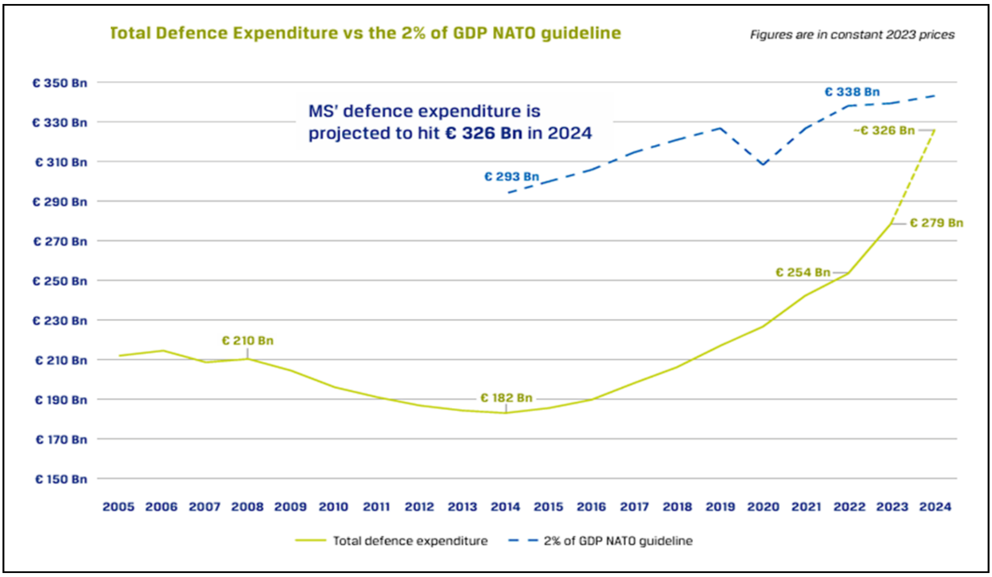


Fig. 5. Comparative evolution of NATO and EU defense budgets (CARD: 2024)

According to the *EDA report for the period 2023-2024*, financing for Defence Research and Development (D&R) has doubled since 2016, with a total of €11 billion in 2023 (EDA:2024, p. 3).

It is notable that the United States and China, overtake the EU Member States in terms of investment in defense R&D, highlighting the growing importance of this strategic activity. This reflects the urgent need to adapt military technologies to the new realities of modern warfare, in which enemies are increasingly technologically sophisticated. In this context, investment in research and development is not just a matter of technological superiority, but a necessity to maintain national security and to face possible conflicts with state or non-state actors with advanced technological capabilities. Therefore, in order for the European Union to remain relevant on the global defense scene, it is essential to invest significantly in innovation and the development of emerging technological solutions that will ensure a long-term strategic advantage.

In the last two years, the significant increase in defense budgets and the progress made in this domain can be attributed in large part to the joint policies adopted by NATO and the European Union in the face of Russian aggression. These measures are grounded in a unified and coordinated vision of the Euro-

Atlantic community, primarily aimed at countering the Russian Federation’s expansionist and aggressive actions.

A key element in this approach has been the active involvement of the United States in the conflict in Ukraine, which has profoundly influenced the strategy and alignment of NATO and EU members. The clear positioning of the US and its continued support for Ukraine have been decisive factors in creating a unified and rapid response from the allied states.

Recent changes suggest that a realistic goal for all NATO countries would be to allocate 3% of GDP to defense. These measures have a positive impact on the development of defense capabilities and emerging and disruptive military technologies of European member states, including NATO and the EU.

4. CONCLUSIONS

The article’s conclusions highlight the importance of emerging and disruptive technologies in the security strategies of NATO and the European Union, outlining concrete steps taken by both organizations to adapt to the new technological paradigm. From the adoption of an EDT roadmap by NATO in 2019 to the launch of strategic initiatives such as *DIANA* and the *NATO Innovation Fund*, both organizations have demonstrated a clear commitment to invest in technological development to maintain a strategic advantage over global adversaries. The European Union, through institutions such as *the EDA, the EIT and the Digital Europe Programme,* is also supporting defense innovation, thus enhancing the defense capabilities of member states.

Another crucial aspect highlighted is the increased cooperation between NATO and the EU, a partnership considered essential for maintaining security and stability in the Euro-Atlantic region. Collaboration between the two organizations, particularly in the field of emerging technologies, continues to be a determining factor for the success of European and North American foreign and defence policy. In this context, the progress made in the allocation of financial resources for defense, including the increase in the NATO and EU budget, is essential for strengthening this partnership and regional security.

The war in Ukraine has accelerated the need for security measures, and the financial and military response of NATO and the EU, including a significant increase in defense spending, is a demonstration of their commitment to protecting shared values. The strategic allocation of funding, especially toward emerging and disruptive technologies, is essential for strengthening the defence posture of NATO and the EU, facilitating timely and impactful responses to evolving global challenges.

In conclusion, the common objectives of adapting to new technological realities, combined with the significant increase in defense investments, enhance NATO and the EU's position as strategic actors in today's global environment. Moreover, fostering stronger engagement from the private sector and industry will not only accelerate progress toward security objectives but also bolster international alliances.

REFERENCES

[1]. Chrystensen M. Clayton, Joseph L.Bowell, Disruptive tehnologies: Catching the wave, Harvard Bussiness Review, January-February 1995.

[2]. Chrystensen M. Clayton, Innovator’s dilemma – When new technologies cause great firms to fail, Harvard Bussiness School, 1997.

[3]. Chrystensen M. Clayton, Michael Raynor, Rory McDonald, The big idea: What is disruptive innovation, Harvard Bussiness Review, Decembrie 2015, p.50.

[4]. Council of the EU, A Strategic Compass for Security and Defence For a European Union that protects its citizens, values and interests and contributes to international peace and security, nr. 7371/22, Bruxelles, March 21, 2022.

[5]. Council of the EU, EU-NATO cooperation, 2024. Accessed on 07.01.2025. https://www.consilium.europa.eu/ro/policies/eu-nato-cooperation/

[6]. Council of the EU, Joint Declaration on EU-NATO Cooperation, 10 Januarty 2023, no. 12. Accessed on 07.01.2025. https://www.consilium.europa.eu/ro/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/

[7]. Council of the EU, EU defence in numbers, 2025. Accessed on 05.02.2025. https://www.consilium.europa.eu/ro/policies/defence-numbers/

[8]. CARD - Coordinated Annual Review on Defence – Report 2024, EDA, 2024. Accessed on 08.01.2025. https://eda.europa.eu/docs/default-source/documents/card-report-2024.pdf

[9]. DIANA, 2025. Accessed on 26.01.2025. https://www.diana.nato.int/about-diana.html

[10]. EDA, 2024, Driven by global threats, shaped by civil high-tech. Accessed on 22.01.2025.

https://eda.europa.eu/webzine/issue22/cover-story/driven-by-global-threats-shaped-by-civil-high-tech

[11]. EDA, 2025. Accessed on 26.01.2025. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-defence-agency-eda_en

[12]. European Defence Agency (EDA), DEFENCE DATA 2023-2024, 2024, p.3, doi: 10.2836/0704767. Accessed on 25.01.2025. https://eda.europa.eu/docs/default-source/brochures/eda---defence-data-23-24---web---final.pdf

[13]. European Defense Fund (EDF), 2025. Accessed on 25.01.2025. https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-(edf)

[14]. International Institute for Strategic Studies (IISS), Defence Spending and Procurement Trends, February 12, 2025. Accessed on 27.02.2025. https://www.iiss.org/publications/the-military-balance/2025/defence-spending-and-procurement-trends/

[15]. International Institute for Strategic Studies (IISS), 2025. Accessed on 25.02.2025. https://www.iiss.org/online-analysis/military-balance/2025/02/global-defence-spending-soars-to-new-high/

[16]. Jens Stoltenberg, The Secretary General’s Annual Report, 2022. Accessed on 10.01.2025. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/sgar22-en.pdf

[17]. Jens Stoltenberg, The Secretary General’s Annual Report, 2023. Accessed on 10.01.2025. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/3/pdf/sgar23-en.pdf

[18]. Katarzyna A. Klasa, Benjamin D. Trump, Igor Linkov, James H. Lambert, Identifying New Partnerships for Innovation: Governance and Policy Challenges, 2020. Accessed on 21.01.2025. https://par.nsf.gov/servlets/purl/10195959

[19]. Ministry Of Research, Innovation And Digitization (MCID), Government of Romania, 2022, Memorandum pe tema: Aprobarea acțiunilor privind participarea României la Fondul NATO de inovare, p.2. Accessed on 22.02.2025. https://sgg.gov.ro/1/wp-content/uploads/2022/05/MEMO-15.pdf

[20]. Markides Constantinos, Disruptive Innovation: In Need of Better Theory, The Journal of Product Innovation management, 2006, p.20-24. Accessed on 13.01.2025. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=05a8242406374a0d971c622e21c25457b058430b

[21]. The National Academies Press (NAP), Persistent Forecasting of

Disruptive Technologies, Washington D.C., 2010.

[22]. NATO, 2019, NATO Summit in London. Accessed on 22.02.2025. https://www.nato.int/cps/uk/natohq/official_texts_171584.htm?selectedLocale=en

[23]. NATO, Brussels Summit Communiqué, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, June 14, 2021, no. 6d. Accessed on 22.02.2025. https://www.nato.int/cps/ra/natohq/news_185000.htm

[24]. NATO, 2022 Annual Report on NATO Common Funding, p.2. Accessed on 17.02.2025. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/8/pdf/2022_Annual_Report_on_NATO_Common_Fundin.pdf

[25]. NATO Summit in Madrid, NATO 2022 Strategic Concept, p.5. Accessed on 22.02.2025. https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf

[26]. NATO, 2023 Annual Report on NATO Common Funding, p.2. Accessed on 22.02.2025. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/2023-AR-common-funding.pdf

[27]. NATO, Emerging and disruptive technologies, August 08, 2024. Accessed on 20.01.2025. https://www.nato.int/cps/bu/natohq/topics_184303.htm

[28]. NATO, 2024, Defence Expenditure of NATO Countries (2014-2024). Accessed on 22.02.2025. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/6/pdf/240617-def-exp-2024-en.pdf

[29]. NATO Science & Technology Organization (STO), Science&Technology Trends 2020-2040. Exploring the S&T Edge, Bruxelles, 2020, p.13. Accessed on 21.01.2025. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

[30]. Official Journal of the European Union, REGULATION (EU) 2021/697 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092. Accessed on 26.01.2025. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0697

[31]. Official Journal of the European Union, REGULATION (EU) 2021/694 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240. Accessed on 26.01.2025. https://eur-lex.europa.eu/legal-

content/EN/TXT/PDF/?uri=CELEX:32021R0694

[32]. Rotolo D., Hicks D., Martin B. What Is an Emerging Technology? SPRU Working Paper Series (SWPS), 2015-06: 1-40. Accessed on 29.01.2025. https://www.techethos.eu/glossary/emerging-technologies/

[33]. Sequeira Keith, Backing visionary entrepreneurs, The European Innovation Council, Workshop for ERC PoCs, 29/03/2021, p.4. Accessed on 04.02.2025. https://eic.ec.europa.eu/system/files/2021-04/ERC_EIC_Keith%20Sequeira.pdf

[34]. Soare R. Simona, Innovation as Adaptation: NATO and Emerging Technologies, GMF, June 11, 2021. Accessed on 07.02.2025. https://www.gmfus.org/news/innovation-adaptation-nato-and-emerging-technologies

[35]. UEFISCDI, 2025. Accessed on 07.02.2025. https://uefiscdi.gov.ro/news-consiliul-european-de-inovare-noua-facilitate-step-de-300-de-milioane-eur-deschisa-pentru-depuneri-pentru-investitii-de-pan

EU - NATO COOPERATION IN THE CBRN FIELD

Givi AMIRANASHVILI

School of Governance, Caucasus University, Tbilisi, Georgia

This paper examines the European Union Chemical, Biological, Radiological and Nuclear Risk Mitigation Centres of Excellence (EU CBRN CoE) initiative and NATO's CBRN defence policy, with particular emphasis on bilateral cooperation between the EU and NATO in addressing CBRN threats. The research traces the establishment of the EU CBRN CoE initiative and analyzes how it promotes international cooperation and synergy with other global actors, especially NATO. Through a historical review of NATO-EU security cooperation, the paper investigates both organizations' CBRN policies, defence capabilities, and current challenges. While focusing on bilateral cooperation, the study also explores how these organizations independently counter CBRN threats. The publication concludes with practical policy recommendations aimed at enhancing the effectiveness of EU-NATO cooperation in CBRN risk reduction, acknowledging the limitations of available public information regarding NATO's CBRN activities.

Key words: *EU CBRN CoE; NATO CBRN defence policy; EU-NATO cooperation; CBRN risk mitigation; international security; bilateral cooperation; defence capabilities; security policy; risk reduction; chemical, biological, radiological and nuclear threats.*

1. INTRODUCTION

This publication is dedicated to the European Union Chemical, Biological, Radiological and Nuclear Risk Mitigation Centres of Excellence (EU CBRN CoE) initiative, NATO’s CBRN defence policy and NATO-EU bilateral cooperation in the CBRN field.

It illustrates how the EU CBRN CoE initiative was launched and provides an analysis of how the EU CBRN CoE initiative promotes international cooperation and synergy with other international actors, in particular with NATO.

The article also reviews the history of NATO-EU security cooperation and discusses their CBRN policies, defence capabilities and current challenges. The focus is on bilateral cooperation, but also on how these international organisations work separately to counter CBRN threats.

This publication also aims to contribute to the policy-oriented discussion on how to improve EU-NATO cooperation and to better address CBRN risk reduction policy from a practical point of view. In this respect, this article proposes key recommendations to enhance the effectiveness of joint cooperation between these organisations.

In principle, NATO-EU cooperation in the CBRN domain is a broad and complex issue that cannot be fully covered in this article, especially considering that much of the information on NATO's CBRN activities is not publicly available.

2. GEOPOLITICAL CHALLENGES

It is quite apparent that many of the security threats the world faces today, such as terrorism, cybercrime, pandemics, illicit trafficking, hybrid warfare, regional conflicts that have given rise to forced displacement and uncontrolled migration flows, are interconnected and increasingly complex in themselves. Besides, security risks associated with chemical, biological, radiological, and nuclear materials threatens both developing and industrialised countries equally.

In addition to this, the EU's global leadership and security environment have deteriorated as a result of the financial crisis, a collapse of the management of unexpected and extraordinary migration and the refugee crisis, rising Euroscepticism, and the crises spreading on the EU's frontiers [1].

Basically, after the Cold War, the international system was somewhat dynamic. Many positive events happened during this period of time. New opportunities have been arisen that might allow for a better and ambitious world.

Thirty years after the Cold War, however, it is clear that Europe continues to face increasingly complex threats and new challenges. Illegal immigration and, more recently, terrorism and organised crime have emerged as new dangers and threats [2].

In recent years, the world has been confronted with scenarios such as nuclear disasters like Fukushima, chemical warfare in Syria, the Ebola epidemic in West Africa and the COVID 19 global pandemic.

After the attacks of 11 September 2001, the international community increased their vigilance with regard to the possibility of the terrorist use of chemical, biological, radiological, and nuclear weapons and subsequently came to the agreement that there was a high risk of use of the CBRN materials by terrorists.

With the 2001 “anthrax letter” attacks, as well as with the use of Sarin gas in a Tokyo subway, there was a clear illustration of this line of thought. It is important to note that there are still attempts to obtain CBRN materials as well as to use them for terrorist purposes.

Several authors have described factors that make chemical, biological, radiological, and nuclear terrorist events unique and demanding. What needs to be emphasised is that the IS terrorist attacks became the turning point with regard to changing Europe's security dimensions significantly and, currently, countering terrorist access to CBRN agents and materials is a currently top priority for the EU and NATO.

For instance, 21 August 2013 saw the most serious CBRN crisis since 2003. There was evidence of mass chemical weapon (CW) bombing of areas surrounding the Syrian capital that resulted in the deaths of 1,400 Syrians. It should be noted that it was the biggest chemical weapons attack since Saddam Hussein's bombardment of Halabja, Iran, in 1988 (with 5,000 deaths) [3].

Besides, the IS Paris attacks on 13 November 2015 showed an increased threat of new skills acquired by jihadists returning to their home countries, as well as radicalised groups and individuals.

Furthermore, recent war in Ukraine and policies enacted by Russia have reduced stability and changed the EU security environment. The use of the Novichok nerve agent in Salisbury in March 2018 was the first such attack on European soil since World War II and subsequently resulted in the death of an EU citizen [4].

All these incidents demonstrate the importance of close cooperation among countries in the CBRN field at the regional and international levels, because the process of the globalisation and intensive industrialisation increase the potential risk of CBRN hazards.

From the analysis carried out by Bonfanti and Capone (2005), certain questions have arisen regarding addressing this issue, for instance: what kind of legal and political framework exists and which instruments have been developed to prevent and respond to this kind of emergency? Are the EU Member States up to this task? What is the state of the European security environment [5]?

These questions became actual and logical because they respond to the starting discussion point about the series of attacks in Paris on 13 November 2015, where terrorists attacked six places synchronously so as to split the targets of counter-terrorist forces [6].

In recent years, threats to European security have become more complex, hybrid, asymmetric, rapidly evolving and difficult to predict. As such, they are beyond the capacity of any single state and therefore require, more than ever, a coherent, comprehensive, multi-faceted and coordinated response.

The evolution of global CBRN threats, and indeed the response to these threats, has been highly visible since the first use of chemical weapons in the First World War. In the last fifteen to twenty years, the threat of a terrorist group acquiring CBRN materials has somehow forced governments and international organisations to adopt relevant regulations and programmes to protect populations from CBRN risks and hazards [7].

So, bearing in mind the lessons learned from these terrible incidents, by 2005 the European Union had developed a comprehensive counter-terrorism strategy which builds on four pillars, namely "prevent, protect, disrupt, and respond." It should be noted that the second pillar of the EU counter-terrorism strategy, namely "protect", deals with the issue of CBRN and highlights the importance of strengthening the cooperation with international organisations and partners, as well as offering technical assistance to third countries so as to prevent the proliferation of CBRN materials.

The fact is that Britain's exit, the US administration under Donald Trump and its statements on the EU and NATO, US relations with Russia and Turkey, and the migration and refugee crisis have all played a positive role in this process and have subsequently led to the mobilisation of common political goals and objectives within the EU. The European Union is committed to a global order based on international law, including the principles of the UN Charter and the provisions of the Lisbon Treaty.

Given the global nature of security threats, CBRN risks cannot be addressed in isolation due to their multidimensional nature (health, environment, security, crisis management), as demonstrated by the Syrian chemical threat and more recently by the COVID-19 pandemic.

More than ever, there is a need for a stronger Europe that acts in a unified manner at the global level to address the many global challenges that directly or indirectly affect the security of individual states and their citizens.

The EU and NATO must therefore promote a culture of CBRN security in Europe and internationally. The aim is twofold: to prevent CBRN incidents and to strengthen the capacity of partners to respond to such incidents in order to protect people, the environment and critical infrastructure.

3. WHAT IS EUROPEAN UNION CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR RISK MITIGATION CENTRES OF EXCELLENCE (EU CBRN COE) INITIATIVE?

As a global actor, the EU has always considered CBRN threats and risks to be a major challenge to security and peace around the world. For instance, disease surveillance, waste management, emergency planning, early warning, civil protection, export control of dual-use goods, cross-border trafficking of CBRN materials, retraining and alternative employment of former weapons scientists, are areas of concern both to the EU and its partner countries.

The EU CBRN Risk Mitigation CoE Initiative is the EU's largest civilian external security programme funded and implemented by the EU through the IcSP, with a budget of €130 million for 2014-2020. This is the EU's main instrument of international cooperation supporting security initiatives and peace-building activities in Partner Countries [8].

The EU Chemical, Biological, Radiological, and Nuclear Risk Mitigation Centres of Excellence (EU CBRN CoE) were launched in 2010 under the European External Cooperation Instrument for Stability (IfS), as an initiative of the European Union (EU). This initiative is implemented and funded by the European Commission in cooperation with the United Nations Interregional Crime and Justice Research Institute (UNICRI**).** The European External Action Service (EEAS) is also deeply involved in the follow up to the Initiative.

The EU CBRN Centres of Excellence (CoE) Initiative aims to mitigate chemical, biological, radiological, and nuclear threats and risks from outside the EU that may create a threat to the EU.

The main objectives of EU policy in this respect are highlighted in Article 4.2 of the former Instrument for Stability (IfS), and of Article 5 1-b of the Instrument Contributing to Stability and Peace (IcSP, 2014). It should be noted that the EU CBRN Centres of Excellence, an innovative EU initiative, has been welcomed at the international level by the UN Security Council and the G8 Global Partnership.

The CoE Initiative has been developed with the technical support of relevant international/regional organisations, the EU Member States, and other stakeholders through coherent and effective cooperation at national, regional, and international levels. This approach involves multilateral partnerships between the European

Union and its 27 Member States with more than 63 countries worldwide and focus on regional cooperation.

For instance, the CoE Initiative covers the EU Southern and Eastern neighbourhood, the Middle East, the Gulf, Africa, Central Asia, and Southeast Asia. In total, these regions are covered by eight CoE regional secretariats worldwide. CBRN risk mitigation has now become a significant dimension of EU cooperation with other regions worldwide.

It was therefore started as a new methodology for providing technical assistance to countries outside the EU. Specifically, the CoE Initiative aims at assisting partner countries in the development of national CBRN policies/strategy and building capacities to effectively mitigate safety and security risks posed by chemical, biological, radiological, and nuclear materials. The origin of these risks can be criminal (proliferation, theft, sabotage, and illicit trafficking), accidental (industrial catastrophes, in particular chemical or nuclear, waste treatment and transport), or natural (mainly pandemics but also be the consequence of natural hazards on CBRN material and facilities).

The 2014–2016 Ebola virus outbreak in West Africa and the COVID-19 Pandemic in 2020, and also incidents such as the Fukushima nuclear reactor meltdown in 2011, the use of sarin and chlorine gas in Iraq and Syria, and of the nerve agent VX at Kuala Lumpur airport in February 2017, are stark reminders of the dangers that can ensue when CBRN risks occur.

One of the main goals of the EU CBRN CoE Initiative is to respond to the increasing global public concern about chemical, biological, radiological, and nuclear risks and to boost cooperation at national, regional, and international levels, and hence to develop a coherent CBRN risk mitigation policy. Such risk mitigation includes prevention, preparedness and post-crisis management.

It should be stressed that the CBRN Centres of Excellence can be considered a unified platform for all of the CBRN domains, such as border monitoring, illicit trafficking, export control, biosafety and biosecurity, etc.

In addition to the development of the National CBRN Action Plan/Strategy in CoE partner countries, the CoE has, for example, pursued improved CBRN risk mitigation policies in CoE partner countries through the tailored assistance packages (19 actions in five regions, €21.5 million in 2011). Currently, more than 100 CoE regional projects have been implemented and 24 are ongoing in the 8 regions.

Due to CBRN threats knowing no borders, the EU cannot restrict its actions to EU territories. Taking this into account, the European Council, the Council of the European Union, and the European Parliament [9] have systematically stressed the importance of linking the EU's internal and external security policies, which itself covers CBRN matters.

In practice, the initiative enhances the protection of partner countries and EU citizens against events that may have widespread and serious cross-border consequences. More generally, the Centres of Excellence promote the development of and focus on multilateral cooperation. Ultimately, the Centres of Excellence contribute to peace, security and prosperity.

4. NATO AND ITS CBRN DEFENCE POLICIES

In principle, the preamble to the North Atlantic Treaty sets out the basic principles that should guide NATO's security policy. For example, the peace, freedom, heritage, stability and prosperity of each NATO member are principles that NATO must collectively protect.

As mentioned above, the dangers and threats posed by CBRN incidents are extremely serious. Therefore, not only states but also international organisations should be prepared to deal with this problem properly. All these threats and dangers have a direct impact on the security of EU and NATO member states.

Actually, the situation in the case of a large-scale CBRN incident is critical. The definition of a large-scale incident is given by NATO (2019a, pp. 3-4), clarified it in the following way: a CBRN incident which is *"large enough to stress a nations capacity to respond effectively*" [10].

Generally, there are different types of CBRN incidents which can occur: first, attack by a non-state actor like a terrorist group, and second, a CBRN incident caused by a state actor like the 2018 Salisbury attack [11]. The incident within Salisbury shows that if states have sufficient capability and goodwill to counter CBRN incidents, at least on the local level, this does not require military assistance so as to put into operation Article 5 of the North Atlantic Treaty [12].

However, even if CBRN incidents do not have a serious impact on state security itself, such as the Salisbury attacks, they still pose a high risk to the general population, which is why any country can request NATO or EU assistance in this situation.

As a state actor, Russia's invasion of Ukraine and its military aggression against the Ukrainian people has created a new reality on the global security agenda.

Besides, the Democratic People's Republic of Korea (DPRK) is still attempting to expand its nuclear arsenal and missile potentiality in violation of the relevant UN Security Council Resolutions. Kim Jong-Nam, who was poisoned by a nerve agent in Malaysia in 2017, shows that the DPRK is capable of using prohibited weapons outside its borders.

The evolution of the Syrian conflict has also raised massive concerns about the threat of chemical weapons. The use of sarin gas in the Syrian war (in the Ghouta area, a suburb of Damascus) on 21 August 2013 demonstrates the increasing need to plan and conduct military operations under CBRN conditions [13].

As for non-state actors, such as terrorists, there is international evidence that non-state actors have already used chemical weapons in Syria. Also, non-state actors will attempt to weaponize toxic industrial chemicals. Moreover, scientific and technological developments mostly have allowed increased access to CBRN materials and have reduced the barriers to acquiring such materials. So, the risk of the use of CBRN materials by non-state actors remains actual [14].

Thus, NATO today faces a security environment in which CBRN threats have become more numerous and diverse, in which state and non-state actors pose a major threat to the use of weapons of mass destruction, and in which technological developments are rapidly increasing these risks [15].

It therefore remains an open question whether NATO or the EU have sufficient resources and capabilities to deal adequately with CBRN incidents.

Thus, NATO's CBRN Defence is based on two complementary principles and obligations: the first embraces Alliance commitments to develop and maintain the necessary CBRN defence capabilities, including intelligence, personnel, equipment, policies, plans, exercises and training, whilst the second includes the protection of society and the necessary resilience against CBRN threats.

Remarkably, NATO's CBRN defence doctrine provides guidance and instructions on how to tackle CBRN threats. In practical terms, this document defines an applicable approach to addressing this issue. It can be stated that the policy encompasses different stages, *inter alia* the prevention of the proliferation of WMDs, protection against WMDs and CBRN attacks, and recovering from a WMD attack or CBRN incident. With respect to each area, NATO take particular actions so as to prevent a WMD attack or CBRN incident.

Also, the focus is to ensure that NATO has sufficient ability to react to and recover from a CBRN incident or WMD attack [16]. In the case of WMD attack, NATO is ready to use its military capabilities so as to disrupt, deny, and defeat the use of WMDs, to protect Alliance populations and territories, and to assist partners.

NATO's CBRN Defence Policy covers complementary commitments to provide necessary military capacities and thereby enhance NATO's flexibility against CBRN threats [17]. This policy supports the goals presented in the new Strategic Concept. A new strategic doctrine adopted by the Heads of State and Government at the 1999 Washington Summit has committed NATO to 'actively contribute' to the development of arms control, disarmament, and non-proliferation agreements, and reduce the threats arising from the proliferation of WMDs and their means of delivery [18].

NATO's CBRN Defence Policy is also in line with its Military Strategy and supports the implementation of this document, including the Concept for the Deterrence and Defence of the Euro-Atlantic Area and the NATO Warfighting Capstone Concept. It further complements the Comprehensive Cyber Defence Policy, the Strategy on NATO's Role in Countering Hybrid Warfare, and the Coherent Implementation Strategy on Emerging and Disruptive Technologies [19].

NATO has taken an important step towards establishing a Senior Politico-Military Group on Proliferation (SGP). It has committed itself to an effective response to proliferation [20]. Furthermore, In May 2000, the NATO Weapons of Mass Destruction Centre was opened to provide a focal point for NATO expertise and to support the work of the SGP. Notably, the Centre itself comprises an interdisciplinary team with expertise in chemical and biological weapons, ballistic missiles, intelligence and the political aspects of arms control and non-proliferation regimes. Most importantly, the Centre has a special focus on Russia.

Notably, the process of overestimation and improvement of the role and objective of NATO missions began to be discussed at global level on the 13 September 2006 at the Allied Transformation Headquarters in Norfolk (USA).

Later, the Summit in Riga on 28-29 November, 2006 was dedicated to sufficient analysis of the organisation's transformation in terms of changing world security and of post-bipolar system risks [21]. The most important fact in this context has been the adoption of the comprehensive political guidance at the Riga Summit. By its adoption, NATO took steps towards its military transformation for the next 10-15 years, determining the limitations of the organisation's transformation, its means and capabilities, as well as modification of the defence planning policy.

NATO's security environment has become more complex and challenging since 2009, when Allies approved *NATO's Comprehensive, Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending against Chemical, Biological, Radiological and Nuclear (CBRN) Threats."*

From the standpoint of M. Mureşan and D. Muresan, NATO's future role is very much defined by its transformation "*which makes it capable to fulfil new and complex missions for the 21st century, in a world globally threatened by terrorism and the mass destruction weapons and marked by unconventional and asymmetrical risk [...].*" [22]

In order to properly fulfil NATO's core missions and respond effectively to all these challenges, in particular to protect itself against a wide range of CBRN threats, the Alliance should enhance its CBRN defence capabilities at the operational level.

The mechanism dealing with CBRN threats used by NATO is the so-called 'Clearing House Mechanism'. In case of any NATO Member State, partner country, or partner organisation, such as the UN, asking for assistance, their request is redirected to the Euro-Atlantic Disaster Response Coordination Centre (EADRCC). The Centre is obliged to send it on to all other NATO Member States. In response to this, a Member State that has sufficient resources and supplies at its disposal can assist the country requesting assistance. The EADRCC itself provide assistance in the delivery and deployment of such resources [23].

Actually, military CBRN defence capabilities make it possible for NATO forces to rapidly deploy for and quickly recover from the consequences of CBRN incidents, as well as to further support the recovery of affected populations, territories, and forces. The COVID-19 pandemic reaffirmed the importance of civil-military cooperation in a crisis.

In fact, in the instance of a large-scale CBRN incident when national first responders' response capabilities are overloaded or incapable of responding appropriately, national military capabilities are used. Nevertheless, such military CBRN defence capabilities might be limited [24].

The Chemical, Biological, Radiological and Nuclear Defence Battalion was established in 2003 to provide CBRN defence capabilities in circumstances other than CBRN incidents, including during conflict. However, the battalion is also deployed in instances of natural disasters and industrial accidents. The CBRN Defence Battalion is "*capable of reconnaissance, monitoring, sampling, identifying and detection of CBRN-related subjects, as well as providing CBRN assessments and hazard management [25]*."

Important changes to the PCC were offered by the creation of a CBRN defence task force, entitled the "Combined Joint CBRN Defence Task Force" (CJ-CBRND-TF). It comprised a CBRN Joint assessment Team (CBRN-JAT) and a CBRN Defence Battalion (CBRN-Bn) tackling reconnaissance, monitoring, sampling, and detection of CBRN substances, as well as decontamination [26]. Both are well trained and experienced and are fully capable of operating effectively during military conflict [27].

It is therefore safe to say that NATO's CBRN defence capabilities are capable of preventing the development, possession, proliferation and use of WMD materials, technologies and means of delivery. This pathos is also enshrined in the defence policy, according to which NATO forces "*will be ready to deny access to CBRN materials and their means of delivery, disable and dispose of WMD and CBRN materials in operational contexts, respond against the source of any WMD attack, mitigate the effects of CBRN use, and eliminate an aggressor's WMD capabilities*" [28].

Moreover, NATO's 2022 CBRN Defence Policy creates an appropriate framework through which the planning, exercising, training, equipping, and assessing of NATO capabilities to counter WMD proliferation and CBRN threats are available [29].

Today, one might ask whether NATO, as a major military organisation, has an important role to play in disaster response. The answer is simple. Although NATO plays an important role in this area, it is not a major humanitarian organisation.

The establishment of a NATO Rapid Reaction Corps underlined NATO's need to become involved in crises management, peace keeping/building, and humanitarian assistance [30].

Nevertheless, if we take a historical perspective, we can see disaster response and humanitarian operations undertaken by NATO almost 60 years ago. In 1953, the

Alliance provided assistance to Belgium and the Netherlands [31]. Both countries had been damaged by floods. Besides, NATO has provided assistance to many countries, not only within but also outside NATO [32].

5. NATO NETWORK OF CENTRES OF EXCELLENCE (COES) - JCBRN DEFENCE COE

What is NATO's Joint CBRN Defence Centre of Excellence (JCBRN Defence CoE)?

The mission of the JCBRN Defence CoE is to: "a) Provide advice in all CBRN defence related areas; b) develop CBRN defence doctrines, standards, knowledge to support improvement of interoperability and capabilities; c) provide opportunities to enhance education and individual training; d) directly support NATO's collective training; e) contribute to the relevant lessons learned processes and lead the CBRN portion; f) direct support to ACT's Training Requirements Analysis (TRA) process; and g) within a Programme of Work (POW) approved by the Steering Committee (SC), assist NATO, Sponsoring Nations (SNs), and other international institutions or organisations in their CBRN defence related efforts, including validation through experimentation [33]."

JCBRND CoE is based in Vyškov, Czech Republic, and is commanded by a Czech army colonel. It comprises a directorate and four departments. The Staff is multinational and 30 out of 81 positions are open to Allied personnel. There are twelve Sponsoring Nations and one Contributing Partner: Austria, Czech Republic, France, Germany, Greece, Hungary, Italy, Poland, Romania, Slovakia, Slovenia, United Kingdom, and the United States [34].

It has been pointed out that JCBRND CoE plays an important role in CBRN capability development efforts [35]. Furthermore, NATO Centres of Excellence represent an expertise network for the Alliance. The JCBRN Defence CoE "*serves as a critical focal point for CBRN defence-related analysis, insight, and innovation.*" [36] The special training, capacity-building, CBRN defence concept and doctrines, as well as modelling and simulation, are provided by the NATO Centres of Excellence.

In addition, the JCBRN Defence CoE organise NATO CBRN "Reachback capabilities process" [37], which provides assistance to the deployed forces. This assistance can be seen as comprehensive advice on CBRN hazards and defensive countermeasures in the process of dealing with WMD proliferation, protection, and recovery [38].

In 2018, the Joint Chemical, Biological, Radiological and Nuclear Defence Centre of Excellence (JCBRN Defence CoE) adopted a document entitled "Cross-border Cooperation in case of CBRN incidents". This document includes "an analysis of civil military cooperation between NATO and individual nations in case of a large-scale CBRN incident." (JCBRN Defence CoE, 2018).

This document is also the basis for the JCBRN Defence CoE Advisors Conference. The first Conference was held in Prague, Czech Republic, from 17 – 19 September 2019. This conference was attended by 39 participants from 10 countries as well as participants from international organisations. Participant countries included the Czech Republic, Finland, France, Germany, Greece, Italy, the Netherlands, Poland, Romania, and the United States of America. As for the participants from international organisations, these included NATO Headquarters – International Staff, Supreme Headquarters Allied Powers Europe (SHAPE), and JCBRN Defence CoE [39].

The main outcomes of this conference can be seen as the development of a joint-military concept for NATO coordination on CBRN consequence management issues, the review of NATOs Advisory Support Teams (AST) and Rapid Reaction Teams (RRT), the introduction of biological and chemical incidents into scenario-based discussions (SBD) at the North Atlantic Council (NAC) level, and the introduction of large-scale incidents into NATO's major exercises [40]. The most important recommendation of the conference was to strengthen NATO-EU cooperation concerning civil-military cooperation in the CBRN domain [41].

In order to further develop CBRN defence capabilities, the JCBRN Defence CoE developed the network of partner organisations including international organisations, governmental and non-governmental organisations, nations, and other institutions. Moreover, the NATO JCBRN Defence CoE's cooperation with the EU CBRN CoEs continues to be a high priority for both NATO and the EU.

In addition to the Joint CBRN Defence CoE, there are other NATO CoEs and education and training facilities which play important role in CBRN defence, for instance, the Defence against Terrorism CoE, Military Medicine CoE, Maritime Security CoE, Explosive Ordinance Disposal CoE, Strategic Communications CoE, and the

NATO Maritime Interdiction Operational Training Centre.

6. NATO-EU CBRN BILATERAL COOPERATION: COMMON AND DIVERGENT INTERESTS

The EU and NATO have shared interests, both strategically and operationally, especially to support international peace and security in crisis management and to develop their defence capabilities [42].

It is important to bear in mind that CBRN incidents require coordination at many levels in order to respond effectively. Historically, the EU and NATO have worked well in the Balkans and in Afghanistan, even though formal relations are not fully defined. Both therefore need to strengthen their strategic partnership at the operational level, while fully respecting the decision-making autonomy of each organisation.

At the strategic level, both NATO and the EU have approved their non-binding guidelines or plans to ensure cooperation and CBRN defence/risk mitigation. NATOs non-binding guidelines and the EU Action Plan can be mentioned in this regard.

Its notable that the "EU Action plan to enhance preparedness against CBRN security risks", adopted in 2017, focused on building stronger internal and external links with key regional and international EU partners (preparedness and response) and enhancing knowledge on CBRN risks [43]. Because these plans embrace the individual vision of each organisation, there is a need to enhance mutual cooperation despite the differences in their operating procedures [44].

According to the paper "EU preparedness against CBRN weapons", there are ongoing efforts to strengthen cooperation between NATO and the EU, including in the CBRN domain [45]. As reported in the above paper (drafted by the Policy Department for External Relations), "*The CBRN Action Plan stresses the need for close cooperation with key partners and organisations. However, some European Member States made it clear that the European Union's own capacity-building initiatives should not compete with those of NATO. Taking into account political considerations, available resources but also challenges related to CBRN threats, it is thus crucial to develop closer cooperation with the Organisation and avoid duplication.*" This is why active communication and close partnership between NATO and the EU is crucial.

In fact, because of military organisation and due to the main objective of NATO is collective defence, it is countering vast range of threats by strengthening its deterrence and defence, helping to prevent and manage crisis situations and encouraging cooperative security, as enshrined in the 2022 Strategic Concept. As for the EU, the main objective of this organisation is to promote peace, follow the EU's values, and improve the wellbeing of nations.

It should be pointed out that the Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by the Heads of State and Government in Lisbon on 19 November 2010 underlines the importance of cooperation with the EU in the view of the fact that the EU is both a 'unique' and 'essential' partner to NATO [46].

NATO's Strategic Concept outlined that the proliferation of nuclear weapons and other weapons of mass destruction (WMD), and their means of delivery, threatens incalculable consequences for global stability and prosperity [47]. It also declares that NATO would commence to deal with all stages of such a crisis [48].

Furthermore, NATO's Comprehensive, Strategic-Level Policy for Preventing the Proliferation of the WMD and Defending Against CBRN Threats, planning for CBRN consequence management represents a multidimensional effort. It requires not only coordination within the organisation at all levels, but also with other international organisations [49].

As far as the European Union is concerned, the European Council decided to deepen defence cooperation with NATO through the adoption of an EU-NATO Joint Declaration on cooperation on hybrid threats, operational cooperation, cyber security, defence capabilities, industry and research, exercises and capacity building.

NATO follows a partnerships format for which CBRN defence and resilience are focus areas. It can be noted that CBRN defence is a main element of engagement with regional partnership groupings such as the Partnership for Peace, Mediterranean Dialogue and Istanbul Cooperation Initiative. Bearing in mind the transnational factors of CBRN threats, NATO realised that "*strengthening the CBRN defence of its partners helps to sustain the overall security of the Alliance [50]*."

In addition, staff-to-staff communication between NATO and the EU is essential. Usually, both organisations organise *ad hoc* meetings, if needed. In addition, there are different channels used by both NATO and the EU in the realm of CBRN/risk mitigation, including workshops, meetings, and conferences. For instance, the workshop “Resilience and cross-sectoral cooperation in responding to CBRN threats with hybrid elements” took place in July 2019 [51].

Also, structured Dialogue meetings are conducted at least twice a year in which NATO International Staff (IS), International Military Staff (IMS), and different bodies of the EU, such as the European External Action Service (EEAS), gather together to discuss CBRN defence/risk mitigation and NATO-EU cooperation as well. Also, liaison officers are periodically contribute to communication and cooperation between NATO and the EU [52].

In addition to formal agreements, there are informal channels of communication that have played an important role in the development of NATO-EU relations (Græger, 2016) [53]. Such forms of cooperation include personal relationships among staff.

Also, the NATO Secretary General took part in an informal meeting between EU foreign ministers, especially concerning the annexation of Ukraine (NATO, 2014) [54]. In addition, numerous formal and informal cooperation have been organised within the operation of Concordia. From these few examples, it can be seen how important informal cooperation has been for both organisations.

It is reasonable to highlight that one of the most active channels in cooperation and communication between the two institutions in CBRN domains has been set up within the framework of the EU CBRN CoE Initiative. For example, NATO assists the EU CBRN CoE Initiative in developing their training curriculum and, from a practical perspective, invites participants from the EU CBRN CoE partner counties to participate in NATO’s training as organised through the NATO joint CBRN Defence Centre of Excellence (Vyškov, Czech republic).

So, this is an excellent opportunity for CBRN practitioners from the EU CBRN CoE regions/partner countries to participate in advanced CBRN training with live agents and to accordingly enhance professional knowledge and skills on how to tackle CBRN incidents. This is also a practical implementation of an idea of networking EU and non-EU CBRN training facilities.

The first training course, where practitioners and relevant national experts from EU CBRN CoE partner countries from the Southeast and Eastern Europe CoE Regional Secretariats (SEEE), and from the Gulf and Middle East CoE Regional Secretariat participated, was held on 2-6 October 2017.

Selection of participants from the NATO JCBRN CoE and the EC on the basis of the CVs of the proposed trainees after receipt of the candidatures from the respective CoE partner countries. Following sessions of the Live Agent Training (LAT) at the NATO Joint CBRN Centre of Excellence in Vyskov were held in 2018 and on 30 September - 4 October 2019. The CoE countries of the EU CBRN CoE Initiative were again invited to participate.

In addition, Horizon 2020 can be seen as a good example of successful cooperation between NATO and the EU while working on the e-NOTICE project [55]. Also, the joint work within the framework of the Joint CBRN Defence Capability Development Group, the Joint CBRN Defence CoE, and the Nations Concept Cluster CBRN Protection should be mentioned in this respect. So, it can be stated that NATO, together with its partners, organises joint exercises and shares CBRN defence-related expertise, knowledge, and information.

As can be seen, the security of both organisations is interrelated. However, there are differences in the interests and approaches of EU Member States in the CBRN field. Moreover, certain facts show that the cooperation between NATO and the EU is limited. Therefore, their cooperation in the CBRN field needs to be modified in order to work comfortably.

As argued by Juncker, Soltenberg and Tusk (2016), there are still some obstacles between the two organisations that hinder successful cooperation [56].

As stated by Elizaveth Tamara Janette Bijl, "*there are no systems, mandates or procedures for the common cooperation between NATO and EU, which are accepted by all members and at all levels of NATO and EU [57].*"

In her view, today, NATO-EU cooperation is not good enough, "*which was wanted during the signing of the Joint Declarations [--].*" [58] She believes that there are many reasons for this. According to her, one of the barriers to cooperation between NATO and the EU is a lack of trust which "*leads to other obstacles of cooperation such as communication problems, lack motivation to cooperate [----.]*" [59] As believed by E. Tamara Janette Bijl, NATO-EU cooperation should continue in a permanent manner rather than just being occasional in nature. So, she evaluates this cooperation "as *partially unprepared, especially if action has to be taken quickly and effectively [60].*"

In view of the fact that both organisations operate in the same geographical area, similar threats can be characterised by each. The fact is that NATO and the EU share twenty-one Member States, where NATO have nine non-shared Member States and the EU have only six. Nevertheless, both organisations have particular peculiarities that influence their key objectives and tasks. Basically, there are several factors that can influence the dissimilarities in the EU Member States' policies and interests regarding CBRN policy, particularly WMD non-proliferation.

The fact is that some EU Member States are members of NATO and others are not, and this can indeed influence their nuclear weapons policies. For this reason, the EU's relationship with NATO has experienced some obstacles.

For example, France's policy towards the NPT was initially negative, especially before the 1990s. The main reason for this was that France was seeking to develop its own nuclear capabilities. After developing its own nuclear arsenal, France eventually became a party to the NPT (1992), and its subsequent contribution to EU non-proliferation policy has been particularly visible [61].

Besides, EU Member States have different energy interests, which surely affects their policies in this regard. The fact is that some Member States want to use their nuclear capabilities for purely peaceful purposes. Some EU Member States are against using such capabilities at all.

In general, those EU Member States which are also members of the NATO Alliance are actively supporting the Alliance's nuclear policy in accordance with the defence commitments within this framework [62].

Another is the use of NATO's military force in a crisis. According to Lindstrom and Tardy, for example, this difference can be seen in NATO's position on the use of military force. Moreover, political obstacles existed between certain members (Greece, Turkey) of NATO and/or the EU that may additionally reflect on their cooperation.

None of this, however, has had a significant impact on the mutual understanding and bilateral cooperation between NATO and the EU as a whole. Moreover, together they have the capacity to mobilise a wide range of instruments and resources to address the challenges that remains.

In general terms, to set up successful cooperation between two powerful international organisations is an ambitious and complex issue that requires a lot of effort in order to deal with the disagreements and obstacles between them in a satisfactory way.

6.1. Joint Declarations

NATO and the EU signed joint declarations on their partnership in 2016 and 2018. The first addressed the "unprecedented challenges" to both organisations. Actually, it encompasses hybrid- and cyberthreats, increasing resilience, defence industry, coordination on exercises, education, training, information sharing, and migration.

The key objectives of cooperation are set out in the Joint NATO-EU declaration of 2016, namely, "*In light of the common challenges we are now confronting we have to step up our efforts: we need new ways of working together and a new level of ambition; because our security is interconnected; because together we can mobilise a broad range of tools to respond to the challenges we face; and because we have to make the most efficient use of resources. A stronger NATO and a stronger EU are mutually reinforcing. Together they can better provide security in Europe and beyond*."

The second strategic partnership declaration signed in 2018 revised the previous one with a view to addressing more issues then were enshrined in 2016. It reaffirmed the importance of a continued cooperation and states: "*NATO and the European Union are strengthening cooperation in a range of areas, including military mobility, counter-terrorism, resilience to chemical, biological, radiological and nuclear-related risks, and promoting the women, peace and security agenda*."

The second declaration demonstrated that there was an important development concerning nuclear risks as well as progress in the CBRN realm. This document covers staff-to-staff dialogues, workshops, scenarios-based discussions and, most importantly, cooperation between CBRN Centres of Excellence of both organisations/NATO and the EU. Also, in order to counter hybrid threats, NATO and EU set up hybrid analysis offices at the cooperative level. For instance, NATO established the Hybrid Analysis Branch, and the EU created the EU Hybrid Fusion Cell [63].

Both Joint Declarations underline the need, importance, and willingness for cooperation between the two organisations. They declare that daily communication is crucial and becoming the norm [64].

So, in accordance with the declarations, both organisations state that EU efforts will be complementary to NATO in its tasks. Indeed, nobody can replace NATO in the security realm on the European continent, but the EU should become a partner with the purpose of establishing itself as a security provider, despite having less means and tools than NATO [65].

It is reasonable to highlight that one of the objectives enshrined in the EU Global Strategy is about the synergy and consolidation of the NATO-EU partnership. More specifically, the EU Global Strategy concludes: "*while NATO exists to defend its members, most of which-European countries, from outside attacks, Europeans need to be better prepared, trained and organised, to be able to contribute decisively to these collective efforts, and act independently if and when it is needed. For Europe to promote peace and to guarantee security on its territory and beyond is of extreme importance to have the necessary ambition and certain level of strategic autonomy [66].*"

According to the Council Conclusions on implementing the EU Global Strategy and the European Defence Action Plan, the essential element of broader cooperation is to strengthen "*the Union's ability to act as a security provider [67].*"

6.2. Joint Declaration on ESDP

It is important to note that the first declaration which encompass the possibilities of NATO-EU cooperation was the EU-NATO Declaration on European Security and Defence Policy (ESDP), signed in 2002. The document declared that the relationship between the European Union and NATO would be based on the strategic partnership. It stated the need for: "*ensuring that the crisis management activities of the two organisations are mutually reinforcing, while recognising that the European Union and NATO are organisations of a different nature; Effective mutual consultation, dialogue, cooperation and transparency; Equality and due regard for the decision-making autonomy and interests of the European Union and NATO; Respect for the interests of the Member States of the European Union and NATO [68].*"

So, the 'EU-NATO Declaration on ESDP' is based on shared values. Furthermore, the strategic partnership established between the European Union and NATO in crisis management addressed the challenges of the new century [69].

As can be seen, the most important thing is that the decision-making procedures should be based on the principles of reciprocity, without prejudice to the specific features of the security and defence policy of any Member State. Indeed, both organisations have specific characteristic features based on their own interests. So, it is very important that they should cooperate in full respect for each other's autonomy.

Also, it needs to be taken into account that, in accordance with this declaration, the European Union is ensuring the fullest possible involvement of non-EU European members of NATO within the ESDP, which is very important. NATO itself, in coordination with the partners, supports the ESDP as a significant part of European integration in terms of European Security. In addition, the High Representative and Vice President of the European Commission have established a direct channel in cooperation with NATO, which places "the EU in a favourable position [70]."

6.3. Berlin Plus Agreement

In the partnership between NATO and the European Union, the Berlin Plus Agreement (BPA) must be mentioned as an important document signed in 2003. This agreement once again reaffirmed that NATO and the European Union would work together to prevent and resolve crises and armed conflict in Europe and beyond. They have both also decided to develop cooperation to combat terrorism and the proliferation of weapons of mass destruction [71].

Berlin Plus covers the main elements of cooperation, *inter alia*: a) assured access of the EU to NATO planning capabilities with a view to effective use in the context of military planning of EU-led crisis management operations; b) assured access to NATO's collective assets and capabilities (communication units, headquarters, etc.) for EU-led crisis management operations; and c) integration into NATO's longstanding defence planning system regarding the military requirements and capabilities which may be needed for EU-led military operations, in order to guarantee the availability of well-equipped forces trained for either NATO-led or EU-led operations, etc [72].

As claimed by Simon J. Smith, Berlin Plus can be reproduced from the agreements of 1996 between NATO and the Western European Union (Smith, 2013) [73].

De Hoop Scheffer argued that the BPA can be considered a milestone in NATO-EU relations (de Hoop Scheffer, 2007) [74]. However, he outlines that the BPA is only one which better match a situation in which the EU operate, especially when NATO is out of the same area (de Hoop Scheffer, 2008) [75]. In accordance with the document, NATO can provide support for EU operations even if NATO, as an organisation, is not directly involved [76].

Later, de Hoop Scheffer (2008) concluded that the BPA limits certain activities and has been seen "*too often [as] a straitjacket rather than a facilitator*." Smith agrees with him as he considers the formal arrangement to be constraining, rather than enabling [77].

Since the BPA, NATO and the EU cooperated with each other through Operation Concordia, which has been the first operation led by the EU, under the BPA. Operation Concordia has operated under the mandate of the EU and the command system and rules was manged by the EU. It is noteworthy that, on the strategic level, the Political and Security Committee (PSC) of EU and NATO's North Atlantic Council (NAC) (Mace, 2004) were responsible for the cooperation [78].

From the perspective of Lynch and Missiroli, it can be outlined that the objective of operation Concordia has been one of supporting a stable and secure environment and ensuring successful implementation of the Ohrid framework [79] since 2001 [80].

7. SUMMARY

The following conclusions can be drawn from an analysis of the documents/treaties and CBRN policies of both organisations: NATO and the EU share similar values, as enshrined in their Founding Treaties and reflected in their two Joint Declarations. Thus, their CBRN policies cover common principles, norms, values, defence and security policies, as well as common member states.

As for the dissimilarities, they can be seen in their crisis management and CBRN plans that regulate procedures on how to tackle CBRN incidents. Also, differences can be seen in non-shared Member States interest and in the ambitions to preserve the autonomy of their country at the international level.

In addition, it is important to bear in mind that decisions are taken by consensus in NATO and by consensus (sanctions) and qualified majority of countries in the EU. It depends mostly on the issues under discussion.

It can be stated that communication remains one of the most critical aspects of cooperation and coordination. As mentioned previously, basically, communication between these two organisations is ongoing in the form of *ad hoc* communication or via a mediator such as UN OCHA [81].

However, regardless of a few exceptions, generally speaking the members of NATO and the EU stand ready to intensify cooperation not only within the framework of these organisations but also beyond, in other formats of cooperation [82].

As already mentioned, the main issues with bilateral cooperation between NATO and the EU are related to hybrid threats, terrorism, migration, cyberthreats, and a large-scale CBRN incident. So, both institutions require support from each other as well as assistance from other institutions in order to properly address any of the abovementioned challenges.

It is important to note that the benefits of sharing resources, capabilities and knowledge are remarkable and provide the advantage of being able to address hybrid issues that neither institution can do unilaterally. However, CBRN defence is an issue that should be addressed by NATO as the superior institution.

It is noteworthy that the lessons learned from NATO's operations in Afghanistan and the Western Balkans make it clear to both organisations that a comprehensive political, civilian and military approach is required to enable effective crisis management [83].

Moreover, it remains an open question as to whether NATO and the EU can increase and upgrade their level of cooperation. It must be stressed that several necessary steps remain to be taken in this regard.

8. RECOMMENDATIONS

It is reasonable to point out that there are some areas and directions of bilateral cooperation between NATO and the EU that still need to be improved.

First, the state of cooperation between two organisations needs to be enhanced, especially in the case of CBRN incidents. Because some major CBRN incidents have demonstrated that it is not fully clear how both organisations would respond to the emergency in synchrony and a collective manner.

Second, terrorism can be seen as a serious challenge requiring close cooperation with specific actors such as Europol, because terrorism is an internal European security problem. Moreover, there is a growing recognition of the destabilising effect of terrorism on the security of the EU and NATO.

Third, NATO should continue to strengthen its partnerships with international actors to improve common understanding of regional and global CBRN risks and threats and areas of shared responsibility and activity.

One of the recommendations can be seen as the creation of a common framework for cooperation. Both organisations need such a format to avoid overlap and duplication of their efforts in the CBRN field. This will allow them to share certain information about their plans, actions and exercises, and will make bilateral cooperation much more operational and well-organised. All of this will strengthen the synergy between NATO and the EU in responding adequately to CBRN threats.

NATO and the EU, together with their partners, should identify efforts that can enhance the security of both organisations in the areas of building CBRN defence capabilities, organising joint exercises and training, implementing security-related programmes and reforms, and civil preparedness. Bilateral relations can be developed through the organisation of joint events and other formats of dialogue between NATO and EU staff. Another possibility would be to invite each other to similar CBRN events.

However, these activities are not sufficient in themselves. There is also a need to share their objectives and, where possible, to identify common goals in the field of security in general and in the CBRN field in particular.

Communication continues to be seen as an important mechanism for building confidence and strengthening the partnership between NATO and the EU. As mentioned above, this can involve various channels, including communication between the CBRN focal points of both organisations. Other related actors and stakeholders may also be included in a crisis management communication platform in general.

Most importantly, both institutions must enhance the security not only of the shared, but also their non-shared Member States, which is essential for strategic purposes.

The best way to achieve the objectives of countering CBRN threats on a practical level is to organise many more joint exercises, where it is easier to identify caps, successes and capabilities. Testing technologies and training curricula in a real-life situation would be helpful for future objectives. In this context, the regular use of the capabilities of the joint NATO CBRN Defence Centre of Excellence (based in Vyškov) for the EU CBRN CoE initiative would be one of the recommendations for improving NATO-EU cooperation at the practical level.

Other recommendations deal with the harmonisation of the training curricula of both organisations, as well as the training itself. Of course, both the EU and NATO have their own CBRN training curricula and modus operandi, but there is a need to synchronise them. This would allow the CBRN personnel of each organisation to know what the other is doing and who is doing what. However, any cooperation should also take into account any institutional interests and respect the autonomy of both institutions and individual Member States [84].

Indeed, the Treaty on the Non-Proliferation of Nuclear Weapons remains the main pilar against the spread of nuclear weapons. NATO and the EU should therefore continue to support the policy and objectives of the Organisation for the Prohibition of Chemical Weapons, the Organisation for Security and Cooperation in Europe, the Comprehensive Test-Ban Treaty Organisation, and the International Atomic Energy Agency, and to strengthen the implementation of the Biological and Toxin Weapons Convention.

Effective cooperation with the UN as a global actor in global security, including in the CBRN domain, is also crucial for both NATO and the EU.

Today's world is interlinked with common security challenges. For example, NATO and the EU should always be able to adapt to such significantly changed CBRN threats from both state and non-state actors, including challenges to arms control, disarmament and non-proliferation regimes, and to the risks posed by uncontrolled technologies.

In principle, NATO and the EU have a wide range of instruments at their disposal to respond adequately to CBRN challenges. To achieve this goal, both organisations should build up capabilities that can be used effectively in a CBRN incident. The idea is to create a single CBRN force (proposed by Tamara J. Bijl) by combining the CBRN defence capabilities of both organisations. This is an interesting idea that at least needs to be discussed. The rationale for this recommendation reflects the situation that the modern world would face in the case of a large-scale CBRN incident and, especially, with the COVID-19 epidemic.

In conclusion, it is safe to assume that the crisis in the realm of nuclear arms control will continue to pose challenges to European security, especially in light of the current security situation in Europe. Russia's decision to undermine the international order and the European security system through its aggression against Ukraine violated international law, including a number of arms control agreements.

That is why the effective partnership between NATO and the EU is so important. Together, NATO and the EU can play a mutually reinforcing role in supporting world peace, where only such cooperation can guarantee a secure international political and security system.

ENDNOTES

[1] European Parliament, 018)0513, Resolution on the annual report on the implementation of the Common Foreign and Security Policy (2018/2097(INI)), (2020/C 388/08) Official Journal of the European Union, 12 December 2018,

[2] Council of the European Union, European security strategy a secure Europe in a better world, ISBN 978-92-824-2421-6, 2009, p. 7

[3] A. Oppenheimer, Chemical Weapons in the 21st Century: Syria and Beyond, *the security almanac,* Military Technology, 11/2013, p. 60

[4] Council Regulation (EC) no. 1717/2006 of the European Parliament and of the Council of 15 Nov. 2006 establishing an Instrument for Stability, *Official Journal of the European Union,* L327, 24 Nov. *2006*

[5] M Bonfanti and. E. F. Capone, Fostering a comprehensive security approach: an exploratory case study of CBRN crisis management frameworks in eleven European countries, *information & security: an international journal* vol.33:1, 2015, pp. 55-80

[6] A. kasznár, New Tendencies in the Terrorist Attacks Against Europe, *The Security Compendium 3rd Edition,* 11/2014, p. 143

[7] European Commission, communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Brussels, 24.6.2009, COM(2009) 273 final P8_TA(2018)0514

[8] European Union, EU Chemical, Biological, Radiological and Nuclear Risk Mitigation Centres of Excellence (CoE),
from https://europa.eu/cbrn-risk-mitigation/index_en

[9] European Parliament, resolution of 29 April 2015 on the Court of Auditors' special reports in the context of the 2013 Commission discharge. Document P8 TA (2015)0119, 2015

[10] NATO (2019a). Guidelines for Civil-Military Medical Cooperation in response to Chemical, Biological, Radiological and Nuclear (CBRN) Mass Casualty Incidents. Pp. 3-4.

[11] W. Wojtas, Action Plan to enhance preparedness against CBRN security risks. Presentation at Conference for Community of Users. BAO Congress Centre, Brussels. 2019, Retrieved from https://www.securityresearch-cou.eu/13th-Meeting-CoU

[12] R. Krause, JCBRN Defence COE, Comprehensive Publication on Civil – Military& NATO – EU Cooperation, part I, Cross-Border Cooperation in Case of CBRN incident – EXTRACT, (JCBRN Defence COE); 2021 p. 21, www.jcbrncoe.or

[13] A. Herciu, Use of CBRN defence structures in CBRN consequences management, *international scientific conference strategies xxi - volume 2,* 2018, p. 4, url: https://www.ceeol.com/search/chapter-detail?id=741330

[14] NATO's chemical, biological, Radiological and Nuclear (CBRN) Defence policy 5 Ju. 2022, retrieved on 3 October 2022, https://www.nato.int/cps/en/natohq/index.htm

[15] Ibid

[16] E. Tamara Janette Bijl, NATO-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, 2021 p. 121

[17] NATO's chemical, biological, Radiological and Nuclear (CBRN) Defence policy, op. cit.

[18] NATO, The Alliance's Strategic Concept approved by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, DC, on 23–24 Apr. 1999, press release NAC-S (99) 65, 24 April. 1999, URL <http://www.nato.int/docu/pr/1999/p99-065e.htm.

[19] NATO's chemical, biological, Radiological and Nuclear (CBRN) Defence policy, op. cit.

[20] NATO Handbook, key to the principal NATO committees and to institutions of cooperation, partnership and dialogue, Key to the principal NATO committees, Senior Politico-Military Group on Proliferation, Chapter 13: URL http://www.nato.int/docu/handbook/2001/hb130116.htm

[21] M. Mureşan, D. Muresan, NATO transformation and expansion, *Strategic Impact 1:5-10.* Issue: *1/2007, p.* 2 *The Central and Eastern European Online Library*, https://www.ceeol.com/search/article-detail?id=836166

[22] M. Mureşan, D. Muresan, NATO transformation and expansion, op. cit. p. 2

[23] E. Tamara Janette Bijl, Nato-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, op. cit. p. 111

[24] Z. Hýbl, CBRN Defence COE, Comprehensive Publication on Civil – Military& NATO – EU Cooperation, part IV, NATO's involvement in Crisis Management and Disaster Response – COVID-19: Legal Considerations, p. 209, 2011

[25] J. R. Krause, JCBRN Defence COE, Comprehensive Publication on Civil – Military& NATO – EU Cooperation, part I, Cross-Border Cooperation in Case of CBRN incident – EXTRACT, op. cit.

[26] NATO multinational chemical, biological, radiological and nuclear defence battalion. retrieved from shape (n.d.b).

[27] NATO (2020d). Combined Joint Chemical, Biological, Radiological and Nuclear Defence Task Force. Retrieved from NATO - Topic: Combined Joint Chemical, Biological, Radiological and Nuclear Defence Task Force

[28] NATO's chemical, biological, Radiological and Nuclear (CBRN) Defence policy, op. cit.

[29] NATO's chemical, biological, Radiological and Nuclear (CBRN) Defence policy, op. cit.

[30] M. Mureşan, D. Muresan, NATO transformation and expansion, op. cit. p. 2

[31] G. W. Bretschneider, Cooperation in Natural Disaster Management and Prevention Coordination between States and between Military and Civilian Actors, Case Study: NATO's Involvement in Pakistan Earthquake Relied in 2005, Presented by G. W. Bretschneider, 22nd *OSCE Economic and Environmental Forum "Responding to environmental challenges with a view to promoting cooperation and security in the OSCE area", First Preparatory Meeting*, Vienna, 27-28 January 2014, Session IV

[32] Assistance provided to the United States in 2005 after Katrina hurricane; Assistance provided to Pakistan in 2005 after the devastating earthquake; etc.

[33]https://trainingportal.jcbrncoe.org/index.php

[34] Ibid

[35] NATO’s chemical, biological, Radiological and Nuclear (CBRN) Defence policy, op. cit.

[36] Ibid

[37] E. Tamara Janette Bijl, Nato-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, op. cit. p. 110

[38] Ibid, p. 110

[39] B. Allert & Z. Kralikova, JCBRND COE Advisors Conference 2019. Retrieved from JCBRND COE Advisors Conference 2019 (jcbrncoe.cz)

[40] B. Allert, First JCBRND COE Advisors Conference. *Presentation,* ATA (2017). *Final Report: Chemical, Biological, Radiological, and Nuclear Threats.* 2020). Retrieved from https://images.politico.eu/wp-content/uploads/2017/11/CBRN-Final-Report.pdf

[41] E. Tamara Janette Bijl, Nato-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, op. cit. p. 92

[42] Council of the European Union, Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, p. 4, Brussels, 6 December 2016 (OR. en) 15283/16

[43] European Commission, *Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks*, 2017 Brussels 20171018_action_plan_to_enhance_preparedness_against_chemical_biological_radiological_and_nuclear_security_risks_en.pdf (europa.eu)

[44] E. Tamara Janette Bijl, Nato-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, op. cit. p. 125

[45] Policy Department for External Relations Directorate General for External Policies of the Union “EU preparedness against CBRN weapons” p. 9, PE 603.875, January 2019 https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603875/EXPO_STU(2019)603875_EN.pdf

[46] E. Tamara Janette Bijl, Nato-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, op. cit. p. 109

[47] A. Stan, D. Perkins, United Nations Security Council resolution 1540: a military perspective, *Central and Eastern European Online Library,* 2013, p. 2 https://www.ceeol.com/search/article-detail?id=832228

[48] E. Tamara Janette Bijl, Nato-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, op. cit. p. 98

[49] Z. Hýbl, JCBRN Defence COE, Comprehensive Publication on Civil – Military& NATO – EU Cooperation, part IV, NATO’s involvement in Crisis Management and Disaster Response – COVID-19: Legal Consideration; op. cit. p. 230, 2021

[50] NATO's chemical, biological, Radiological and Nuclear (CBRN) Defence policy by 5 July 2022, op. cit.

[51] NATO & EU Fifth progress report of 2020 on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017, p. 144

[52] Tamara Janette Bijl, NATO-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, op. cit. p. 124

[53] N. Græger, European security as practice: EU–NATO communities of practice in the making? *European Security,* 25:4, 478-501, DOI: 10.1080/09662839.2016.123602, 2016

[54] NATO, *NATO, EU Ambassadors hold joint informal talks on Ukraine*. NATO. (2014).Retrieved 15 May 2020, from https://www.nato.int/cps/en/natolive/news_107742.htm.

[55] The eNOTICE Project. H2020 (n.d.a). Retrieved from Project (h2020-enotice.eu)

[56] J. C. Juncker, J. Stoltenberg & D. Tusk, Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 2016

[57] E. Tamara Janette Bijl, Nato-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, op. cit. p. 28

[58] Ibid p. 27

[59] Ibid p. 128

[60] Ibid p.123

[61] M. Cebeci, The European Union and Weapons of Mass Destruction Terrorism, Defence Against Terrorism Review, Vol. 5, No. 1, Spring & Fall 2013, p. 67

[62] Ibid

[63] J. R. Krause, JCBRN Defence COE, Comprehensive Publication on Civil – Military& NATO – EU Cooperation, part I, Cross-Border Cooperation in Case of CBRN incident – EXTRACT, op. cit. p. 38, 2021

[64] E. Tamara Janette Bijl, Nato-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, op. cit. p. 124.

[65] J. R. Krause, JCBRN Defence COE, Comprehensive Publication on Civil – Military& NATO – EU Cooperation, part I, Cross-Border Cooperation in Case of CBRN incident – EXTRACT, op. cit. p. 54

[66] I. Angelov, the new partner of the European Union in the field of security and defense, *scientific research and education in the air force*, 2018, p. 14

[67] Council of the European Union, Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, p. 2 Brussels, 6 December 2016 (OR. en) 15283/16

[68] https://www.nato.int/cps/en/natolive/official_texts_19544.htm, retrieved on 8 October, 2022

[69] J. R. Krause, JCBRN Defence COE, Comprehensive Publication on Civil – Military& NATO – EU Cooperation, part I, Cross-Border

Cooperation in Case of CBRN incident – EXTRACT, op. cit. p. 78

[70] Ibid p. 54

[71]https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/berlinplus_/berlinplus_en.pdf, retrieved on 8 October, 2022

[72]https://eur-lex.europa.eu/EN/legal-content/summary/cooperation-with-nato.htmlm, retrieved on 8 October, 2022

[73] S. J. Smith, the European Union and NATO Beyond Berlin Plus: the institutionalisation of informal cooperation (PhD). Loughborough University, 2013

[74] J. de Hoop Scheffer, *NATO and the EU: Time for a New Chapter*, Speech (2007) Berlin, Germany.

[75] J. de Hoop Scheffer, Speech (2008) by NATO Secretary General Jaap de Hoop Scheffer at the High-level seminar on relations between the European Union and NATO. JFC Brunssum, Netherlands.

[76] E. Tamara Janette Bijl, Nato-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, op. cit. p. 103

[77] S. J. Smith, the European Union and NATO Beyond Berlin Plus: the institutionalisation of informal cooperation, op. cit.

[78] C. Mace, Operation Concordia: developing a 'European' approach to crisis management? *International Peacekeeping,* 11(3), 475-187. 2004

[79] The Ohrid Agreement created a framework for North Macedonia as a civic state, ending the armed conflict between the National Liberation Army and the security forces of Macedonia. https://en.wikipedia.org/wiki/Ohrid_Agreement

[80] M. Lewis-Beck, & T. Liao, Encyclopedia of Social Science Research Methods (1st ed., pp. 1143-1144). *SAGE Publications, Inc.: Thousand Oaks*, 2004.

[81] E. Tamara Janette Bijl, Nato-EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents, op. cit. p 130

[82] Ibid p. 131

[83] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, adopted by Heads of State and Government at the NATO Summit in Lisbon 19 – 20 November 2010

[84] J. R. Krause, JCBRN Defence COE, Comprehensive Publication on Civil – Military& NATO – EU Cooperation, part I, Cross-Border Cooperation in Case of CBRN incident – EXTRACT, op. cit. p. 31

REFERENCES

[1] A. Oppenheimer, Chemical Weapons in the 21st Century: Syria and Beyond, *The security almanac*, Military Technology, 11/2013

[2] M Bonfanti and. E. F. Capone, Fostering a comprehensive security approach: an exploratory case study of CBRN crisis management frameworks in eleven European countries, *Information & security: an international journal* vol.33:1, 2015

[3] A. kasznár, *New Tendencies in the Terrorist Attacks Against Europe*, The

Security Compendium 3rd Edition, 11/2014

[4] W. Wojtas, *Action Plan to enhance preparedness against CBRN security risks*. Presentation at Conference for Community of Users. BAO Congress Centre, Brussels, 2019, Retrieved from https://www.securityresearch-cou.eu/13th-Meeting-CoU

[5] J. R. Krause, JCBRN Defence COE, *Comprehensive Publication on Civil – Military& NATO – EU Cooperation*, part I Cross-Border Cooperation in Case of CBRN incident – EXTRACT, (JCBRN Defence COE); p. 38, 2021 www.jcbrncoe.org

[6] A. Herciu, *Use of CBRN defence structures in CBRN consequences management*, International scientific conference strategies xxi - volume 2, 2018, p. 4, url: https://www.ceeol.com/search/chapter-detail?id=741330

[7] E. Tamara Janette Bijl, *NATO - EU cooperation, with special focus on coordination and interaction, in case of large-scale CBRN incidents*, 2021

[8] M. Mureşan, D. Muresan, *NATO transformation and expansion*, Strategic Impact 1:5-10. Issue: 1/2007, p. 2 The Central and Eastern European Online Library, https://www.ceeol.com/search/article-detail?id=836166

[9] Z. Hýbl, CBRN Defence COE, *Comprehensive Publication on Civil – Military& NATO – EU Cooperation*, part IV, NATO's involvement in Crisis Management and Disaster Response – COVID-19: Legal Considerations, 2011

[10] R. Krause, *JCBRN Defence COE, Comprehensive Publication on Civil – Military& NATO – EU Cooperation*, part I Cross-Border Cooperation in Case of CBRN incident – EXTRACT, (JCBRN Defence COE); p. 38, 2021 www.jcbrncoe.org

[11] B. Allert, First *JCBRND COE Advisors Conference,* Presentation, ATA Final Report: Chemical, Biological, Radiological, and Nuclear Threats. 2017. https://images.politico.eu/wp-content/uploads/2017/11/CBRN-Final-Report.pdf

[12] B. Allert & Z. Kralikova, JCBRND COE Advisors Conference 2019, Retrieved from JCBRND COE Advisors Conference 2019 jcbrncoe.coe

[13] J. R. Krause, *JCBRN Defence COE, Comprehensive Publication on Civil – Military& NATO – EU Cooperation*, part I Cross-Border Cooperation in Case of CBRN incident – EXTRACT, (JCBRN Defence COE); p. 38, 2021 www.jcbrncoe.org

[14] I. Angelov, *The new partner of the European Union in the field of security and defense*, Scientific research and education in the air force, National Military University „Vasil Levski“ AFASES, 2018

[15] N. Græger, *European security as practice: EU–NATO communities of practice in the making?*, European Security, DOI: 10.1080/09662839.2016.1236021, 2016.

[16] J. C. Juncker, J. Stoltenberg & D. Tusk, *Joint declaration on EU-NATO cooperation* by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 2018.

[17] M. Cebeci, *The European Union and Weapons of Mass Destruction Terrorism*, Defence Against Terrorism Review, Vol. 5, No. 1, Spring & Fall 2013.

[18] S. Smith, *The European Union and NATO Beyond Berlin Plus: the institutionalisation of informal cooperation (PhD)*, Loughborough University 2013.

[19] J. de Hoop Scheffer, *NATO and the EU: Time for a New Chapter*, Speech, 2007, Berlin, Germany.

[20] J. de Hoop Scheffer, Speech by NATO Secretary General Jaap de Hoop Scheffer at the High-level seminar on relations between the European Union and NATO, Speech, JFC Brunssum, Netherlands, 2008.

[21] C. Mace, Operation Concordia: developing a 'European' approach to crisis management? *International Peacekeeping*, *11*(3), 2004.

[22] M. Lewis-Beck & T. Liao, *Encyclopedia of Social Science Research Methods* (1st ed., pp. 1143-1144). SAGE Publications, Inc.: Thousand Oaks, 2004.

[23] A. Stan & D. Perkins, *United Nations Security Council resolution 1540: a military perspective*, Central and Eastern European Online Library, 2013, https://www.ceeol.com/search/article-detail?id=832228

[24] European Commission, communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Brussels, 24.6.2009, COM(2009) 273 final P8_TA(2018)0514

[25] Council of the European Union, *European security strategy a secure Europe in a better world*, ISBN 978-92-824-2421-6,

[26] European Union, *EU Chemical, Biological, Radiological and Nuclear Risk Mitigation* Centres of Excellence (CoE), from https://europa.eu/cbrn-risk-mitigation/index_en

[27] European Commission, *Establishing an instrument for stability*, regulation (EC) no 1717/2006 of the European Parliament and of the council of 15 November 2006, official journal of the European Union 24.11.2006 l 327/1.

[28] Council of the European Union, *Council Conclusions on the Implementation of the Joint Declaration* by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, Brussels, 6 December 2016 (OR. en) 15283/16

[29] European Commission, *Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks*, 2017 Brussels, Retrieved from 20171018_action_plan_to_enhance_preparedness_against_chemical_biological_radiological_and_nuclear_security_risks_en.pdf (europa.eu)

[30] Policy Department for External Relations Directorate General for External Policies of the Union "*EU preparedness against CBRN weapons*" p. 9, PE 603.875, January 2019

https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603875/EXPO_STU(2019)603875_EN.pdf

[31] European Parliament, *Resolution of 29 April 2015* on the Court of Auditors' special reports in the context of the 2013 Commission discharge. Document P8_TA(2015)0119, 2015

[32] European Parliament, 018) 0513, *Resolution on the annual report on the implementation of the Common Foreign and Security Policy* (2018/2097(INI)), (2020/C 388/08) 12 December 2018, Official Journal of the European Union

[33] North Atlantic Treaty Organization, *NATO Guidelines for Civil-Military Medical Cooperation in response to Chemical, Biological, Radiological and Nuclear (CBRN) Mass Casualty Incidents*, 2019.

[34] NATO's chemical, biological, Radiological and Nuclear (CBRN) Defence policy 5 July 2022, retrieved on 3 October 2022, https://www.nato.int/cps/en/natohq/index.htm

[35] North Atlantic Treaty Organization, *The Alliance's Strategic Concept*, Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, DC, on 23–24 Apr. 1999, press release NAC-S (99) 65, 24 Apr. 1999, URL http://www.nato.int/docu/pr/1999/p99-065e.htm

[36] NATO Handbook, key to the principal NATO committees and to institutions of cooperation, partnership and dialogue, Key to the principal NATO committees, Senior Politico-Military Group on Proliferation, Chapter 13: URL http://www.nato.int/docu/handbook/2001/hb130116.htm

[37] North Atlantic Treaty Organization, Enlargement, 2020a. Retrieved from NATO - Topic: Enlargement

[38] NATO & EU Fifth progress report of 2020 on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017

[39] North Atlantic Treaty Organization, NATO, EU Ambassadors hold joint informal talks on Ukraine, 2014. Retrieved https://www.nato.int/cps/en/natolive/news_107742.htm

[40] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, adopted by Heads of State and Government at the NATO Summit in Lisbon 19 – 20 November 2010

[41] OSCE, Cooperation in Natural Disaster Management and Prevention Coordination between States and between Military and Civilian Actors, Case Study: NATO's Involvement in Pakistan Earthquake Relied in 2005, Presented by G. W. Bretschneider, 22nd OSCE Economic and Environmental Forum "Responding to environmental challenges with a view to promoting cooperation and security in the OSCE area", First Preparatory Meeting, Vienna, 27-28 January 2014, Session IV

[42] The Ohrid Agreement created a framework for North Macedonia as a civic state, ending the armed conflict between the National Liberation Army and the security forces of Macedonia.

https://en.wikipedia.org/wiki/Ohrid_Agreement

[43]https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/berlinplus_/berlinplus_en.pdf

[44]https://www.nato.int/cps/en/natolive/official_texts_19544.htm

[45]https://trainingportal.jcbrncoe.org/index.php

[46]https://eur-lex.europa.eu/EN/legal-content/summary/cooperation-with-nato.htmlm

[47] European Union, EU Chemical, Biological, Radiological and Nuclear Risk Mitigation Centres of Excellence (CoE), from https://europa.eu/cbrn-risk-mitigation/index_en

[48] The eNOTICE Project. H2020 (n.d.a). Retrieved from Project (h2020-enotice.eu)

THE IMPORTANCE OF ARTIFICIAL INTELLIGENCE IN THE WORLD AND THE PROBLEMS RELATED TO IT

Anuki TOGONIDZE

Ministry of Defense, Tbilisi, Georgia

The actual issue of the twenty-first century is determining the essence, importance, application areas of digital technologies and their impact on the economy. Digital technologies are a discrete (intermittent) system based on information coding and transmission methods, which allows multi-planned tasks to be performed in the shortest possible time; Technologies are used to collect, store, process, retrieve, and transmit data in electronic form. Software and hardware tools and systems depend on their functionality. They are in demand in all sectors of the economy as creators of new markets and transformers of business processes.

The components of the technology are the devices, but the main thing is through which these transformations are carried out. Innovation is what makes technological progress happen. High technologies (Hi-Tech) are used in all spheres of human activity today. Its use in the economy causes special changes. Its development trends are changing. With the help of technology, the prosperity and competitiveness of the country increases. It increases the inflow of investments and facilitates the launch of new start-up businesses.

Fast and accurate information delivery is impossible without digital technologies. These technologies are driving the forms of business management that are being introduced worldwide and whose goal is to reduce costs, simplify the service field, make it faster and more flexible, and replace manual work.

The most important technologies of the fourth industrial revolution are the Internet of Things, 3D printing, artificial intelligence, machine learning, robotics, big data, and others. However, today we will briefly review the stages of artificial intelligence's development worldwide.

Key words: *artificial intelligence, digital technologies, industrial revolution.*

1. INTRODUCTION

Artificial intelligence (AI) is a branch of computer science that aims to create an intelligent computer machine/program that can understand human intelligence. Determining the level of intelligence depends on what task we set out to solve.

The Council of Europe defines artificial intelligence as: *"a set of sciences, theories, technologies, the purpose of which is to reproduce human cognitive skills by a machine"*. Given the current level of development, artificial intelligence means delegating complex intellectual tasks performed by a human to a machine."

Artificial intelligence works like human intelligence, but notably it lacks creativity and inspiration. Its use in routine processes is quite simple. To perform similar tasks, artificial intelligence algorithms are being created, which can be predicted, and guessed.

AI has the potential to transform a wide range of industries, however, there is still much uncertainty about the exact impact of AI.

As for the use of artificial intelligence in business, it helps to increase financial well-being.

PricewaterhouseCoopers (PwC) predicts in a report that by 2030 artificial intelligence will bring $15.7 trillion in financial benefits to the global economy. In Thailand, mobile operator AIS opened its first store without staff. The robot "*Lisa*" works there, which is controlled by artificial intelligence and provides general information to the user.

Studies show that the use of artificial intelligence in healthcare could potentially generate $150 billion in annual savings for the US healthcare economy by 2026. Robots, AI, machine learning, and automation will replace 16% of US jobs by 2025. The impact of AI technologies on business will help increase labor productivity by up to 40%.

Artificial intelligence, like other technologies, has positive characteristics as well as negative ones, which are discussed in the world. For example, the English astrophysicist Stephen Hawking believed that the destroyer of humanity is artificial intelligence. His abilities are so great that he can replace a person. And with this, humanity has reached the *"point of no return"*. He believed that the use of artificial intelligence for military purposes was unacceptable. To control this technology, it is necessary to create "some form of world government".

A good example of his point being ignored is the USA and Russia, which are striving to create weapons controlled by artificial intelligence, of course for military use. This event is already called a technological singularity.

The Summit on Responsible Artificial Intelligence in the Military Domain (REAIM) was held in The Hague in 2023. A document (Call to Action) was adopted within the summit, which defines what dangers the uncontrolled use of AI may contain. It calls on states to develop a national legal framework for artificial intelligence.

At the summit, the USA presented a political declaration on the responsible use of artificial intelligence in the military dimension. The purpose of the declaration is to build an international consensus on how militaries can responsibly use AI during military operations. It also aims to help states develop and use this technology for defense purposes while respecting international law, and ensuring security and stability.

The Declaration provides non-legally binding guidelines that describe best practices for the responsible use of AI in the defense context. This means, among other things, that military AI systems are auditable, have explainable and well-defined uses, are subject to comprehensive testing, and can be deactivated in the event of malfunction. The US State Department believes that the mentioned declaration may become the basis for the development of international norms and principles for the responsible use of AI in the military dimension.

Notably, the US National Artificial Intelligence Act, initiated in 2020 and enacted into law in 2021, defines *artificial intelligence* as *„An automated machine-based system that can make predictions, recommendations, or decisions for human-defined objects to influence real or virtual environments”*.

For years, AI was an isolated phenomenon that was used on a limited theoretical level in narrow circles. Along with the development of technologies, AI has gained special relevance. Since global aggressive forces are actively looking for easy and cheap means to influence the national security systems of opponents, in recent times, the use of AI for malicious purposes is increasing.

Based on the above, Western states are trying to pay significant attention to the phenomenon of AI and to develop international legal norms that will bring the actions of states regarding the use of AI into a certain legal framework. That is why the REAIM summit and the political declaration initiated by the USA were an important step forward in the mentioned direction. In addition, it should be emphasized that according to the National Cyber Security Strategy of Georgia, Georgia considers AI only in the context of cyber security.

2. THE IMPACT OF ARTIFICIAL

INTELLIGENCE ON THE ECONOMY

Regarding the contribution of artificial intelligence to the economy, there is still much uncertainty about the exact impact of this technology on economic growth, especially in the context of gross domestic product (GDP).

The impact of artificial intelligence on the economy is still being researched worldwide. However, few studies have attempted to evaluate the benefits of the technology. A study by Brynjolfsson and McAfee found (Brynjolfsson, 2014) that artificial intelligence has the potential to increase economic growth by up to 1.7% per year in the United States alone.

Other studies have shown that artificial intelligence can lead to significant increases in productivity in a wide range of industries, from manufacturing to healthcare (McKinsey Global Institute (MGI), 2018), but as mentioned there are concerns around the world that the use of AI can have negative effects.

A McKinsey Global Institute study suggests that artificial intelligence could add $3.5 trillion to $5.8 trillion to the global economy by 2030. Research suggests that AI could boost productivity and create new jobs, particularly in healthcare, retail, and manufacturing. AI can also lead to income inequality (McKinsey Global Institute, 2017).

The study by Wagner, Schoenherr, and Pfohl builds on an analysis of the existing literature and examines the impact of AI on GDP in 42 countries. The authors use the data using regression analysis to estimate the impact of AI on GDP and control for other factors that may affect GDP.

Research shows that AI has a positive impact on GDP and that the impact is stronger in high-income countries. Research also suggests that education and research and development (R&D) are essential to maximizing the benefits of artificial intelligence. The results of the mentioned research show the positive impact of artificial intelligence on GDP (Schoenherr, 2020).

The authors found that a 10% increase in investment in AI (as measured by the number of AI patents per capita) is associated with a 0.3% increase in GDP. The authors also found that the impact of AI on GDP is stronger in high-income countries and the service sector than in other sectors. Research has found that AI has a positive impact on labor productivity. The positive effect of AI on GDP is more pronounced in countries where higher education is at a high level and attention is paid to the research and development part (Schoenherr, 2020).

Studies have been conducted on countries such as the USA, China, Japan, Germany, Great Britain, and others.

It is worth noting here the research conducted by Georgian scientists, which calculates the impact of artificial intelligence on GDP. They use regression analysis to calculate all this and propose the following formula:

*GDP_t = GDP_(t-1) * (1 + g_t)*, where:

- *GDP_t*: gross domestic product at time t;
- *GDP_(t-1)*: gross domestic product (t-1) in time;
- *g_t*: GDP growth rate at time t, which is a function of AI adoption, productivity growth, innovation, job mobility, and income inequality.

Here, the GDP growth rate (g_t) can be broken down as follows: *g_t = f(AI_t, P_t, I_t, J_t, Y_t)*, where:

- *AI_t*: AI adoption index at time t, representing the level of AI integration in the economy;
- *P_t*: productivity gains at time t as a result of adopting AI;
- *I_t*: innovation index at time t, indicating the extent to which artificial intelligence drives the creation of new industries and technologies;
- *J_t*: index of job change at time t, reflecting the negative impact of artificial intelligence on employment;
- *Y_t*: index of income inequality at time t, which accounts for the effects of artificial intelligence on income;

The relationship between these variables can be specified as follows:

*P_t = α_1 * AI_t;*
*I_t = α_2 * AI_t;*
*J_t = β_1 * AI_t;*
*Y_t = β_2 * AI_t*.

- *α_1* and *α_2* are positive parameters representing the impact of AI adoption on productivity growth as well as innovation.
- *β_1* and *β_2* are negative parameters representing the impact of AI adoption on job change and income inequality.

Substituting these relationships into the GDP growth rate equation, we get the following model:

*g_t = f(α_1 * AI_t, α_2 * AI_t, β_1 * AI_t, β_2 * AI_t*

As a result, they found that AI has both positive and negative effects on GDP growth. While the adoption of AI leads to increased productivity and innovation, it also promotes job changes and income inequality, which may not bode well for long-term economic growth.

3. CALCULATION OF THE ARTIFICIAL INTELLIGENCE IMPACT ON THE GROSS DOMESTIC PRODUCT (GDP)

Based on the research in the world, we developed a methodology (approach) mathematical model (regression analysis) that takes into account several key variables such as AI investment, AI adoption, and AI quality, which calculates the impact of artificial intelligence on GDP.

$GDP = \alpha + \beta 1AI\ investment + \beta 2AI\ intake + \beta 3AI\ quality + \varepsilon$

where *GDP* is the dependent variable, *AI investment*, *AI adoption*, and *AI quality* are the independent variables, and ε is the error term.

Investment in AI refers to the amount spent on research and development, as well as the implementation and maintenance of artificial intelligence technologies. The level of investment in AI can have a major impact on the development and use of these technologies, as well as their quality and capabilities.

AI adoption refers to the extent to which AI technologies are used by businesses, organizations, and individuals in a given country. The level of adoption can be influenced by factors such as the availability of financing, the regulatory environment, and the overall level of technological development in a country.

AI quality refers to the efficiency, reliability, and accuracy of artificial intelligence technologies. The quality of AI can be affected by a variety of factors, including the quality of the data used to train and test AI algorithms, the sophistication of the algorithms themselves, and the level of expertise of the researchers and engineers working on the AI development.

Together, these variables can help explain the relationship between AI and GDP because, as we have seen, countries that invest more in AI are more likely to adopt AI technologies and produce higher-quality AI, so they will reap greater economic benefits from this. From technologies. However, as we know, everything has both positive and negative sides. We have seen that certain factors affect GDP in different ways.

However, as for the mathematical model proposed by us, it is worth noting the fact that the compilers of the formula are currently incomplete in the world. When their indices appear on the financial markets after that, it will be possible to calculate the mentioned formula better. Therefore, it is necessary to continue research in this direction.

Therefore, in time (when the compilers exist), this research will be of great importance to policymakers trying to promote economic growth through investments in artificial intelligence. As we've seen from research, increased investment in AI can lead to significant gains in GDP, especially in industries with high potential for automation and productivity growth. However, we also saw that the impact of AI on GDP varies across countries, highlighting the importance of developing a tailored approach to AI investments based on a country's unique economic and social context.

However, there is still much uncertainty about the potential impact of technology on employment. Its implementation may lead to job cuts, but on the positive side, it may lead to new jobs and new industries.

4. CONCLUSION

Given the dynamics of the world and Georgia's vulnerability to network-based technologies, it is important that relevant government agencies pay more attention to the phenomenon of AI in the context of national security. However, it is important that national-level strategic documents properly reflect AI and the future threat from it.

REFERENCES

[1] Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. https://psycnet.apa.org/record/2014-07087-000

[2]Notes from the AI frontier: modeling the impact of AI on the world economy https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economy-September-2018.ashx

[3]Schoenherr, T., Wagner, S. M., & Pfohl, H. C. (2020). The impact of artificial intelligence on GDP: Evidence from 42 countries. Technological Forecasting and Social Change, 159, 120204

[4]Gondauri D., Batiashvili M. The impact of artificial intelligence on GDP: A global analysis, International Journal of Innovative Science and Research Technology. 2023. https://ijisrt.com/assets/upload/files/IJISRT23APR1794.pdf

[5]National Artificial Intelligence Act: https://www.congress.gov/116/bills/hr6216/BILLS-116hr6216ih.pdf

[6.] https://www.coe.int/en/web/human-rights-rule-of-law/artificial-intelligence/glossary

[7]https://www.pwc.com/gx/en/issues/data-and-analytics/artificial-intelligence.html

[8]https://www.marketer.ge/ais-shop-without-seller/

[9]https://blog.zoominfo.com/statistics-about-artificial-intelligence/

[10]https://www.government.nl/ministries/ministry-of-foreign-affairs/news/2023/02/16/reaim-2023-call-to-action

[11]https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/

CRITICAL INFRASTRUCTURES: EUROPEAN CONTEXT AND EVOLUTION OF THE LAW

Francesco TRINCHILLO

University of Rome Tor Vergata, Italy

This conceptual paper aims to investigate the European regulatory framework of topic "protection of critical infrastructures", starting from the genesis of the terminology up to the examination of the contents of the most recent European legislation. The normative study, initially, focuses on the contents of Directive 2008/114/EC - the first real European legislative reference - received in Italy with Legislative Decree 61 of 2011; the second part, instead, is dedicated to the analysis of the more recent Directive (EU) 2022/2557 which represents the current European regulatory instrument aimed to regulate a theme that has become increasingly central, also in light of the growing number of attacks against Member States. Directive (EU) 2022/2557, in addition to repeal the previous one, is proposed as a much broader and more complete rule capable of providing the elements to regulate a very complex topic. The paper shows how the European Union is making great efforts not only to regulate the matter, but also to clarify its boundaries and transversal aspects.

Key words: *privacy, behavior, challenges, regulation, solutions*

1. INTRODUCTION

The most developed countries are characterized, among other things, by having extensive and sometimes very complex infrastructure systems, which, as will be analyzed below, are defined as Critical Infrastructures, such as, for example, energy distribution networks and transport infrastructures. As specified in European legislation, a critical infrastructure is not necessarily constituted by a physical infrastructure but can also be represented by an immaterial system such as an IT system, which, even if it is not easily understood, makes the protection of these systems much more complex.

Critical Infrastructures can be subject first to malfunctions, linked to breakdowns or technological problems of various origins, but also to natural disasters and intentional attacks. The globalized society that is increasingly based on a complex system of interconnection both physical and digital, now present in all sectors, has determined that a very large amount of activity depends on the correct functioning of said systems, from this has derived a growing attention towards security, in this perspective, the concern to protect critical infrastructures has always increased. The terrorist attacks of 11 September 2001 in the United States and those that hit the subway and railways in Madrid in 2004 and in 2005 in London, have further highlighted the problem especially regarding intentional attacks. In fact, right after these events - first the United States and then Europe - have concentrated on a precise regulation of the topic, it is reiterated, of certain interest but also very complex. The attention of the countries, initially, focused - almost exclusively - on intentional attacks, especially terrorist ones; subsequently, starting from the occurrence of Hurricane Katrina in 2005, which had devastating effects on the city of New Orleans and the states of Louisiana, Alabama and Mississippi, up to the terrible flood that hit Valencia and the surrounding areas on 29 October 2024, the regulatory approach was recalibrated, reasoning in a multi-risk vision that also extended to natural disasters and technological accidents such as massive fires, explosions and dispersions of chemical or biological agents.

The European Union, in fact, today takes into consideration the totality of the risks that may arise, even if in many Member States the attention is still focused on the threat posed by terrorism. It is also true that, today, terrorist threats constitute an important alert factor for industrialized countries because, generally, they concern places of passage of large masses, such as railway stations, airports, maritime stations. It is therefore essential to provide adequate and increasingly updated legislation for the protection of Critical Infrastructures to protect the health and safety of citizens, but also to avoid undermining the economy of the Member States themselves.

2. CRITICAL INFRASTRUCTURES: FROM THE ORIGIN OF THE TERM TO THE FIRST REGULATION IN EUROPE

The term Critical Infrastructure was born in America with the enactment of the USA Patriot Act (acronym of Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act), federal law of the United States of America specifically approved on 26 October 2001 to fight terrorism following the attacks of 9 September 2001 that hit New

York and Washington, causing approximately 3,000 victims. In the law (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 26 October 2001, s. 1016) , the first definition of Critical Infrastructure is reported: “the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters”. In Europe, however, the concept began to be formalized on 20 October 2004 with the communication 702 from the Commission to the Council and the European Parliament to prepare a global strategy for the protection of Critical Infrastructures; the document presents a series of proposals to increase Member States' prevention, preparedness and response to terrorist attacks affecting critical infrastructures. In fact, similarly to the first definition of critical infrastructures born in the United States, the European Union, defining them as those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States (Communication from the Commission to the Council and the European Parliament of 20 October 2004). It is understood, therefore, that critical infrastructures are present in many sectors of the economy, including banking and finance, transportation and distribution, energy, services, healthcare, food supply and communications as well as essential public services. For some of these sectors, we cannot strictly speak of infrastructure, but they are still networks or distribution chains that provide a product or service of strategic importance.

The European Commission identifies the types of critical infrastructures (Communication from the Commission to the Council and the European Parliament of 20 October 2004):

- Energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system).
- Communications and Information Technology (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet).
- Finance (e.g. banking, securities and investment).
- Health Care (e.g. hospitals, health care and blood supply

facilities, laboratories and pharmaceuticals, search and rescue, emergency services).

• Food (e.g. safety, production means, wholesale distribution and food industry).

• Water (e.g. dams, storage, treatment and networks).

• Transport (e.g. airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems).

• Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials).

• Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments).

The European Commission's communication 702 was followed first by the publication of communication 576 of 11.17.2005 - better called Green Paper - and then by the Communication 786 of 12 December 2006, which established the principles, objectives and contents of the European Programme for Critical Infrastructure Protection (EPCIP). Specifically, these new issues contain the following key principles that guide the implementation of the programme (Communication from the Commission of 12 December 2006):

• Subsidiarity - The Commission's efforts in the CIP field will focus on infrastructure that is critical from a European, rather than a national or regional perspective. Although focusing on European Critical Infrastructures, the Commission may where requested and taking due account of existing Community competences and available resources provide support to Member States

Concerning National Critical Infrastructures.

• Complementarity - the Commission will avoid duplicating existing efforts, whether at EU, national or regional level, where these have proven to be effective in protecting critical infrastructure. EPCIP will therefore complement and build on existing sectoral measures.

• Confidentiality - Both at EU level and MS level, Critical Infrastructure Protection Information (CIPI) will be classified appropriately and access granted only on a need to know basis. Information sharing regarding CI will take place in an environment of trust and security.

• Stakeholder Cooperation - All relevant stakeholders will, as far as possible, be involved in the development and implementation of EPCIP. This will include the owners/operators of critical infrastructures designated as ECI as well as public authorities and other relevant bodies.

• Proportionality - measures will only be proposed where a need has been identified following an analysis of existing security gaps and will be proportionate to the level of risk and type of threat involved.

• Sector-by-sector approach - Since various sectors possess particular experience, expertise and requirements with CIP, EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors.

3. COUNCIL DIRECTIVE 2008/114/EC

The documents of 2004, 2005 and 2006 represent the theoretical basis that led to the approval of the Council Directive 2008/114/EC on 12.8.2008 "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" which in fact constitutes the first legislative reference in the European context on the theme of Critical Infrastructures. The directive, defines what is meant by Critical Infrastructure and European Critical Infrastructure (ECI): in the first case we are referring to: an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions; by European Critical Infrastructures, instead, we mean: critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States (Council Directive 2008/114/EC of 8 December 2008, art.2). The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure.

The Council Directive 2008/114/EC is limited to considering only the Energy (Electricity, oil and gas) and Transport (Road, rail, maritime, air) sectors, although it is expressly stated that the list of ECI sectors in itself does not generate a generic obligation to designate an ECI in each sector (Council Directive 2008/114/EC of 8 December 2008, annex 1). This last clarification demonstrates how the Council itself recognizes that the issue of critical infrastructures is strongly complex and not easily circumscribed within a defined scope. The document provides that each Member State identifies among its critical infrastructures those that can be designated as ECI in the sense that satisfy those cross-sectoral criteria and respond to the definitions reported above. The Council Directive does not limit to establish just this principle, but it indicates (Council Directive 2008/114/EC of 8 December 2008, annex 3) a procedure – essential but very effective - to allow each Member State to carry out an analysis with the aim of identifying only specific national critical infrastructures such as ECI; only the latter will be reported to the other Member States that may be significantly affected by such infrastructures.

According to the directive, the inter-sectoral criteria that in fact constitute the main parameter for the designation of an ECI are not generic, in fact, it is the directive itself that identifies them and groups them into the following three categories (Council Directive 2008/114/EC of 8 December 2008, art. 3), in this way as to allow the Member States have tangible and quantifiable indices:

a) casualties criterion (assessed in terms of the potential number of fatalities or injuries);

b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);

c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services).

Moreover, the Council Directive defines which owners/operators of ECI “means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive” (Council Directive 2008/114/EC of 8 December 2008, art. 2) and always according to the dictates of the directive, the Member States are required to prepare an Operator Security Plan (OSP) aimed to identify the safety solutions to protect the designated ECI (Council Directive 2008/114/EC of 8 December 2008, art. 5); the contents of the OSP must comply with the following procedure (Council Directive 2008/114/EC of 8 December 2008, annex 2):

1. identification of important assets;

2. conducting a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact;

3. identification, selection and prioritisation of countermeasures and procedures with a distinction between:

- permanent security measures, which identify indispensable security investments and means which are relevant to be always employed. This heading will include information concerning general measures such as technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems,

- graduated security measures, which can be activated according to varying risk and threat levels.

In addition to the preparation of OSP, each Member State is required to name, for each ECI identified, a Security Liasons Officer (SLO) (Council Directive 2008/114/EC of 8 December 2008, art. 6) who will act as a point of contact for safety issues between the owner/operator of the ECI and the competent authority of the Member State in order to allow maximum effectiveness for the exchange of useful information relating to the risks and threats identified.

For the role he/she is invested with, this figure must have high relational and managerial skills in addition to adequate training and technical competence that is as transversal as possible due to the nature of the problems he/she finds. The risks that arise, indeed, can be very varied, not only on a case-by-case basis, but because, sometimes, even a danger that is the object of a specific assessment can generate a chain reaction of other emergencies that, although of a totally different nature, are activated by the initial triggering event. Despite the SLO role being so important, the directive does not provide any indication on the nature and type of his/her role, his/her responsibilities and specific competences; without a doubt, it is advisable that the profile is chosen internally to the infrastructure considered in order to guarantee greater knowledge of the internal processes, this will favor the methods for implementing the actions useful for managing the activities specific to the role to be performed.

Since 2008, each Member State has implemented the Council Directive 2008/114/EC in a different way, for example Italy has approved the Legislative Decree N. 61 of 11 April 2011, which, therefore, establishes - at a national level - the guidelines for the designation of European

Critical Infrastructures identifiable on Italian territory. Moreover, this law aims to introduce the Interministerial Situation and Planning Unit (defined with Italian acronym NISP) (Legislative Decree of President of Italian Republic N. 61 of 11 April 2011, art. 4), which, among other things, is assigned the tasks for the identification and designation of the ECI (Legislative Decree of President of Italian

Republic N. 61 of 11 April 2011, art. 6). In general, the contents and provisions of the decree are therefore, overall, fully aligned with the 2008 European directive, thus Italy, as a Member State, has decided to apply to the letter what has already been indicated by the Council.

4. DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

After 11 years, Europe - also in light of the Covid-19 pandemic and the increasingly frequent cyber-attacks perpetrated against various critical infrastructures - decides to update the legislation by issuing, on 14 December 2022, the Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities that repeals Council Directive 2008/114/EC. With the repealing of the previous directive, a modernization of the legislation is proposed and a several innovations are introduced with a new point of view by European Union; in fact, while before, the inspiring reason was the simpler concept of protection now, instead, we focus on that of resilience, that - wanting to use a single and concise definition - consists in a critical entity’s ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art. 2).

The innovations introduced by the new Directive (EU) 2022/2557 are many and all of considerable interest: first of all, the directive abandons the designation of European Critical Infrastructures and consequently of their operators/owners and introduces what is defined as a “critical entity” that means a public or private entity which has been identified by a Member State in accordance with a specific procedure as belonging to one of the categories set out in the directive (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, annex). The list includes - obviously - the energy and transport sectors, but broadens the categories considered to 11, it returns to a broader and more widespread classification similar to that made in the communication 702 of 2004 according to which critical infrastructures had to be included in 9 different sectors (Communication from the Commission to the Council and the European Parliament of 20 October 2004):

- Energy (Electricity, District heating and cooling, Oil, Gas, Hydrogen);

- Transport (Air, Rail, Water, Road, Public Transport);
- Banking;
- Financial market infrastructure;
- Health;
- Drinking water;
- Waste water;
- Digital infrastructure;
- Public administration;
- Space;
- Production, processing and distribution of food.

According to the provisions of the directive, by 17 July 2026 each Member State will be required to identify the critical entities for the sectors and subsectors listed in the directive. In general, the criteria to be followed for the designation of a critical entity are (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art. 6):

a) the entity provides one or more essential services;

b) the entity operates, and its critical infrastructure is located, on the territory of that Member State;

c) an incident would have significant disruptive effects, on the provision by the entity of one or more essential services or on the provision of other essential services in one or more of 11 the sectors that depend on that or those essential services.

It is necessary to specify that the importance of the disruptive effects is assessed according to some criteria, already indicated by the directive itself. Specifically, the criteria are related to the number of users relying on the essential service provided by the entity concerned; the extent to which other sectors and subsectors depend on the essential service in question; the impact that incidents could have, in terms of degree and duration, on economic and societal activities, the environment, public safety and security, or the health of the population; the entity's market share in the market for the essential service; the geographic area that could be affected by an incident, including any cross-border impact and - at the end - the importance of the entity in maintaining a sufficient level of the essential service, considering the availability of alternative means for the provision of that essential service (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art. 7).

With reference to the provision of essential services, the directive specifies that a critical entity is qualified as a European critical entity if, in addition to being preliminarily identified as a critical entity, it provides identical (or similar) essential services in six or more Member States; such entity will be given specific notification as indicated in the Directive (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art. 17).

A further innovation concerns the risk assessment which becomes more complex and is now divided into two levels: a first risk analysis is carried out directly by the Member State and subsequently the critical entity carries out one for its critical infrastructure(s). Specifically (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.12), the Member State's risk assessment takes into account all the relevant natural and man-made risks which could lead to an incident, including those of a cross-sectoral or cross border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541.

Critical entities shall, within nine months of receiving notification of identification as such, be required to assess, and based on Member States' risk analysis and other relevant sources of information, all relevant risks that could disrupt the provision of their essential services. This evaluation shall be repeated when necessary and at least every four years, without prejudice to the cessation of the designation of critical entity. Critical entities have the obligation to prepare and then apply a resilience plan in which the adequate and proportionate technical, security and organisational measures to guarantee their resilience are described, therefore the OSP (Operator

Security Plan) provided for by the previous directive disappears and the resilience plan of the critical entity is born in which specific measures are included (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.13).

However, the critical entity remains required to appoint its own liaison officer to act as a point of contact with the competent authority of the Member State. In this regard, it should be noted (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.9) that each Member State is required to designate one or more competent authorities responsible for the correct application of this Directive at national level and that, therefore, they will be the ones to interface and receive communications from critical entities exclusively through the single point of contact already appointed by them. Critical entities - unless they are operationally unable to do so - shall make an initial notification of the occurrence within 24 hours of becoming aware of the incident, this communication shall then be followed, if deemed appropriate, by a detailed final report at the latest after one month (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.15).

A final innovation introduced is the establishment of the group for the resilience of critical entities which has the task of supporting the Commission and facilitating cooperation between Member States and the exchange of information on issues relating to the themes of the directive itself (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.19). The group is composed of representatives of the Member States and is chaired by the representative of the European Commission. By 17 January 2025 - and every two years thereafter - the Critical Resilience Group is required to draw up a work program on the actions to be undertaken to achieve its objectives.

A very important aspect of the directive is that it does not apply to matters covered by Directive (EU) 2022/2555 (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.1), without prejudice to the provisions of the same for Critical entities in the banking, financial market infrastructure and digital infrastructure sectors (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.8).

Considering the relationship between the physical security and cyber-security of critical entities, Member States shall ensure that this Directive and Directive (EU) 2022/2555 are implemented in a coordinated manner. This shows, first of all, that the issue of cyber security has now become so central as to dedicate an entire regulation to the matter and, furthermore, that cyber-attacks can have strong repercussions on the entire system of critical infrastructures and therefore cannot be considered isolated attacks and must be treated in all respects as incidents that can significantly disrupt the provision of essential services of a Member State (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.1).

5. CONCLUSIONS

The identification and consequently the protection of critical infrastructures is a relatively recent topic, in fact, in Europe, it has been regulated for less than twenty years. It is a theme in continuous change and updating, also due to the application of not only physical but also digital technologies that are increasingly sophisticated and aggressive, capable of significantly disrupting the functioning of one or more systems of a Member State of the European Union.

The European legislation was updated in 2022 with Directive (EU) 2022/2557 which proposes important innovations on the topic, drawing attention to the resilience of critical entities, i.e. the capacity to resist, adapt and restore their operational functions. Each Member State of the Union is aligning its legislation with European directives, for example Italy, will certainly adapt to the provisions of Directive (EU) 2022/2557 and therefore it is very likely that - already in the next few months - there will be an update of the Italian legislation which, currently, with the validity of Legislative Decree No. 61 of 11 April 2011 remains anchored to the previous Council Directive 2008/114/EC.

REFERENCES

[1] Communication from the Commission to the Council and the European Parliament of 20 October 2004. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF (Accessed: 18 September 2024).

[2] Communication from the Commission of 12 December 2006. Available at: https://eurlex. europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786 (Accessed: 18 September 2024).

[3] Council Directive 2008/114/EC of 8 December 2008. Available at: https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32008L0114 (Accessed: 23 September 2024).

[4] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0541. (Accessed: 25 September 2024).

[5] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557 (Accessed: 23 September 2024).

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555 (Accessed: 25 September 2024).

[7] Green Paper on a European Programme for Critical Infrastructure Protection of 17 November 2005. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576 (Accessed: 18 September 2024).

[8] Legislative Decree of President of Italian Republic N. 61 of 11 April 2011. Available at: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2011-05-04&atto.codiceRedazionale=011G0101&elenco30giorni=false (Accessed: 23 September 2024).

[9] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 26 October 2001, s. 1016. Available at: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm (Accessed: 16 September 2024).

METHODS OF DETECTING AND RECOVERING AFTER HOMOGLYPH ATTACKS

Roman TOLSTOSHEYEV

Baku Higher Oil School, Baku, Azerbaijan

The problem of homoglyph attacks has become significant nowadays. Due to the increasing range of characters in modern encoding systems, similar symbols are being added. This tendency causes problems in distinguishing characters, which hackers exploit in spoofing attacks. In this research, an attempt is made to examine the problem of homoglyph attacks and provide an overview of practical solutions, such as different algorithms. Additionally, a solution to address the issue of spoofing attacks using the Levenshtein edit distance algorithm, widely used in spell checking, will be provided. The proposed solution, which utilizes a backend application written in the Java programming language with the Spring technology stack, can detect homoglyphs and attempt to replace them with normal characters. Additionally, a desktop client for the application is also presented.

Key words: *homoglyph, UTF-encoding, obfuscation, spoofing, dynamic programming.*

1. INTRODUCTION

The main topic of this work is to analyze current solutions against homoglyph attacks and evaluate their positive and negative aspects and propose a new solution. Chapter 2 provides a brief description of the history and prevalence of encoding systems, as well as a full description of homoglyphs and their examples, to establish the genesis of the research problem. Chapter 3 depicts and classifies the security issues regarding homoglyph attacks. The systematization given in this chapter helps identify where this kind of attack is most likely to be applied.

Chapter 4 attempts to analyze previously proposed solutions to the problem, comparing their merits and demerits. This chapter also provides implementations of the main algorithms in the Java programming language. Chapter 5 describes a suggested method to oversee the problem, divided into two sub-chapters. This chapter aims to propose a solution that meets all requirements and is more effective than existing solutions by considering one or more specific traits. Additionally, that chapter introduces a solution called “Ambiglyph,” which was specially created during this research to solve the homoglyph attack problem. The proposed solution implements the aspects mentioned in earlier chapters, providing a comprehensive description of “Ambiglyph,” its main components, and their working principles.

2. CHARACTER ENCODING STANDARDS

Encoding systems play a crucial role in information exchange. The problem of encoding characters starts from the epoch of communication via telegraph, when people started to encode their text messages using electric signals (McEnery and Xiao:2005, p.47). The most popular was encoding using Morse code which used short and long electric signals for encoding letters, digits and punctuation marks and long absence of signal to separate characters.

With the appearance of computers, the issue of encoding messages became acute. Data was to be encoded using a sequence of bits that were related to the presence and absence of signal. Hence, binary logic of computers with “long signal” incommutability led to new encoding systems were to be invented.

Early encoding systems used 5 and then 6 bits to encode each character; however, it was insufficient and 7-bits encoding systems were in use. The most noticeable example of this kind of system is the American Standard Code for Information Interchange or ASCII announced in 1963. ASCII is used to encode all litters of the Latin English alphabet, digits, punctuation marks and special characters. ASCII was adopted by all computer manufacturers of that time and turned into standard ISO 646 by the International Organization of Standardization (ISO) in 1972.

The significant demerit of ASCII character was that it was adopted only for English letters and did not include native characters of some other countries and languages. The solution of that time was to introduce a new set of characters. The series of ISO standards ISO-8858-X and usage of 8-bit encoding were turned to solve this problem. Additionally, in some languages like Chinese, it was impossible to encode all necessary characters using 8 bits.

The large variety of ASCII character tables created a significant problem in information exchange. Sometimes, it was not practical to process text due to the lack of supported ASCII tables of a software or its regional settings. In other cases, text files can be damaged in case of using inappropriate ASCII encoding format. Furthermore, other encoding systems were still in use: JIS (Japan), GB (China), GOST (USSR), EUC

(Unix), CP (IBM, Microsoft), and many more. Most of them we incompatible with one another, creating obstacles in decoding.

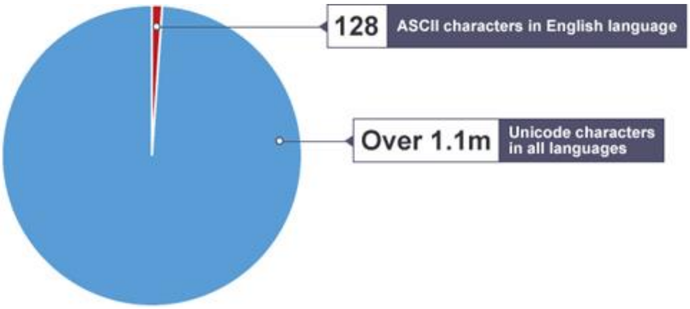


Fig. 1 Comparison of ASCII and Unicode character sets

The establishment of Unicode in early 1989 played a key role in addressing these problems. Unicode encoding system gives a chance to store a character in several bytes and allows people to enlarge characters set in case of necessity with saving backward compatibility with ASCII. Unicode standard updates regularly and adds new symbols. The latest version of Unicode for May 2024 is Unicode 15 (Unicode inc.:2021). The comparison of ASCII and Unicode characters set is given in Figure 1.

Unicode has several implementations; the most popular ones are UTF-8 and UTF-16. 97% of websites around the world use UTF-8 (Q-Success:2024). Modern character encoding standards try to cover as many practical symbols used by humans as possible to be more versatile according to the variety of natural and formal languages. This versatility can cause problems related to the visual identity of some symbols and the probability of mismatching them (Miller:2013, p.4). Modern encoding systems such as Unicode use more than 140,000 symbols in version 14, with about 6,000 concerns regarding its visual similarity and symbol understanding (Unicode inc.:2021).

The poor contrast in the visual representation of some characters can depend on the fonts used in their display (without considering the quality, technical parameters, and settings applied to a display device) (The MITRE Corporation:2017). However, commonly used fonts can display several different symbols with extremely limited differences or even without them, proving to be an issue.

More formally, symbols that resemble one another are called homoglyphs. A homoglyph can be a full copy of another character or resemble it. For instance, the Latin character “O” (UTF-16 code is

\u004f) can be mismatched with the Cyrillic “O” (\u041e) and the digit zero “0” (\u0030). In the first case, it is almost impossible to distinguish the difference between the two characters, while in the second case, it is possible in most instances (Miller:2013, p.4). As an example, possible homoglyphs of letter "A” are provided on Figure 2.

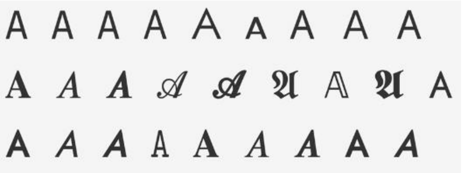


Fig. 2 Homoglyhs of a capital letter “A”

3. SECURITY ISSUES OF HOMOGLYPHS

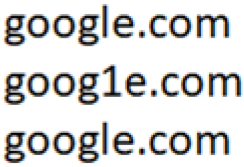
Homoglyphs can be widely used for various malicious purposes, especially in cyberspace (The MITRE Corporation:2017) (Woodbridge et al.:2018, p.22). For example, consider a PC running on Windows OS. Suppose there is a normal Windows system process called “svchost.exe.” An attacker can disguise a malicious process with the name “svch0st.exe.” Without attentiveness, it can sometimes be difficult to detect a process with a non-standard or peculiar name that can indicate maliciousness (Woodbridge et al.:2018, p.22). In the case of “svchost.exe” where Cyrillic “O” is used, the possibility of detecting the attacker’s process without special tools decreases considerably.

The usage of homoglyphs in this manner can be specified as a spoofing attack (Woodbridge et al.:2018, p.22). A spoofing attack is an attack where an attacker tries to modify some data in such a way that it becomes hard or impossible to identify these modifications (Malwarebytes:2024). The aim of spoofing attacks is usually to gain access to other data or to infect the system itself. There are several types of spoofing attacks (Balaban:2020):

- *ARP Spoofing*: In this kind of attack, an attacker sends an ARP without a request being sent. The idea of the attack is to update ARP tables of devices in such a way that all traffic will go through the attacker's PC.
- *MAC Spoofing*: A type of attack where a hacker changes their own MAC address or masquerades to access a network with access restrictions.
- *IP Spoofing*: Spoofing an IP address to impersonate another computer.

- *DNS Cache Poisoning (DNS Spoofing):* Changing values in the DNS cache to redirect to sites with different domains.
- *Email Spoofing*: A method of disguising malicious emails using the trust given by the address or content of the mail. These emails can use identical or similar domains, sender identifications, and signatures.
- *Website Spoofing*: Creating an exact copy of a site for malicious purposes, which can even be located at a similar address.
- *Caller ID Spoofing*: An attack based on replacing a phone number, ID, or identity to deceive the receiving person.
- *Text Message Spoofing*: A technique of substituting the sender's phone number with letters or numbers to deceive the recipient.
- *Extension Spoofing*: A method of adding or changing file extensions to make them executable.
- *GPS Spoofing*: Sending manually generated or edited GPS signals to the antenna of a victim to affect the navigation device's behavior.
- *Facial Spoofing*: Bypassing face recognition authentication/identification using a photo or any kind of graphical picture of the victim.

The meaning of homoglyphs allows them to be applied in all types of spoofing attacks (excluding facial spoofing). However, they are not always effective. If the corrupted data from a spoofing attack is checked by a computer, it will at once give a different result, which is understandable. An example of obfuscated words differentiation is given in Figure 3.



google.com

goog1e.com

gооglе.com

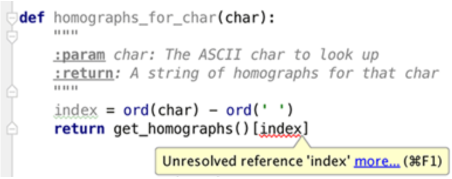
Fig. 3 Example for spoofed with homoglyphs web address. First is normal domain, second – “l” was replaced with “1”, third – English “o” and “e” were replaced with Cyrillic letters.

From the above-mentioned list, we can drop ARP, MAC, and GPS spoofing, but in the case of manual checking without a special device, these attacks can still be dangerous. The rest (from 4 to 9) become a standard place for spoofing attacks. In DNS spoofing, homoglyphs can be used to edit a web address so that the difference between the original DNS record and the edited one is barely noticeable (Unicode inc.:2024).

The same technique can be used in the creation of phishing sites during a website spoofing attack. From the victim's side, it is sometimes impossible to visually distinguish the difference between the original domain name and the spoofed one. This problem is related to the International Domain Name System (IDN) (Opera Team:2017) like depicted on Figure 4. In some browsers, safety and security systems can detect this kind of spoofing. However, the efficiency of these systems is not absolute.

One more example of the usage of homoglyphs in malicious activities is file corruption (McDowell:2011). Configuration files are widely popular in modern software and operating systems. A suitable example is grub.cfg in Linux-based operating systems where the GRUB loader is used, or the file called hosts on machines running on Windows. Both files have human-readable characters and are edited manually. Furthermore, these files are crucial for the corresponding operating systems, and their functionality strongly depends on these files.

Homoglyphs can be easily used to corrupt necessary configuration files and partially or fully cause a computer to malfunction. Fixing these symbols or restoring file data manually can be time-consuming since all homoglyphs (including hidden ones) must be found and replaced with proper symbols, or the whole configuration file must be rewritten. An example of broken code is given in Figure 5.



```
def homographs_for_char(char):
    """
    :param char: The ASCII char to look up
    :return: A string of homographs for that char
    """
    index = ord(char) - ord(' ')
    return get_homographs()[index]
```

Unresolved reference 'index' more... (⌘F1)

Fig. 4 Static analyzer inside IDE recognizes spoofed variable as a new uninitialized variable. (https://habr.com/ru/post/385697)

Another application of homoglyph attacks is the concealment of plagiarism. Homoglyphs can be used to visually preserve the meaning and legibility of words but cause a plagiarism detection system to fail to recognize them as the same word. Hence, two texts that are visually and semantically identical to humans will be recognized as different by a computer (Alvi et al.:2017, p.669).

4. RESEARCH METHODOLOGY

One of the most common ways to detect homoglyphs is to use Levenshtein or Hamming edit distance algorithms and prepare dictionary (Woodbridge et al.:2018, p.22). A word is to be checked by editing distance and compared with a beforehand prepared dictionary. The same approach is used in spell checking algorithms (Lhoussain et al.:2015, p.127).

Levenshtein algorithm—one of the classical examples of Dynamic Programming algorithms (Allison:1999) used in Computer Science to compute the minimum number of operations required to transform string a to string b or controversially. The idea of the algorithm is to divide the assumed editing process into three types:

- Insertion of a symbol
- Deletion of a symbol
- Substitution of a symbol

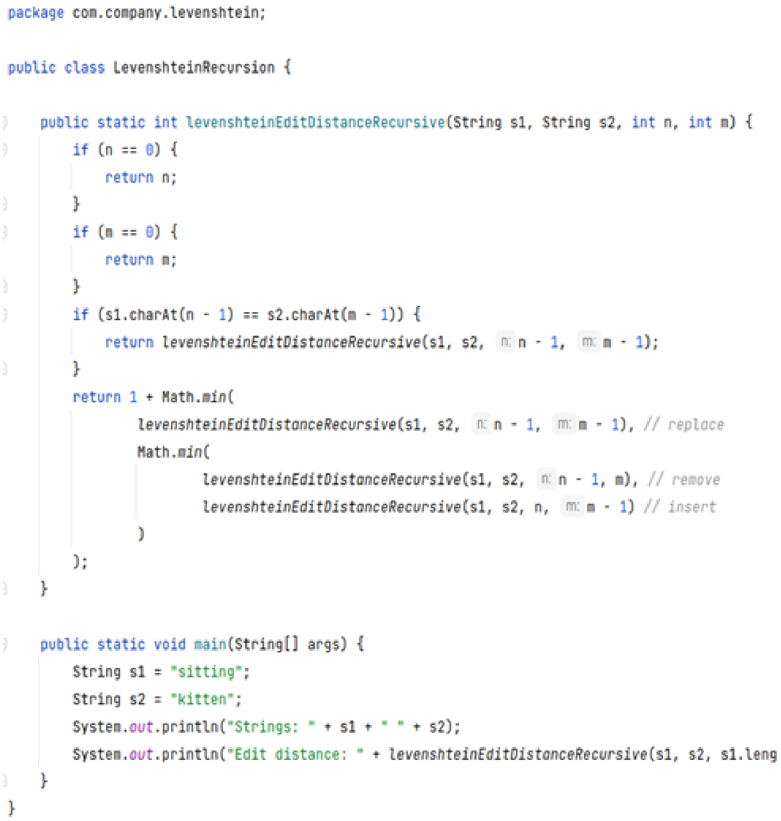
Overall, the recurrent definition of Levenshtein distance function can be presented as on formula 1.

$$lev_{a,b}(i,j) = \begin{cases} \max(i,j), \quad if \ \min(i,j) = 0 \\ min \begin{cases} lev_{a,b}(i-1,j) + 1 \\ lev_{a,b}(i,j-1) + 1, \\ lev_{a,b}(i-1,j-1) + 1_{(a_i \neq b_{j)}} \end{cases} \quad otherwise \end{cases}$$

(1)

where a and b are strings to be compared and i and j are indices of their characters. $lev_{a,b}(i,j)$ stands for the Levenshtein distance between substrings $a_0 : a_i$ and $b_0 : b_j$. The base of the recursion is a situation where the string has length equals to 0 and the value of the function in this case will be length of the second string. Otherwise, we just move forward through the string with i and j being steadily increased. During this movement, the value of the function will calculate on each increase of both indices. Each time the value of function will be calculated by choosing smallest value of the function with smaller i and j that was calculated before and by adding 1. Adding 1 means that we must change manipulation with a symbol.

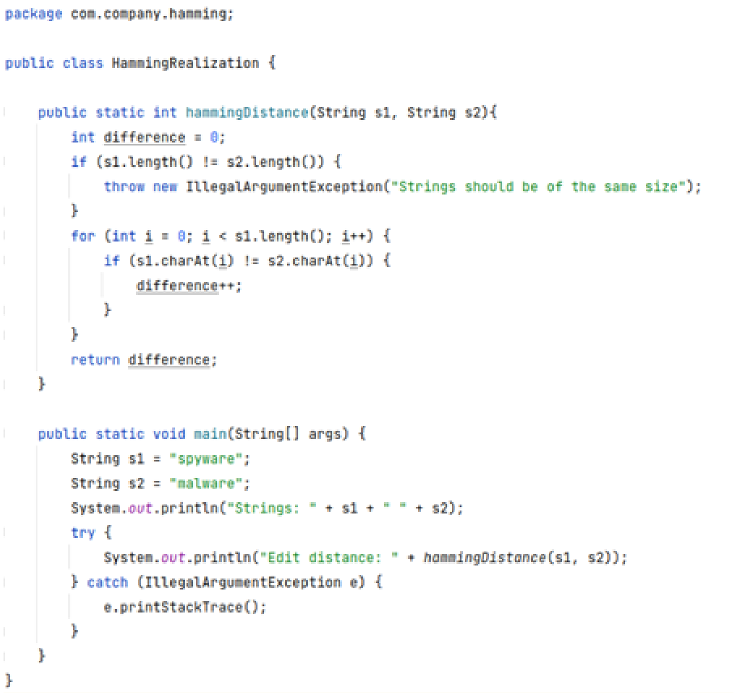
Explaining calculations more dentally, $lev_{a,b}(i-1,j)$ means the absence of the i^{th} symbol in the string a or deletion of that symbol, $(i,j-1)$ means absence of j^{th} symbol in b or insertion of symbol b_j to string a. $lev_{a,b}(i-1,j-1)$ means that we remove both corresponding symbols from both strings which means that we can add another mutual one. The last step is needed only in case of inequality of a_i and b_j. It is possible to write Java code like in Figure 5. Also, the ready realization is available in Apache Commons Text package Java (Apache:2020). Memory and time complexity is for both realizations is $O(n^2)$.



```java
package com.company.levenshtein;

public class LevenshteinRecursion {

    public static int levenshteinEditDistanceRecursive(String s1, String s2, int n, int m) {
        if (n == 0) {
            return n;
        }
        if (m == 0) {
            return m;
        }
        if (s1.charAt(n - 1) == s2.charAt(m - 1)) {
            return levenshteinEditDistanceRecursive(s1, s2, n: n - 1, m: m - 1);
        }
        return 1 + Math.min(
                levenshteinEditDistanceRecursive(s1, s2, n: n - 1, m: m - 1), // replace
                Math.min(
                        levenshteinEditDistanceRecursive(s1, s2, n: n - 1, m), // remove
                        levenshteinEditDistanceRecursive(s1, s2, n, m: m - 1) // insert
                )
        );
    }

    public static void main(String[] args) {
        String s1 = "sitting";
        String s2 = "kitten";
        System.out.println("Strings: " + s1 + " " + s2);
        System.out.println("Edit distance: " + levenshteinEditDistanceRecursive(s1, s2, s1.leng
    }
}
```

Fig. 5 Levenstein edit distance recursive realization

In contrast, the Hamming editing distance algorithm uses a simpler approach. In this algorithm, during the iterating over string the number of characters that differ is counted. Hence, the only constraint in the algorithm is that string should have equal sizes for reliable results. Realization is in Figure 6.



```java
package com.company.hamming;

public class HammingRealization {

    public static int hammingDistance(String s1, String s2){
        int difference = 0;
        if (s1.length() != s2.length()) {
            throw new IllegalArgumentException("Strings should be of the same size");
        }
        for (int i = 0; i < s1.length(); i++) {
            if (s1.charAt(i) != s2.charAt(i)) {
                difference++;
            }
        }
        return difference;
    }

    public static void main(String[] args) {
        String s1 = "spyware";
        String s2 = "malware";
        System.out.println("Strings: " + s1 + " " + s2);
        try {
            System.out.println("Edit distance: " + hammingDistance(s1, s2));
        } catch (IllegalArgumentException e) {
            e.printStackTrace();
        }
    }
}
```

Fig. 6 Realization of Hamming distance algorithm

Overall, if the distance between the given word and a similar word from the dictionary is greater (or lower) than the predefined precision and contains a character that can be a homoglyph, this word will be counted as spoofed.

As follows from the main idea of the method, the effectiveness of these algorithms is limited by the predefined precision and the existence of the word in the dictionary. This will be the main drawback of the given method. Another demerit of using conventional algorithms is their technical inability to detect all types of phishing at once.

Describing the positive sides, in cases where the word exists in the dictionary and the precision is absolute, the method provides a 100% detection rate. Memory and time complexity is $O(n)$.

Another approach is the usage of Machine Learning to detect words that have homoglyphs. One implementation is to convert a word to a vector image and find the distance between the vector-graphical representation of the given word and those from a dictionary of confusable characters or Siamese Networks (Woodbridge et al.:2018, p.22). Considering the disadvantages of the Machine Learning method itself, such as computing performance requirements (Flair:2021) and the ability to poison the data, some implementations of this approach can achieve a higher true-positive rate than conventional algorithms (improvement from 13% to 45%).

Another point that should be mentioned is that a possible solution should not only aim to detect homoglyphs but also to recover files after an attack. Since the recovery process is a problem in homoglyph attacks, this fact should be considered. Detection methods should also consider finding spoofing in specific terminology or abbreviations of a company or enterprise.

The possible comparison using matrix table can be represented as in Table 1.

Table 1

Features	Levenshtein edit distance	Hamming edit distance	Machine Learning approach
Detecting words with different lengths	+	-	+
100% accuracy	+		
Less computing power needed	+		

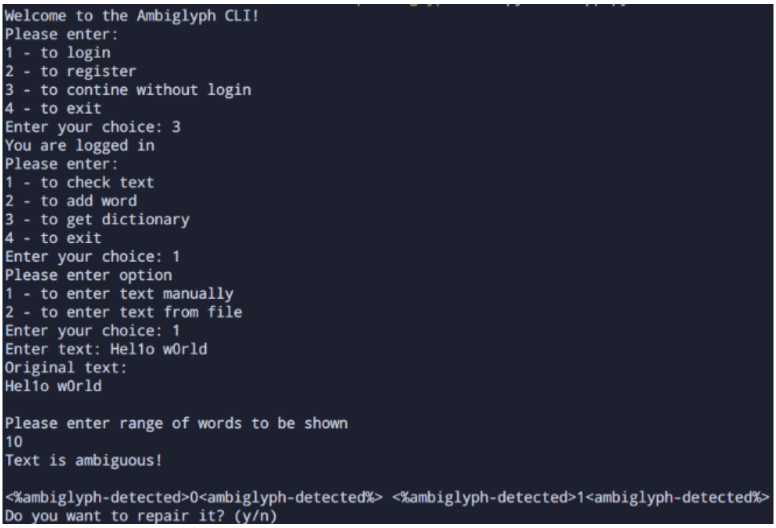
5. SUGGESTED FRAMEWORK

The main problem of homoglyph detection lies in the inability to predict which word a homoglyph can indicate a spoofed word, or if it is used due to the spelling of a particular word in a language. Fortunately, getting the list of homoglyphs is not a significant problem since detecting pairs of similar symbols is easier because the number of symbols in an encoding system is limited and smaller than that of words in a natural language. Thus, the main weak point of any algorithm can be related to a database of words or data needed to detect a spoofed word. The key function of the most effective solution will be the ability to intensively enrich our own database while considering all possible contexts. Another feature that can be implemented is the recovery of obfuscated words using any word-guessing approach.

As one implementation of a possible solution, special software using the Levenshtein algorithm and linear search can be created. A detached backend server will play the role of the main actor in detecting obfuscated text and attempting recovery, with a client-side model in use. The backend server will store all necessary data, such as a database of homoglyphs and a dictionary of words. When the server receives a request with text, all words within it will be checked using the Levenshtein distance to determine similarity with words in the dictionary in case a homoglyph exists. This algorithm has proven to be the most sophisticated in this field in terms of accuracy and time complexity (Hardesty:2015). Thus, it will be used. If words are detected, then linear search takes its turn. Potential words according to the Levenshtein edit distance will be found in the dictionary and given as suggestions to the user for replacement. Of course, the number of suggestions can be significant depending on the precision defined in the Levenshtein algorithm (maximal edit distance between given and suggested words). Since the proper edit distance to be chosen can vary depending on the homoglyph used in spoofing a word, the user must supply boundaries that specify the maximum number of suggestions to be given.

The next problem solved by the solution should be the inclusion of specific words strictly related to the context, for example, of a company or an organization. The main dictionary can be enlarged with words specific to the company. Of course, some of these words can be considered potentially dangerous information if published; therefore, an accounting system is to be introduced. All users will be able to log in using their credentials and use the enlarged dictionary. They can add or remove words to their own data storage.

Talking about client applications, which will do all main interactions with the user. It was decided to use Command Line Interface (CLI) as it will be more comfortable and convenient to use with configuration files or plain text files. An interface is shown in Figure 7.



```
Welcome to the Ambiglyph CLI!
Please enter:
1 - to login
2 - to register
3 - to contine without login
4 - to exit
Enter your choice: 3
You are logged in
Please enter:
1 - to check text
2 - to add word
3 - to get dictionary
4 - to exit
Enter your choice: 1
Please enter option
1 - to enter text manually
2 - to enter text from file
Enter your choice: 1
Enter text: Hel1o w0rld
Original text:
Hel1o w0rld

Please enter range of words to be shown
10
Text is ambiguous!

<%ambiglyph-detected>0<ambiglyph-detected%> <%ambiglyph-detected>1<ambiglyph-detected%>
Do you want to repair it? (y/n)
```

Fig. 7 Ambiglyph CLI

The integration between CLI application and backend application is done by REST API technology (Figure 8). The server side is fully written in Java programming language using Spring technology stack. Ready realization of Levenshtein edit distance algorithm is taken from Apache Commons Text package as a more versatile one. As a database server the MySQL database is used. CLI application is fully written in Python programming language. This application is compatible with macOS and Linux-based operation systems.

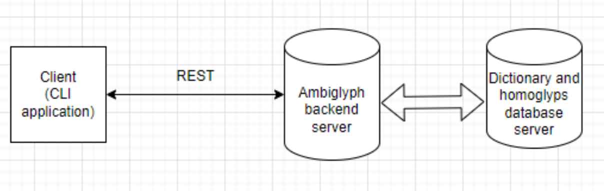
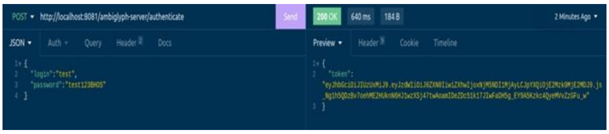


Fig. 8 Client-server structure

The name "Ambiglyph" is given to the software. Both server (Ambiglyph Server) and client (Ambiglyph CLI) applications are available on GitHub platform.

With regards to the client-server architecture, the responsibilities of both sides are separated. The server side will only process incoming text and find suggestions. Also, it can manage Create, read, update and drop (CRUD) operations on word and users by playing a role of authentication server and segregating privileges. Spring security module and authentication is managed by JSON Web Tokens (JWT-tokens).



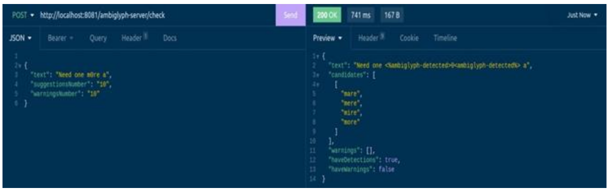
POST http://localhost:8081/ambiglyph-server/authenticate

```
{
  "login":"test",
  "password":"test123BHOS"
}
```

```
{
  "token":
  "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0ZXN0IiwiZXhwIjoxNjM5NDI1MjAyLCJpYXQiOjE2Mzk0MjE2MDJ9.js_Ng1h5QDzBv7oehME2HUknN6HJ1wzXSj47twAoamIDeZDc51k17JIwFaDH5g_EY9ASKzkc4QyeMVvZzGFu_w"
}
```

Fig. 9 Retrieval of JWT-token after successful login

The current main REST API features can be depicted like this. Firstly, it is needed for users to have an account in the system. In test example, user with login "test" will be used. It must be authorized for future actions; hence users must obtain JWT-token from the server (Figure 9). Then, the user can send necessary requests (Figure 10).



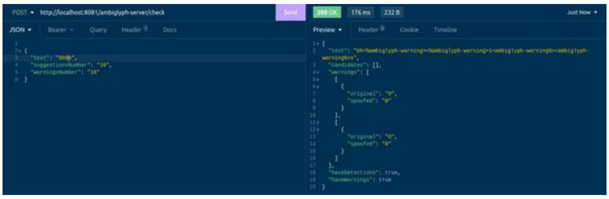
POST http://localhost:8081/ambiglyph-server/check

```

{
  "text": "Need one m0re a",
  "suggestionsNumber": "10",
  "warningsNumber": "10"
}
```

```
{
  "text": "Need one <%ambiglyph-detected>0<ambiglyph-detected%> a",
  "candidates": [
    [
      "mare",
      "mere",
      "mire",
      "more"
    ]
  ],
  "warnings": [],
  "haveDetections": true,
  "haveWarnings": false
}
```

Fig. 10 Obfuscated word "more" ("m0re") is detected, and suggestions are provided.

However, it is not possible to detect spoofed words if it is used only by one company or organization (Figure 11).



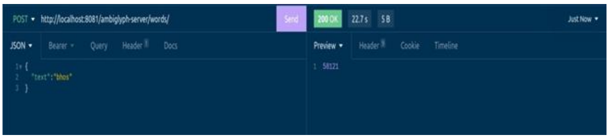
POST http://localhost:8081/ambiglyph-server/check

```

{
  "text": "bh0s",
  "suggestionsNumber": "10",
  "warningsNumber": "10"
}
```

```
{
  "text": "bh<%ambiglyph-warning><%ambiglyph-warning>1<ambiglyph-warning%><ambiglyph-warning%>s",
  "candidates": [],
  "warnings": [
    [
      {
        "original": "O",
        "spoofed": "0"
      }
    ],
    [
      {
        "original": "O",
        "spoofed": "0"
      }
    ]
  ],
  "haveDetections": true,
  "haveWarnings": true
}
```

Fig. 11 Word "bh0s" is recognized as warning, no suggestions are provided.

By default, Ambiglyph uses an open database of words (Corncob Lowercase Dictionary) that consists of about 58,000 commonly used words. Of course, there is no word "bhos" or spoofed version "bh0s". But, by using homoglyph database (Homoglyphs) it is still possible to send a warning that the symbol "0" can be for obfuscation. Anyway, it is still possible to add the word "bhos" to evaluate user's database (Figure 12).



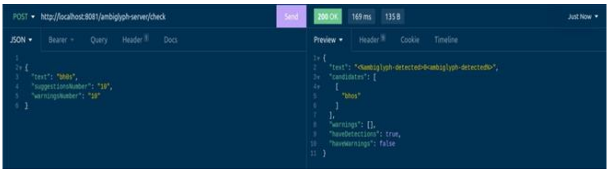
POST http://localhost:8081/ambiglyph-server/words/

```
{
  "text":"bhos"
}
```

```
58121
```

Fig. 12 Adding word “bhos” to the user's words database.

Now, the obfuscation can be detected (Figure 13).



POST http://localhost:8081/ambiglyph-server/check

```

{
  "text": "bh0s",
  "suggestionsNumber": "10",
  "warningsNumber": "10"
}
```

```
{
  "text": "<%ambiglyph-detected>0<ambiglyph-detected%>",
  "candidates": [
    [
      "bhos"
    ]
  ],
  "warnings": [],
  "haveDetections": true,
  "haveWarnings": false
}
```

Fig. 13 Word “bh0s” recognized as obfuscated word “bhos.”

By contrast, the client side is only responsible for reading files, chunking them and sending them to the server. After the server responds, the client tries to restore a text according to the suggestions provided by the server and choice of user. Also, it can add unfamiliar words to the users’ dictionary or remove them. CLI ensures versatileness of the application usage, especially when graphic user interface (GUI) is not accessible.

6. CONCLUSION

Overall, modern encoding systems are quite rich in terms of the symbols they can stand for; however, this leads to the indistinguishability of some similar characters, known as homoglyphs. This vulnerability is actively exploited by hackers to perform several types of spoofing attacks. The problem needs to be addressed using various techniques, such as classical algorithms or Machine Learning approaches. Nevertheless, it is still impossible to guarantee absolute detection and recovery of texts corrupted by homoglyphs. This issue is related to the imperfections of current algorithms and challenges in creating and supporting sufficient databases. Recovery techniques also suffer from these problems.

The solution of guessing obfuscated words using the Levenshtein edit distance, which is commonly used in spell checking, and dividing dictionary databases into users who can extend them with their own terminologies and words used in the context of their organization or enterprise, can be considered a successful attempt to solve the problem of detecting homoglyph attacks. Additionally, linear search on given suggestions can also be efficient for recovery after homoglyph attacks.

However, there are still negatives that interfere with making the solution sophisticated. The first is the requirement to always be connected to a database server, which is sometimes not possible, for example, due to the absence of an internet connection. Another negative is the human factor related to the choice of words to be replaced by the server suggestions. Users can mistakenly replace a spoofed word with an inappropriate option. The same issue arises with updating a user's database. Furthermore, a lack of specific words used by a user can hinder the process of proper word guessing by the server, resulting in the inability to recover a word. Lastly, the Command Line Interface of the client application may not be suitable or user-friendly for some users.

REFERENCES

[1] Allison, L., Dynamic Programming Algorithm (DPA) for Edit-Distance, 1999. Available: https://users.monash.edu/~lloyd/tildeAlgDS/Dynamic/Edit.

[2] Ambiglyph CLI, Ambiglyph CLI, Available: https://github.com/IZOBRETATEL777/ambiglyph-cli.

[3] Ambiglyph Server, Ambiglyph Server, Available: https://github.com/IZOBRETATEL777/ambiglyph-server.

[4] Apache, Commons Text, 2020. Available: https://commons.apache.org/proper/commons-text/.

[5] Balaban, D., 11 Types of Spoofing Attacks Every Security Professional Should Know About, March 24, 2020. Available: https://www.securitymagazine.com/articles/91980-types-of-spoofing-attacks-every-security-professional-should-know-about.

[6] Corncob Lowercase Dictionary, corncob_lowercase.txt, Available: http://www.mieliestronk.com/corncob_lowercase.txt.

[7] Flair, Data, Advantages and disadvantages of machine learning language, 2021.

[8] Homoglyphs, Homoglyphs, Available: http://homoglyphs.net/.

[9] Lhoussain, Aouragh Si, Gueddah, Hicham, and YOUSFI, Abdellah, Adaptating the levenshtein distance to contextual spelling correction, *International Journal of Computer Science and Applications*, Vol. 12, No. 1, pp. 127-133, 2015.

[10] Malwarebytes, What is a spoofing attack?, Available: https://www.malwarebytes.com/spoofing.

[11] McDowell, M., Understanding Hidden Threats: Corrupted Software Files, March 9, 2011 (updated in 2019). Available: https://us-cert.cisa.gov/ncas/tips/ST06-006.

[12] Cox, L.A., What’s Wrong with Risk Matrices? In: *Risk Analysis,* Vol. 28, No. 2, 2008.

[13] Flouris, G.T., Lock D., (2009) *Managing Aviation Projects from Concept to Completion,* Ashgate Publishing Company, Farnham, pp. 304-306.

DATA PRIVACY TRENDS IN EU: AN OVERVIEW OF RECENT DEVELOPMENTS

Cristina ANTONOAIE*, Mihai ALEXANDRESCU**

* Regional Department of Defense Resources Management Studies, Brasov, Romania
** Spiru Haret University Bucharest, Faculty of Economic Sciences and Juridic Sciences Brasov, Romania

The article highlights growing trends in data privacy behaviors among internet users, in the EU. People are increasingly limiting cookies and tracking, using privacy protection software, and reading privacy policies before sharing personal data. Many are also restricting geolocation access, limiting social media profile visibility, and refusing to allow their data to be used for advertising. Additionally, users are more cautious about website security, checking for HTTPS before entering sensitive information. These behaviors reflect heightened awareness of data protection and a desire to safeguard personal information in response to concerns about privacy, surveillance, and online tracking. This shift is influenced by regulations like GDPR and the growing mistrust of data exploitation practices.

Key words: *privacy, behavior, challenges, regulation, solutions*

1. INTRODUCTION

The EUROSTAT database, within the item Digital Economy and Society, has provided us with some information about individuals' behavior regarding trust, security, and privacy when navigating the internet. We analyzed this behavior in 8 different situations using the most recent data available, that of 2023.

Firstly, individuals have changed the settings in their internet browser to prevent or limit cookies on any of their devices. This reflects an increasing trend of individuals taking control of their privacy. With growing concerns over tracking and data harvesting by advertisers and websites, this indicates a shift towards greater online privacy awareness and proactive data protection.

Secondly, individuals use software that limits the ability to track their activities on the internet. The use of privacy-enhancing software is becoming more widespread as people seek to minimize their digital footprint. Tools like VPNs, ad-blockers, and browser extensions help users reduce online tracking, which aligns with increasing public awareness about the need for anonymity and security while browsing.

Thirdly, individuals manage access to personal data on the internet (3 months): read privacy policy statements before providing personal data. More users are now scrutinizing privacy policies before sharing personal information, which indicates a growing understanding of the risks associated with sharing personal data. However, the challenge remains that many privacy policies are complex and difficult to interpret, suggesting room for improvement in terms of clarity and transparency.

Fourthly, individuals manage access to personal data on the internet (3 months): restricted or refused access to the geographical location. The refusal to share geolocation data is a strong sign of privacy-conscious behavior. Many users are becoming aware of the risks involved with location tracking, which can be used for intrusive advertising and surveillance. This trend reflects a desire for greater control over personal information and where it's shared.

Fifthly, individuals manage access to personal data on the internet (3 months): limited access to profile or content on social networking sites or shared online storage. Users are increasingly cautious about the privacy of their social media profiles and content. By limiting access to personal information, they are taking steps to protect themselves from data breaches, misuse, and the commercialization of their personal data. This trend highlights the growing demand for more privacy on social media platforms.

Sixthly, individuals manage access to personal data on the internet (3 months): refused allowing the use of personal data for advertising purposes. Many individuals are opting out of having their data used for personalized advertising. This is a response to concerns over the commercialization of personal data and a growing mistrust of targeted advertising techniques. It underscores the desire for more autonomy over personal information and how it's utilized.

Seventhly, individuals manage access to personal data on the internet (3 months): checked that the website where personal data provided was secure. The practice of checking website security (e.g., looking for HTTPS) before submitting sensitive data is a crucial step in protecting personal information. This trend reflects an increasing awareness of cybersecurity threats, as users are more cautious about where and how they provide their personal information.

Eighthly, Individuals manage access to personal data on the internet (3 months): at least one of I_MAPS_RPS [1], I_MAPS_RRGL [2], I_MAPS_LAP [3], I_MAPS_RAAD [4], I_MAPS_CWSC [5]. This indicates that individuals are actively engaging with various privacy and security measures, such as using privacy-enhancing tools, adjusting settings, or refusing certain data uses. This overall behavior shows that privacy has become a priority for many users, with a shift toward more informed and deliberate online actions to safeguard their personal data.

2. DATA ANALYSIS

2.1. Percentage of individuals that have changed the settings in their internet browser to prevent or limit cookies on any of their devices in 2023

Table 1 Percentage of individuals that have changed the settings in their internet browser to prevent or limit cookies on any of their devices in 2023

% of individuals 2.1.	Countries	No of countries
less than 10	BG	1
10-20	CY, RO	2
20-30	EL, FR, HR, IT, LT, LV, PL, SI, SK	9
30-40	AT, BE, CZ, EE, ES, HU, MT, PT, SE	9
40-50	DE, DK, IE, LU	4
more than 50	FI, NL	2
Total		27

Bulgaria is the only country in the category (less than 10%), indicating a low level of awareness or interest in online data protection among users in this country. Possible factors include a lack of digital education, less concern about privacy, or lower access to information about privacy options.

Cyprus and Romania (10.31%) fall into the category 10 – 20%, suggesting a moderate level of interest in online data protection, but not to the extent of other European countries. There could be factors such as partial digital education, lower awareness of the risks associated with cookies, or regulatory differences that influence this behavior.

This category (20 – 30%) includes a wide range of countries, such as France, Italy, and Poland. It’s evident that in these countries there is a greater concern for online privacy, and more users are choosing to control or limit cookies. These countries may have stronger educational initiatives or stricter data protection regulations, such as GDPR.

In this category (30 – 40%), countries such as Sweden, Spain, and Belgium have a significantly higher percentage of users modifying their browser settings for data protection. These countries typically have strong data protection infrastructures and a more educated population regarding their online privacy rights. These percentages suggest proactive user behavior in protecting their personal data.

Germany, Denmark, Ireland, and Luxembourg are countries with a high level (40 – 50%) of awareness of data protection and strict privacy policies. These countries likely benefit from strong educational campaigns and stringent privacy regulations, leading a significant number of users to adjust their browser settings to control cookies.

Finland and the Netherlands top this list, with more than half of users choosing to modify their settings for online data protection. These countries have a high level of digital education and awareness of privacy rights. They also have a strong culture of privacy and data protection compliance. On the whole, most European countries are in the mid-range for online privacy interest, but there are clear examples of countries with high interest, such as Finland and the Netherlands. Data protection policies, national regulations, and digital education significantly influence user behavior in this regard.

2.2. Percentage of individuals that use software that limits the ability to track their activities on the internet in 2023

Table 2 Percentage of individuals that use software that limits the ability to track their activities on the internet in 2023

% of individuals 2.2.	Countries	No of countries
less than 8	BG, CY	2
8-16	CZ, EL, IT, LV, RO, SI	6
16-24	AT, DE, ES, FR, HU, LT, PL, PT, SK	9
24-32	DK, EE, FI, HR, IE, LU, SE	7
32-40	MT, NL	2
more than 40	BE	1
Total		27

Bulgaria and Cyprus are the two countries in the category (less than 8%), showing a very low adoption of privacy software. This suggests that in these countries, online privacy concerns may not be as prominent among users. Possible factors for this low percentage could include less awareness of online privacy issues, limited access to privacy tools, or a lower level of digital literacy regarding how tracking works and how to avoid it.

Czech Republic, Greece, Italy, Latvia, Romania (10.42%), and Slovenia are in this range (8 – 16%), indicating a moderate but still relatively low usage of privacy-protecting software. The fact that these countries are adopting such tools at a higher rate compared to the previous group shows growing awareness of the importance of online privacy. However, the adoption rate suggests that while there is some interest in online privacy protection, it may still be overshadowed by other concerns like general internet usage habits or the lack of easily accessible, user-friendly tools.

Countries like Austria, Germany, Spain, France, Hungary, Lithuania, Poland, Portugal, and Slovakia fall into the category (16 – 24%). This indicates a stronger uptake of privacy software. The relatively higher usage in these countries could be attributed to increased awareness of data protection issues, including privacy scandals, such as the Cambridge Analytica incident or the implementation of the GDPR (General Data Protection Regulation) in the EU, which has raised awareness around user rights and privacy online. In these countries, users are likely to be more informed about the risks associated with online tracking and may have more access to tools that can help them safeguard their privacy, especially with ongoing digital education initiatives and stronger regulatory frameworks.

The countries in this category – Denmark, Estonia, Finland, Croatia, Ireland, Luxembourg, and Sweden – have a significant proportion of individuals (24 – 32%) using privacy-protecting software, indicating a more robust commitment to online privacy. These countries have generally high levels of digital literacy, education on online privacy, and strong privacy regulations in place. For example, Estonia and Finland are known for their advanced digital infrastructures, while Sweden and Denmark have a long-standing tradition of valuing data protection and privacy. The adoption rate suggests that these countries are likely leading the way in terms of educating users about the importance of privacy tools and providing them with accessible means to protect themselves.

Malta and the Netherlands are the only countries in this category (32 – 40%). This relatively high percentage of users adopting privacy software reflects a strong digital culture focused on personal data protection. The Netherlands, in particular, is known for its high level of privacy awareness and is home to some of the strictest privacy laws in Europe. Malta, though smaller, may also have strong privacy laws and a tech-savvy population. This high percentage may also be due to proactive government policies, privacy advocacy groups, and a digital population that values their privacy rights. These countries likely have high levels of trust in their privacy tools and an informed user base that actively seeks to protect their data.

Belgium stands alone in this category, with over 40% of individuals using software to limit tracking. This is a notable figure, showing that privacy awareness and action are highly prioritized in Belgium. Belgium benefits from a combination of high digital literacy, active privacy advocacy, and strong regulatory frameworks, particularly as part of the European Union's GDPR-compliant policies. The high usage of privacy tools here suggests that users are very proactive about their online security and privacy, possibly due to a deep cultural and governmental focus on data protection and rights.

2.3. Percentage of individuals that manage access to personal data on the internet (3 months): read privacy policy statements before providing personal data in 2023

Table 3 Percentage of individuals that manage access to personal data on the internet (3 months): read privacy policy statements before providing personal data in 2023

% of individuals 2.3.	Countries	No of countries
less than 21	BE, CY, FR, LU	4
21-26	SI	1
26-31	EL, PL, RO, SE	4
31-36	BG, CZ, DE, DK, IT, LV	6
36-41	EE, ES, HR, IE, LT, MT, PT, SK	8
more than 41	AT, FI, HU, NL	4
Total		27

Belgium, Cyprus, France, and Luxembourg fall into this category, with fewer than 21% of individuals reading privacy policy statements before sharing personal data. This indicates a relatively low level of privacy awareness in these countries. While these countries have access to privacy policies and data protection regulations, it appears that many individuals are not fully engaging with them. Possible reasons could include a lack of understanding of the importance of privacy policies, low awareness of the risks associated with sharing personal data, or a general trust in the services they use. Despite the existence of strong regulations like GDPR in the European Union, it seems that not all individuals prioritize reading the terms before providing their personal information.

Slovenia is the only country in this range, with 21-26% of individuals checking privacy policies before providing personal data. This reflects a somewhat moderate level of privacy-conscious behavior, although still on the lower end. It suggests that while there is some awareness, privacy concerns are not yet a widespread practice for most Slovenian internet users. Slovenia may have a growing awareness of privacy and data protection, but like many other countries, there may be competing factors such as convenience and trust in online platforms, leading users to overlook reading privacy policies.

Greece, Poland, Romania (30.73%), and Sweden are in this category, with 26-31% of individuals reading privacy policies before sharing personal data. This shows a moderate level of privacy awareness. The higher percentage in Sweden could be attributed to its strong culture of digital rights and a population more aware of privacy issues due to a high level of digital education and government focus on data protection. In contrast, countries like Greece, Poland, and Romania may still be developing stronger privacy practices, with users showing some concern but not yet engaging with privacy policies on a regular basis.

Bulgaria, Czech Republic, Germany, Denmark, Italy, and Latvia are in this range, where 31-36% of individuals are reading privacy policy statements before providing personal data. This percentage indicates a moderate-to-high level of privacy engagement, suggesting that people in these countries are more aware of the importance of protecting their personal information online. Germany and Denmark are notable for their strong privacy regulations (such as GDPR) and culture, which likely contributes to the higher percentage in these countries. However, there is still room for improvement in other countries in this range, like Bulgaria and Czech Republic, where data privacy concerns may not be as widespread or deeply ingrained.

Countries like Estonia, Spain, Croatia, Ireland, Lithuania, Malta, Portugal, and Slovakia show a higher level of engagement with privacy policies, with 36-41% of individuals reading them before sharing their personal data. This reflects a growing trend toward online privacy awareness and self-protection. Estonia, known for its advanced digital infrastructure, leads the way in digital literacy and data protection. Spain and Ireland also benefit from strong awareness and regulatory frameworks. This indicates that individuals in these countries are becoming more proactive in managing their personal data, perhaps as a result of digital literacy campaigns, data protection laws, and public concern about privacy risks.

Austria, Finland, Hungary, and the Netherlands are the countries in this category, with over 41% of individuals reading privacy policies before providing their personal data. This is the highest level of engagement, showing that these countries have a particularly high awareness of privacy issues. Finland and the Netherlands are known for their strong data protection laws and high levels of digital literacy, leading to a population that is well-versed in privacy rights and protections. In these countries, individuals seem to be actively seeking to manage their personal data and make informed decisions about their privacy online. The high percentage also suggests that privacy is a key concern for these users, and they may take extra steps to ensure they are informed about how their data will be used.

2.4. Percentage of individuals that manage access to personal data on the internet (3 months): restricted or refused access to the geographical location in 2023

Table 4 Percentage of individuals that manage access to personal data on the internet (3 months): restricted or refused access to the geographical location in 2023

% of individuals 2.4.	Countries	No of countries
less than 22	BG	1
22-33	LV, RO, SI	3
33-44	CY, DE, EL, HR, IT, LT, PL, SK	8
44-55	AT, BE, CZ, EE, HU, LU, MT, PT	8
55-66	DK, ES, FR, IE, SE	5
more than 66	FI, NL	2
Total		27

Bulgaria has the lowest percentage in this category, with fewer than 22% of individuals restricting or refusing access to their geographical location. This suggests that privacy concerns related to location tracking are relatively low in Bulgaria, and many users might not be aware of or concerned about the risks of sharing their geographical data. Possible reasons for this could include a lack of privacy education, less emphasis on location-based data privacy, or a general trust in digital platforms. Users in Bulgaria might have less awareness of the risks related to location data. There may be fewer readily accessible tools or resources that allow Bulgarians to manage or limit location access and they may be more focused on other internet usage concerns, such as access to services or convenience, rather than restricting location sharing.

Latvia, Romania (26.60%), and Slovenia fall into this range, with 22-33% of individuals restricting or refusing access to their geographical location. This range suggests a moderate level of privacy concern regarding location tracking in these countries. Latvia and Romania might have lower levels of privacy awareness than other EU countries, which could explain the moderate engagement with location restrictions. Slovenia may be slightly more advanced in privacy awareness but still shows room for improvement. In these countries there is likely a rising awareness of the risks of sharing location data, especially with the growth of location-based services. GDPR has likely raised awareness, but these countries might still be developing stronger digital literacy and tools for location data management.

Cyprus, Germany, Greece, Croatia, Italy, Lithuania, Poland, and Slovakia fall into the 33-44% range. This indicates a stronger, though still moderate, level of concern about location privacy. These countries exhibit a more noticeable engagement with privacy tools to restrict geographical location access, especially in comparison to the first two categories. Germany is likely a standout here, with a long tradition of data protection laws, including GDPR, which has fostered awareness about the risks of location tracking. Cyprus and Greece, while improving, still show moderate privacy practices, which could be related to a combination of trust in local services and a lack of active privacy education.

Countries like Austria, Belgium, Czech Republic, Estonia, Hungary, Luxembourg, Malta, and Portugal fall within this range (44 – 55%). This suggests that in these countries, around half of the population is actively managing their geographical data privacy by restricting or refusing access to location data. Estonia is a clear leader in digital privacy practices, known for its advanced digital services and a culture of privacy protection. Other countries like Austria and Luxembourg are likely to have higher digital literacy and privacy-conscious populations due to strong legal frameworks such as GDPR. Citizens in these countries are likely more aware of the risks associated with location data sharing and are more proactive in managing access to their geographical location. These countries often have high levels of digital literacy, as well as tools that make it easier for users to manage privacy settings. The presence of comprehensive data protection laws like GDPR in many of these countries contributes to higher engagement with privacy tools.

Countries such as Denmark, Spain, France, Ireland, and Sweden fall into the 55-66% range, where more than half of the population restricts or refuses access to their geographical location. These countries show a high level of concern for privacy and indicate that managing location data is an important issue for many users. Denmark and Sweden are particularly well-known for their strong privacy laws and digital literacy. France and Spain have seen increasing privacy awareness, particularly in light of various high-profile data breaches and scandals, motivating users to be more protective of their location data. Scandinavian countries like Denmark and Sweden are generally at the forefront of privacy rights, with a strong focus on user control over personal data. These countries have strong privacy laws, which are enforced, and digital literacy campaigns that help users understand the risks associated with sharing location data. Given the number of high-profile privacy incidents across Europe, users in these countries are increasingly cautious about sharing personal data.

Finland and the Netherlands are the leading countries in this category, with over 66% of individuals restricting or refusing access to their geographical location. These countries demonstrate the highest level of awareness and action regarding location privacy. Finland is particularly notable for its advanced digital infrastructure and strong privacy protections. The Dutch population is known for being highly informed about their digital rights and has a long history of advocating for privacy and data protection. Both Finland and the Netherlands have a culture that strongly emphasizes personal privacy, digital rights, and data protection. These nations often lead the way in adopting digital privacy tools and creating a privacy-conscious population. Citizens in these countries are highly informed about privacy and understand the potential risks of sharing location data, leading them to be more proactive in managing their privacy settings.

2.5. Percentage of individuals that manage access to personal data on the internet (3 months): limited access to profile or content on social networking sites or shared online storage in 2023

Table 5 Percentage of individuals that manage access to personal data on the internet (3 months): limited access to profile or content on social networking sites or shared online storage in 2023

% of individuals 2.5.	Countries	No of countries
less than 20	RO	1
20-31	BG, DE, EL, IT, LV, PL, SI, SK	8
31-42	AT, BE, CY, EE, FR, HR, HU, LT, LU,	9
42-53	DK, IE, MT, SE	4
53-64	CZ, ES, FI, PT	4
more than 64	NL	1
Total		27

Romania (19.65%) has the lowest percentage, with fewer than 20% of individuals limiting access to their profile or content on social networking sites or shared online storage. This suggests that in Romania, many users are either unaware of the privacy risks associated with social networks or may not feel the need to control the access to their personal data online. There may be a cultural tendency to share more openly or a lack of emphasis on digital privacy education. Digital privacy tools and settings on social platforms can be complicated to navigate. Users may not be equipped with the necessary knowledge or skills to manage their privacy settings effectively.

Countries like Bulgaria, Germany, Greece, Italy, Latvia, Poland, Slovenia, and Slovakia fall into the 20-31% range, indicating a moderate level of concern for privacy on social networking sites and shared online storage. Around one-quarter to one-third of individuals in these countries are actively managing their personal data by limiting access to their profiles or content.

Germany, being a leader in privacy law with GDPR, likely stands out in this group, with higher awareness about data protection and personal privacy. However, countries like Bulgaria, Greece, and Slovakia might be at earlier stages in adopting robust privacy practices, with a lower percentage of individuals actively managing access. These countries have varying levels of digital literacy. Some may have strong privacy education programs, while others might not. People in these countries might trust social media platforms and may not see the need to limit access unless prompted by negative experiences or data breaches.

Austria, Belgium, Cyprus, Estonia, France, Croatia, Hungary, Lithuania, and Luxembourg fall within this range (31 – 42%). These countries have a higher percentage of individuals who actively manage their privacy settings by restricting access to personal data on social networks and online storage. France and Estonia are likely to have higher levels of digital literacy and a stronger focus on privacy, especially given the prominence of GDPR. Luxembourg and Austria also have strong privacy laws in place, encouraging individuals to be more proactive about managing their personal data. The influence of GDPR plays a significant role in shaping privacy behavior in these countries. Citizens in these countries might feel that the tools and settings available to them on social platforms are reliable and can help them manage their privacy effectively.

Denmark, Ireland, Malta, and Sweden have a more pronounced percentage (42-53%) of individuals managing their privacy settings on social media and online storage platforms. This range reflects a high level of concern for data protection and a strong trend toward taking proactive steps in managing online privacy. Sweden and Denmark are known for their robust privacy laws and high digital literacy. These countries often lead in global rankings for privacy and data protection, and the population is well-informed about the risks of oversharing online. The presence of user-friendly privacy tools and resources encourages individuals to limit access to their personal data. These countries often have higher levels of digital literacy, making it easier for citizens to understand and implement privacy measures.

Czech Republic, Spain, Finland, and Portugal show a strong commitment to managing access to personal data on social networks and online storage, with 53-64% of individuals limiting access. These countries are likely to have a higher level of concern about online privacy and the risks associated with personal data exposure. Finland and Spain stand out in this group, with Finland having a high level of digital literacy and strong privacy practices. Spain has also seen an increase in privacy awareness due to recent scandals and increased regulation. The influence of GDPR and national privacy laws is likely significant in these countries. Increased awareness around online privacy risks, including potential data breaches and misuse, has led to more individuals taking action to protect their data.

The Netherlands is the only country in this category, with more than 64% of individuals actively limiting access to their profile or content on social networking sites or online storage platforms. This high percentage reflects a high level of privacy awareness and a strong culture of data protection. The Netherlands is known for its strong privacy laws, including GDPR implementation, and a population that is highly aware of digital rights and privacy risks. The Netherlands has a well-established infrastructure for data protection, and individuals are confident in using privacy settings to manage their online data.

2.6. Percentage of individuals that manage access to personal data on the internet (3 months): refused allowing the use of personal data for advertising purposes in 2023

Table 6 Percentage of individuals that manage access to personal data on the internet (3 months): refused allowing the use of personal data for advertising purposes in 2023

% of individuals 2.6.	Countries	No of countries
less than 20	BG	1
20-30	LV, RO	2
30-40	PL, SI, SK	3
40-50	BE, DE, EE, EL, HR, HU, IT, LT, LU, MT	10
50-60	AT, CY, CZ, FR, PT, SE	6
more than 60	DK, ES, FI, IE, NL	5
Total		27

Bulgaria is the only country with fewer than 20% of individuals refusing to allow the use of their personal data for advertising purposes. This indicates that a large majority of people in Bulgaria may either be unaware of the risks associated with data sharing for advertising or may not actively take steps to refuse this practice. Digital privacy issues might not be as pressing or well understood by the population in Bulgaria, especially regarding targeted advertising. Bulgarians may not be aware of available settings or options to limit advertising tracking, or they may trust advertisers more than individuals in countries with higher percentages of refusal.

Latvia and Romania (28.39%) fall within this range, where around 20-30% of individuals refuse the use of their personal data for advertising purposes. This shows that while some awareness of privacy issues exists, a significant portion of the population still allows data sharing for targeted advertising. There may be increasing awareness of digital privacy, but many people still don’t take active steps to prevent advertising tracking. People in these countries may trust advertising platforms or believe that the benefits of personalized ads outweigh privacy concerns. While tools to refuse advertising use may be available, some users may not be fully educated on how to use them, or they may not consider the trade-off significant enough.

Poland, Slovenia, and Slovakia have between 30-40% of individuals refusing the use of their personal data for advertising purposes. This indicates a moderate level of privacy awareness, with a larger portion of the population opting out of data collection for advertising. A growing awareness of privacy issues, including the risks of personalized ads, is likely influencing more people in these countries to take control of their personal data. Privacy regulations like GDPR may have had a significant impact, leading to higher engagement with privacy settings.

Countries such as Belgium, Germany, Estonia, Greece, Croatia, Hungary, Italy, Lithuania, Luxembourg, and Malta have between 40-50% of individuals refusing the use of their personal data for advertising purposes. This range suggests a high level of concern about privacy, where a significant portion of the population is actively managing their data preferences to limit advertising targeting. Countries like Germany and Belgium have a strong tradition of data protection, and the GDPR likely plays a key role in raising awareness and encouraging individuals to take steps to protect their privacy. People in these countries tend to have a higher level of awareness and knowledge about how their data is used, particularly for advertising purposes, and are more likely to use tools to limit its use. Many of these countries have experienced public discussions about data exploitation and surveillance, leading to a greater emphasis on controlling personal data.

Countries like Austria, Cyprus, Czech Republic, France, Portugal, and Sweden have between 50-60% of individuals refusing to allow the use of their personal data for advertising. This demonstrates a very high level of privacy awareness, where more than half of the population in these countries is actively managing their data preferences and refusing the use of their personal data for advertising. The implementation of GDPR across Europe has significantly increased awareness and made it easier for individuals to opt out of data collection for targeted ads. These countries have high digital literacy, meaning people are well-versed in the tools available to limit advertising use and understand the risks associated with online data sharing.

Denmark, Spain, Finland, Ireland, and the Netherlands have more than 60% of individuals refusing the use of their personal data for advertising purposes. This high percentage reflects a very strong privacy culture in these countries, where the majority of people actively refuse targeted advertising based on their personal data. These countries have a very strong emphasis on privacy rights, and people are well-educated about how to manage their data preferences. There is likely a cultural emphasis on individual privacy and data protection, with citizens trusting privacy tools and feeling empowered to control the use of their data for commercial purposes.

2.7. Percentage of individuals that manage access to personal data on the internet (3 months): checked that the website where personal data provided was secure in 2023

Table 7 Percentage of individuals that manage access to personal data on the internet (3 months): checked that the website where personal data provided was secure in 2023

% of individuals 2.7.	Countries	No of countries
less than 6	BG	1
6-16	RO	1
16-26	BE, CY, DE, EL, IT, LT, LV, PL, SI, SK	10
26-36	HR, HU, LU, SE	4
36-46	AT, CZ, EE, FR, IE	5
more than 46	DK, ES, FI, MT, NL, PT	6
Total		27

Bulgaria has fewer than 6% of individuals checking whether a website is secure before providing personal data. This suggests a very low level of awareness or concern about website security when it comes to personal data protection in this country. Many people may not understand the risks associated with providing personal data to unsecured websites or may not know how to verify a website's security. Limited understanding of basic security measures, such as recognizing secure website URLs (with HTTPS) or identifying secure connections, may contribute to this low percentage.

Romania (6.78%) falls into the 6-16% range, indicating a slightly lower percentage of individuals who check the security of a website before providing personal data. However, this still suggests a relatively low level of engagement with online security practices. Users may assume that local or familiar websites are secure and may not think to check the security of unfamiliar sites. Digital literacy might still be developing, with people not fully educated about how to check for website security before sharing personal information.

Belgium, Cyprus, Germany, Greece, Italy, Lithuania, Latvia, Poland, Slovenia, and Slovakia have between 16-26% of individuals checking the security of websites before providing personal data. This suggests a moderate awareness of online security practices in these countries. While the level of security checks is still relatively low, these countries likely have higher digital literacy than those with fewer checks, and individuals are starting to realize the importance of ensuring a website is secure. In countries like Germany (which has strong privacy laws like GDPR), there may be greater awareness of security measures required before sharing personal data online.

Croatia, Hungary, Luxembourg, and Sweden fall into this range, where 26-36% of individuals check whether a website is secure before submitting their personal data. This represents a higher level of awareness and caution about website security. In countries like Sweden, where there is a high level of digital literacy and a strong focus on privacy, individuals are more likely to be cautious about where and how they share personal data. These countries may have stronger digital education systems that teach individuals how to identify secure websites (e.g., recognizing HTTPS and security certificates). Governments and companies in these countries may provide more robust resources and campaigns that help people understand the importance of checking website security.

Austria, Czech Republic, Estonia, France, and Ireland have between 36-46% of individuals checking the security of websites before providing personal data. This reflects a relatively high level of caution and digital awareness. GDPR and other data protection laws have likely influenced individuals in these countries to be more cautious with their personal data, encouraging the practice of checking website security. Countries like Estonia and Ireland have a high level of digital engagement and education, where individuals are likely well-informed about the risks of unsecured websites.

Denmark, Spain, Finland, Malta, the Netherlands, and Portugal have more than 46% of individuals checking whether websites are secure before submitting their personal data. These countries demonstrate a very high level of awareness and concern about online security. Countries like Finland and Denmark are leaders in digital literacy and have strong educational programs focused on online security and privacy, resulting in more individuals checking website security. GDPR and other national data protection laws have contributed to a high level of data protection awareness, encouraging individuals to take responsibility for their online security.

2.8. Percentage of individuals that manage access to personal data on the internet (3 months): at least one of I_MAPS_RPS [1], I_MAPS_RRGL [2], I_MAPS_LAP [3], I_MAPS_RAAD [4], I_MAPS_CWSC [5] in 2023

Table 8 Percentage of individuals that manage access to personal data on the internet (3 months): at least one of I_MAPS_RPS, I_MAPS_RRGL, I_MAPS_LAP, I_MAPS_RAAD, I_MAPS_CWSC in 2023

% of individuals 2.8.	Countries	No of countries
less than 47	RO	1
47-55	BG, LV, PL, SI	4
55-63	HR, IT, LT, SK	4
63-71	BE, CY, DE, FR, LU, EL	6
71-79	AT, EE, ES, HU, MT, PT, SE	7
more than 79	NL, CZ, DK, FI, IE	5
Total		27

The data refers to various privacy management actions that individuals take to control access to their personal data on the internet over a three-month period. Each of the measures outlined in the provided variables – [1] through [5] – reflects a different aspect of how individuals are actively managing their online privacy.

2.8.1. Reading Privacy Policy Statements Before Providing Personal Data (I_MAPS_RPS)

This measure refers to individuals who have actively read the privacy policy statements of websites or services before sharing personal data. This is one of the most basic yet effective ways to understand how a website or service intends to use your personal data. It gives individuals insight into whether their data will be shared with third parties, retained, or used for specific purposes like advertising or profiling. Engaging in this behavior shows a high level of privacy awareness, as users are making informed decisions about their data. However, many individuals may still avoid reading privacy policies due to the length, complexity, or lack of clarity in many policies.

2.8.2. Restricting or Refusing Access to Geographical Location (I_MAPS_RRGL)

This measure indicates that individuals have restricted or refused access to their geographical location while using websites or applications. Many websites and apps ask for access to a user's location for a variety of reasons, such as personalized content or advertisements. By restricting or refusing access, individuals protect their location privacy and prevent unnecessary data collection.

2.8.3. Limiting Access to Profile or Content on Social Networking Sites or Shared Online Storage (I_MAPS_LAP)

This refers to individuals who have limited access to their profiles or shared content on social media platforms or cloud storage services. Limiting who can see certain posts, profiles, or content on social networking sites or shared online storage is crucial for managing one's digital footprint. Restricting access helps ensure that only trusted individuals or groups can view sensitive or personal information. By limiting access, users prevent unauthorized access to personal content, which can help avoid data breaches or exploitation. Social media platforms can often be overly permissive with privacy settings, so users who adjust these settings are taking an important step in safeguarding their online identity.

2.8.4. Refusing Allowing the Use of Personal Data for Advertising Purposes (I_MAPS_RAAD)

This measure reflects individuals who have refused to allow websites or services to use their personal data for targeted advertising purposes that can often be sold to third parties or used to build extensive personal profiles. Refusing permission to use personal data for ads can reduce unwanted data tracking, prevent targeted ads, and help protect personal privacy. Individuals who take this step actively protect themselves from invasive marketing techniques. It’s a clear indication of a user's desire to preserve privacy and limit how companies use their data. The more people who opt-out, the more pressure it puts on companies to offer transparent, privacy-respecting practices.

2.8.5. Checking Whether the Website Where Personal Data Was Provided Was Secure (I_MAPS_CWSC)

This measure indicates whether individuals have checked whether the website they provided personal data to is secure, such as verifying if the site uses HTTPS, a safety logo, or a security certificate. Ensuring website security before sharing personal data helps protect against identity theft, fraud, and other cyber threats. Individuals who take this step demonstrate a strong understanding of online security and are taking proactive measures to protect their personal information from cybercriminals.

Romania (46.28%) is the only country in this range, where less than 47% of individuals engage in at least one of the privacy management actions. There may be limited awareness or understanding of online privacy issues, with many users not fully aware of the available privacy settings. Or the population may have lower levels of digital literacy when it comes to managing privacy online. People may not prioritize privacy management or may trust websites and online services to a higher degree, resulting in less effort to manage personal data.

Bulgaria, Latvia, Poland, and Slovenia are in the range of 47 – 55%. These countries might be starting to recognize the importance of privacy, influenced by regulations like the GDPR (General Data Protection Regulation), leading to a moderate increase in engagement. People in these countries are becoming more cautious about online privacy, though their engagement is still relatively moderate compared to other regions. Also there may be a rising number of digitally literate individuals in these countries who are starting to take privacy more seriously, though broader adoption is still in progress.

Between 55-63% are Croatia, Italy, Lithuania, and Slovakia. People in these countries may have higher levels of understanding about the risks of sharing personal information online, motivating them to take steps to protect their privacy. As privacy regulations like the GDPR continue to take effect, individuals in these countries may feel more empowered to manage their personal data and control access to it. Given the widespread use of social media platforms, individuals might be increasingly aware of the importance of managing their profiles and limiting access to personal data on these platforms.

Belgium, Cyprus, Germany, France, Luxembourg, and Greece are in the range of 63-71%. These countries are more likely to have strict data protection laws, such as the GDPR, that help raise awareness about online privacy and compel individuals to take privacy protection seriously. There may be a cultural emphasis on the importance of safeguarding personal data, which could contribute to higher engagement in privacy management activities. These countries may have a more digitally literate population that is better equipped to navigate the complexities of managing online privacy, leading to a higher adoption of privacy management practices.

Austria, Estonia, Spain, Hungary, Malta, Portugal, Sweden are in the range of 71-79% of individuals that engage in at least one of the privacy management actions. Citizens in these countries are likely to be highly aware of online security and privacy, especially as these countries often have strong digital infrastructures and a highly connected population. The influence of strong data protection laws, such as the GDPR, and national privacy initiatives likely contributes to individuals being proactive about managing their personal data. As data breaches and cyber threats have become more common, individuals in these countries may have developed a heightened awareness of the risks associated with online privacy, motivating them to engage in protective actions.

With more than 79% of individuals that engage in at least one of the privacy management actions are Netherlands, Czech Republic, Denmark, Finland, and Ireland. These countries exhibit the highest level of engagement, possibly due to a well-established culture of privacy protection and strong national regulations that prioritize personal data security. Countries like Denmark, the Netherlands, and Finland have a reputation for robust data protection practices and strong public trust in privacy laws. This trust likely leads to greater participation in privacy management practices. A high level of digital literacy, along with active campaigns to educate citizens about their privacy rights, likely results in a more privacy-conscious population that takes proactive steps to protect their data.

3. CONCLUSIONS

Trust, security, and privacy are very important today. The internet must be used with great caution, and security measures should be regularly updated.

Concerning the use of browser settings to prevent or limit cookies most European countries are in the mid-range for online privacy interest, but there are clear examples of countries with high interest, such as Finland and the Netherlands. Data protection policies, national regulations, and digital education significantly influence user behavior in this regard.

The varying levels of privacy software adoption to limit tracking across EU countries highlight the differing degrees of awareness, education, and government regulation regarding online privacy. Countries with higher usage rates, such as Belgium, the Netherlands, and the Scandinavian countries, demonstrate a more advanced level of understanding and action towards data protection. Meanwhile, countries like Bulgaria and Cyprus show that there is still work to be done in terms of raising awareness and improving access to privacy tools. National regulations like the GDPR have had a significant impact on encouraging privacy protection across the EU, but adoption rates still differ due to factors like digital literacy, accessibility of tools, and the general cultural attitudes toward privacy in each country.

The data shows varying levels of awareness and action regarding privacy policies across European countries. While some countries have made significant progress in terms of data protection awareness (e.g., Finland, Austria, Netherlands), others still lag behind, with lower percentages of individuals engaging with privacy policies before sharing personal data (e.g., Belgium, Cyprus). The overall trend reflects a growing awareness of the importance of online privacy, especially in countries with strong digital infrastructure and privacy regulations. However, there is still a significant gap in how different populations engage with privacy policies, which could be influenced by factors such as digital education, trust in online services, and the perceived complexity or inconvenience of reading privacy policies. Countries with a higher percentage of people reading privacy policies are likely benefiting from stronger privacy regulations, cultural factors, and more accessible information about data rights.

The data reveals a clear trend of increasing privacy awareness and actions related to location tracking across Europe. The countries with higher percentages (e.g., Finland, Netherlands, Denmark) have a strong culture of privacy, with citizens who are well-educated about the risks of sharing geographical data. These countries also tend to have robust privacy laws and regulations, which contribute to a more proactive approach to managing personal information. On the other hand, countries with lower engagement (e.g., Bulgaria, Latvia) may still be in the process of building up their privacy awareness and digital infrastructure. While GDPR has raised awareness about data protection across the EU, cultural and digital literacy factors play a significant role in determining how individuals approach location privacy.

The data indicates a growing trend of individuals across Europe becoming more aware of their digital privacy, particularly regarding social media and online storage platforms. Countries with higher percentages (e.g., Netherlands, Denmark, Finland) have a strong culture of data protection, supported by strong regulations like GDPR and high levels of digital literacy. Conversely, countries with lower percentages (e.g., Romania, Bulgaria) may have lower levels of privacy awareness and fewer tools available to help individuals manage access to their personal data. In summary, while privacy concerns are on the rise across Europe, there remains a significant gap between countries that have established a strong culture of privacy and those still developing such practices. The increasing implementation of GDPR is likely contributing to higher levels of engagement with privacy tools, but digital literacy and public awareness remain key drivers of behavior in this area.

The data illustrates significant variation across Europe in how individuals manage their personal data, specifically with respect to advertising purposes. The trend is clear: countries with stronger privacy protections, such as those with higher percentages (e.g., Denmark, Netherlands, Germany, Sweden), exhibit a higher level of privacy awareness and proactive management of personal data. The influence of GDPR is evident, as it has played a central role in educating and empowering individuals to refuse the use of their personal data for targeted advertising. Countries with lower percentages (e.g., Bulgaria, Romania) may have lower levels of digital literacy or less familiarity with privacy tools, contributing to a lower refusal rate. However, across the board, there is an increasing trend of individuals refusing to allow the use of their personal data for advertising purposes, indicating growing privacy concerns and an increasing desire for control over personal information.

The data highlights a strong correlation between digital literacy, privacy regulations, and the percentage of individuals checking website security before providing personal data. Countries with higher percentages, such as Denmark, Finland, and the Netherlands, demonstrate advanced digital literacy and a culture of privacy, with individuals taking more proactive steps to ensure their data is protected. On the other hand, countries with lower percentages, like Bulgaria and Romania, indicate that awareness and education around online security may still be developing. These countries could benefit from increased awareness campaigns and education on how to identify secure websites to protect personal data. Overall, the trend suggests that across Europe, individuals are becoming more conscious of the importance of checking website security before submitting personal data, with countries with higher digital literacy and stronger privacy regulations leading the way.

As regional trends, the countries in Western Europe and Northern Europe tend to have higher engagement in managing personal data privacy. This may be due to more established privacy laws, higher levels of digital literacy, and a cultural emphasis on personal data protection. Concerning the GDPR Influence, the countries in the European Union (EU), particularly those with strong privacy frameworks like the GDPR, are more likely to see high levels of engagement in data privacy measures. The GDPR has significantly impacted individuals' awareness and understanding of their rights over personal data, leading to a higher percentage of people taking active measures to protect their data.

Taking into consideration the growing privacy awareness we can see that while countries like Romania and Bulgaria show lower engagement, privacy awareness is gradually growing across Europe. As digital literacy and awareness rise, we can expect more individuals in these regions to engage with privacy management practices in the future. In conclusion, the data confirms a significant divide in privacy management practices across Europe, with Western and Northern European countries showing the highest levels of engagement. This reflects the importance of regulatory frameworks, digital literacy, and cultural attitudes toward privacy in shaping how individuals protect their personal data online.

These trends illustrate a significant shift towards increased awareness and control over personal data. Individuals are taking more steps to protect their privacy, from limiting cookies to managing how their data is used for advertising. As privacy concerns continue to grow, it is evident that people are becoming more proactive in managing their online identities, and businesses must adapt to these evolving expectations by offering greater transparency and stronger privacy controls.

ENDNOTES

[1] I_MAPS_RPS – I have carried out the following to manage access to my personal data on the internet in the last 3 months: Read privacy policy statements before providing personal data.
[2] I_MAPS_RRGL – I have carried out the following to manage access to my personal data on the internet in the last 3 months: Restricted or refused access to my geographical location.
[3] I_MAPS_LAP – I have carried out the following to manage access to my personal data on the internet in the last 3 months: Limited access to profile or content on social networking sites or shared online storage.
[4] I_MAPS_RAAD – I have carried out the following to manage access to my personal data on the internet in the last 3 months: Refused allowing the use of personal data for advertising purposes.
[5] I_MAPS_CWSC – I have carried out the following to manage access to my personal data on the internet in the last 3 months: Checked that the website where I provided personal data was secure (e.g. https sites, safety logo or certificate).

REFERENCES

[1]https://ec.europa.eu/eurostat/data/database
[2]https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm
[3]https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_ip20/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci
[4]https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_sp20/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci
[5]https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_prv20/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci
[6]https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_acfas/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci
[7]***Eurostat, *European compilers' manual for statistics on the use of ICT in households and by individuals*, 2023 edition

BOOK REVIEW

TOGETHER, WITHOUT... DISCRIMINATION!
APPLIED-THEMATIC GUIDE

Author: Maria Dorina PAȘCA

Publisher:
- University Press Targu Mureș, 2018 (Romanian version)
- Generis Publishing, 2024 (English translation)

Translation: Roxana-Maria Iagăr

Reviewer: Aura CODREANU, Associate professor, Dr.

Together, without... discrimination! is an applied-thematic guide dedicated to deepening awareness and practical understanding of ethics, cultural diversity, and non-discrimination within the healthcare context. Written by **Maria Dorina Pașca**, a specialist in medical ethics and psychology, the guide offers both conceptual frameworks and applied exercises to support students, healthcare professionals, and educators in navigating sensitive situations with respect and fairness.

The guide is structured in three core sections — conceptual definitions, thematic applications, and bibliography — and provides a reliable educational resource on vulnerable groups, prejudice, stereotypes, equality, and the right to health, with a special focus on real-world, scenario-based learning.

The author's clear writing style contributes to translating complex ethical and psychological concepts into digestible definitions and practical applications. The guide's language and structure make it suitable for both academic and non-formal learning environments.

The salient feature of the book is its interactive nature. Through open-ended exercises, situational prompts, and reflective activities such as "Complete the sentence...", "Your opinion matters...", readers are encouraged to critically engage with issues of discrimination, vulnerability, and diversity.

The greatest achievement of the author is the practical approach she proposes for working in the high-stakes environment of healthcare. Tolerance, inclusivity, human-centered care are of primary concern for the educational objectives inherent in the content of the guide.

The content is highly relevant not only for medical and nursing students, health practitioners, and medical educators navigating multicultural patient care settings, but also for public health policy advocates, human rights activists, and ethics and sociology students exploring applied discrimination cases.

Together, without... discrimination! is a guide demonstrating a drive for social responsibility and practical focus. It effectively manages to steer away from theory to the moral, emotional and professional challenges of dealing with discrimination and vulnerable people.