BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

No. 1/2025

ISSN 2284-936X
eISSN 2284-9378

Publication founded in 1937

SCIENTIFIC PUBLICATION HIGHLY ACKNOWLEDGED IN THE FIELD OF "MILITARY SCIENCES, INFORMATION AND PUBLIC ORDER" OF THE NATIONAL COUNCIL FOR ATTESTATION OF ACADEMIC DEGREES, DIPLOMAS AND CERTIFICATES, INDEXED IN INTERNATIONAL DATABASES EBSCO, CEEOL, GOOGLE SCHOLAR, INDEX COPERNICUS, PROQUEST, DOAJ, ERIH PLUS, CROSSREF

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, 2025

Scientific Reviewers

The articles published in the Bulletin of "Carol I" National Defence University, ISSN 2284-936X, L 2284-936X, are also found – title, author, abstract, content and bibliography – in the Romanian version of the journal, ISSN 1584-1928.

Content

No. 1/2025

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Deep learning on simulated gamma spectra for explosives detection using a NaI detector

Konstantinos KARAFASOULIS, Ph.D.*

*Laboratory Teaching Staff, Hellenic Army Academy, Athens, Greece
e-mail: ckaraf@gmail.com

Abstract

The detection of explosives and contraband materials using neutron activation analysis (NAA) is a critical component of modern security systems. This study investigates the feasibility of identifying explosive materials using a simple sodium iodide (NaI) scintillation detector limited to a 3 MeV gamma energy range. The detector's limitations pose a significant challenge as characteristic gamma photopeaks above this range, such as those near 10 MeV, are excluded. Utilising a 14 MeV neutron source, gamma spectra from simulated neutron interactions with explosive materials were analysed using Geant4. This work demonstrates that with advanced machine learning models, such as convolutional neural networks (CNNs) and tailored data preprocessing methods, effective discrimination between explosives and non-explosives is achievable despite these constraints.

Keywords:
Explosives Detection; Artificial Intelligence; Neutron Activation; Gamma Radiation.

Article info
Received: 29 January 2025; Revised: 17 February 2025; Accepted: 27 February 2025; Available online: 2 April 2025

Citation: Karafasoulis, K. 2025. "Deep learning on simulated gamma spectra for explosives detection using a NaI detector". *Bulletin of "Carol I" National Defence University*, 14(1): 7-18. https://doi.org/10.53477/2284-9378-25-01

Detecting explosives before detonation is vital for security, counterterrorism, and humanitarian efforts. Explosives pose significant risks in airports, government buildings, military bases, and public spaces, where early detection can save lives and prevent destruction. As terrorist tactics evolve with greater reliance on improvised explosive devices (IEDs) and concealed explosives, pre-blast detection has become more critical than ever. The risk of attacks on airports, transit systems, and public events highlights the urgency of early intervention. Beyond terrorism, landmines remain a major threat in post-conflict areas. Hidden beneath the surface, landmines and unexploded ordnance (UXO) continue to injure civilians, obstruct economic recovery, and disrupt essential activities like farming and construction. Detecting and neutralizing these devices is essential for restoring land and protecting communities. Many affected regions still suffer from landmine contamination decades after conflicts.

Pre-blast detection also plays a role in preventing the trafficking of explosives, which supports terrorism and organized crime. Smugglers conceal explosives in cargo, vehicles, and containers, making border and port screening vital. Military forces also require preemptive detection of explosives in war zones, where IEDs and traps pose serious threats. Addressing these challenges requires advanced detection technologies capable of identifying explosives across various environments.

X-ray and computed tomography (CT) scanning are standard methods for detecting bulk explosives based on density and atomic composition. Conventional X-ray systems provide 2D images, helping security personnel identify suspicious objects in luggage, cargo, and vehicles. Dual-energy X-ray systems improve detection by differentiating organic explosives from metals. However, their limited penetration depth makes them ineffective for landmine detection. CT scanning, which generates 3D reconstructions, improves detection in cargo and complex environments but remains too large and costly for field use. While effective in airports and shipping ports, CT is impractical for remote minefields or mobile detection operations.

Nuclear techniques detect explosives by analyzing their elemental composition rather than relying on shape or density. Thermal neutron activation (TNA) involves bombarding a target with low-energy neutrons, which trigger gamma-ray emissions from nitrogen, a key element in many explosives. Similarly, fast neutron analysis (FNA) utilizes high-energy neutrons, enabling deeper penetration into cargo and soil, making it a valuable tool for landmine detection. However, these methods rely on expensive neutron sources and require highly specialized detectors, such as high-purity germanium (HPGe) systems, which provide high-resolution spectral data but come at a significant cost. The combination of costly neutron sources and advanced detection equipment makes these nuclear techniques impractical for large-scale deployment in demining and security screening applications, particularly in resource-limited environments.

Sodium iodide (NaI) detectors, on the other hand, operating at 3-MeV energy limits, provide a low-cost, portable alternative for explosives detection. Unlike high-purity germanium (HPGe) detectors, which require cooling and maintenance, NaI detectors are lightweight, mobile, and cost-effective—ideal for security operations and landmine clearance. Their compact design allows for handheld use, drone integration, or vehicle-mounted deployment. However, NaI detectors have limitations in detecting high-energy gamma-ray photopeaks that are crucial for identifying explosives using neutron activation analysis (NAA). Key markers in the gamma spectra of explosives include:

- Nitrogen (N): 10.83 MeV
- Oxygen (O): 6.13 MeV
- Carbon (C): 4.44 MeV

Since these high-energy peaks exceed the 3-MeV limit of NaI detectors, alternative strategies are necessary to achieve reliable explosives detection. In this work, we present a deep learning-based method utilizing convolutional neural networks (CNNs) to effectively identify explosive materials. CNNs compensate for the hardware limitations of NaI detectors by analysing the lower-energy gamma spectrum, detecting patterns and correlations that are indicative of explosives. By training on simulated gamma spectra, our CNN-based approach extracts valuable features from limited spectral data, enabling NaI detectors to differentiate explosive materials despite their restricted energy range.

Related Work

Previous studies in explosive detection have extensively utilized neutron activation analysis combined with gamma spectroscopy to identify materials based on their elemental composition (Whetstone and Kearfott 2014). The importance of high-energy gamma photopeaks, particularly those above 3 MeV, has been highlighted in works such as (Nunes et al. 2002) where these peaks were instrumental in differentiating explosive materials from benign substances. Similarly, the IAEA's guidelines on neutron activation analysis emphasize the value of these markers for accurate material identification (IAEA 2012).

Recent advancements in machine learning have further enhanced the capability of gamma spectroscopy (Zehtabvar et al. 2024). CNNs, in particular, have shown promise in processing complex spectral data for classification tasks. For example, studies have demonstrated their effectiveness in analysing low-resolution or noisy spectra, making them suitable for applications where detector limitations exist. Moreover, Geant4-based (Agostinelli et al. 2003) simulations have been widely adopted to model neutron interactions and generate synthetic datasets, providing a controlled environment to develop and validate analytical techniques.

While prior research focused predominantly on detectors with broader energy ranges, limited work has explored the feasibility of explosive detection using low-energy detectors like NaI scintillators. This study builds on the existing body of knowledge by specifically addressing the constraints of a 3 MeV-limited detector and investigating the potential of CNNs to overcome these challenges. By leveraging both simulated data and advanced computational methods, this work aims to contribute to the development of cost-effective and efficient explosive detection systems.

Materials and Methods

1.1. Simulated Experimental Setup

The experimental setup was designed to simulate the neutron activation and gamma emission processes for a variety of materials, both explosive and non-explosive. A 14 MeV deuterium-tritium (D-T) neutron generator (Lou 2003) was positioned 30 cm away from the target material, which was modelled as a spherical sample with a radius of 2 cm. The target sphere contained either an explosive or a non-explosive material.

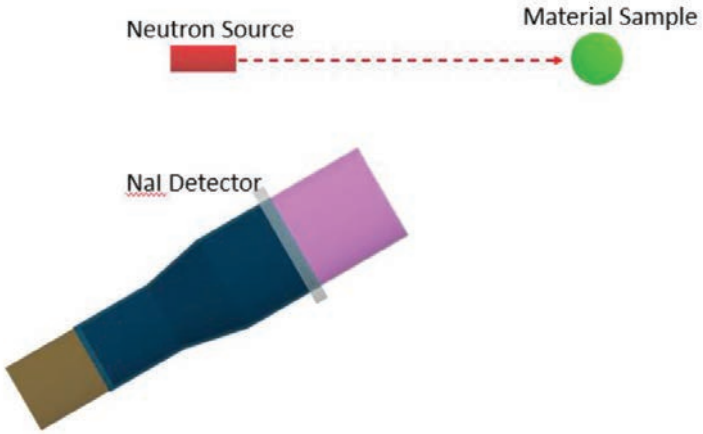


Figure 1 Schematic depiction of the experimental setup: a 14 MeV neutron generator positioned 30 cm from a 2 cm radius target sphere. A 3-inch NaI detector, placed 30 cm from the sphere at a 30° angle, records prompt gamma emissions from activated materials.

A 3-inch sodium iodide (NaI) scintillation detector was placed 30 cm from the target sphere, positioned at an angle of 30 degrees relative to the axis connecting the neutron source and the target, in order to minimize the direct neutron flux interference (Figure 1). The NaI detector was configured to record gamma emissions within its effective energy range of 0-3 MeV.

To simulate neutron interactions with the target materials, Geant4 was utilized to generate 10^9 neutron events directed toward the target sample. These high-energy neutrons activated the material, causing prompt gamma emissions that were subsequently recorded by the NaI detector. To mimic the detector's energy resolution, the recorded gamma energies were smeared using a Gaussian function with a full-width at half-maximum (FWHM) defined as

$$FWHM = A\sqrt{\frac{E}{E_c}}$$

where A = 52.96 keV and E_c = 662 keV. This smearing process ensured that the simulated spectra accounted for the realistic energy resolution of the NaI detector.

From the smeared interaction data, 2000 gamma spectra were generated per material. Each spectrum was created through random sampling of the simulated events, ensuring statistical diversity and robustness. The gamma spectra comprised 2048 bins, spanning the full energy range detectable by the NaI detector (0-3 MeV) and containing a total of 10000 counts. The gamma spectra from six such materials can be seen in Figure 2.

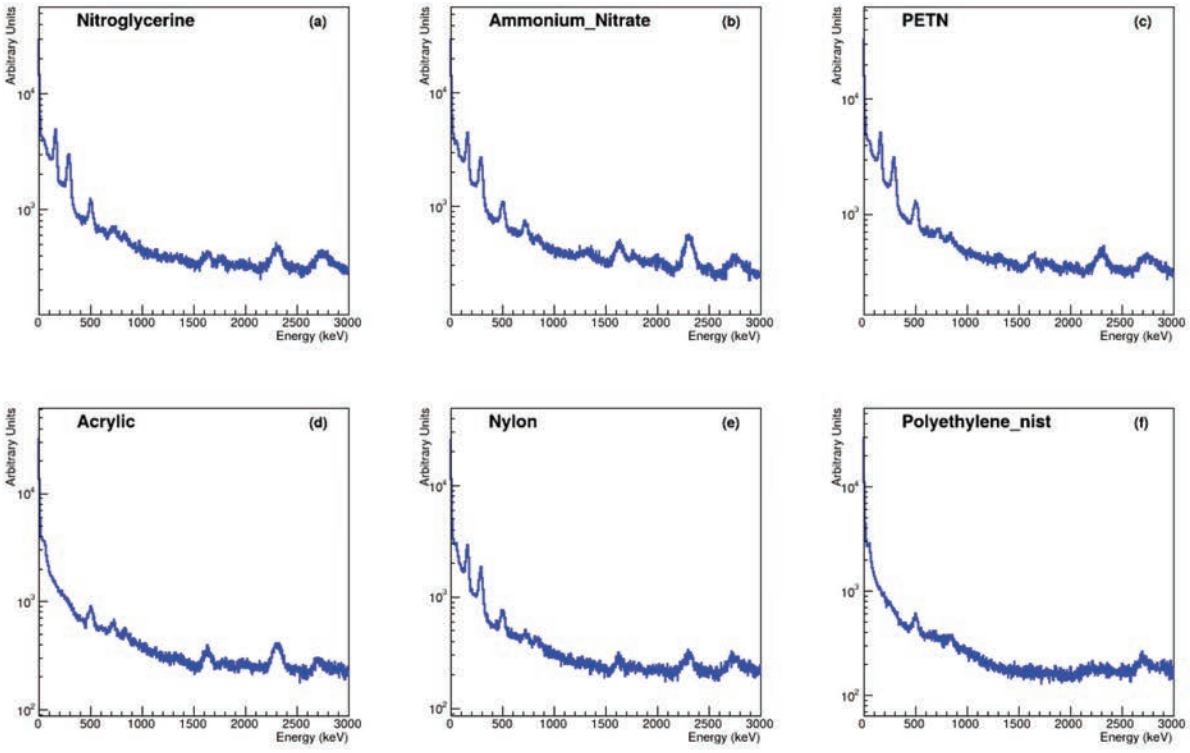


Figure 2 Gamma-ray energy spectra of various materials, plotted on a logarithmic scale. The first row displays spectra for explosive materials: **(a) Nitroglycerine, (b) Ammonium Nitrate, and (c) PETN**, while the second row contains non-explosive materials: **(d) Acrylic, (e) Nylon, and (f) Polyethylene**.

This setup was specifically designed to emulate realistic detection conditions while providing high-fidelity data for subsequent machine learning analysis. The combination of geometric arrangement, simulation accuracy, and spectrum diversity ensures reliable inputs for CNN training and validation.

The materials investigated include a mix of explosives and non-explosives. Their chemical formulas and densities are listed in Table 1.

TABLE NO. 1

Target Material Properties

Material	Chemical	Density	Category
Acrylic	$C_{12}H_{12}N_4$	1.19	Non-
Aluminium (Al)	Al	2.70	Non-
Ammonium Nitrate	NH_4NO_3	1.66	Explosive
C-4	$C_4H_6O_6N_6$	1.83	Explosive
Cellulose	$C_6H_{10}O_5$	1.0	Non-
Cocaine	$C_{17}H_{21}NO_4$	1.40	Non-
Iron (Fe)	Fe	7.87	Non-
Nitroglycerine	$C_3H_5N_3O_9$	1.60	Explosive
Nylon	$C_{11}H_{26}N_2O_4$	1.15	Non-
PAN	C_3H_3N	1.18	Non-
PETN	$C_5H_8N_4O_{12}$	1.77	Explosive
Lead (Pb)	Pb	11.34	Non-
Polyethylene	C_2H_4	0.94	Non-

1.2. CNN Architecture

Convolutional neural networks (CNNs) are powerful machine learning models designed for extracting patterns and features from data, particularly in images and sequential data like gamma spectra. CNNs use convolutional layers to identify localized features, pooling layers to reduce data dimensionality, and fully connected layers for classification. This architecture is well-suited for processing the high-dimensional data obtained from gamma spectroscopy (figure 3).

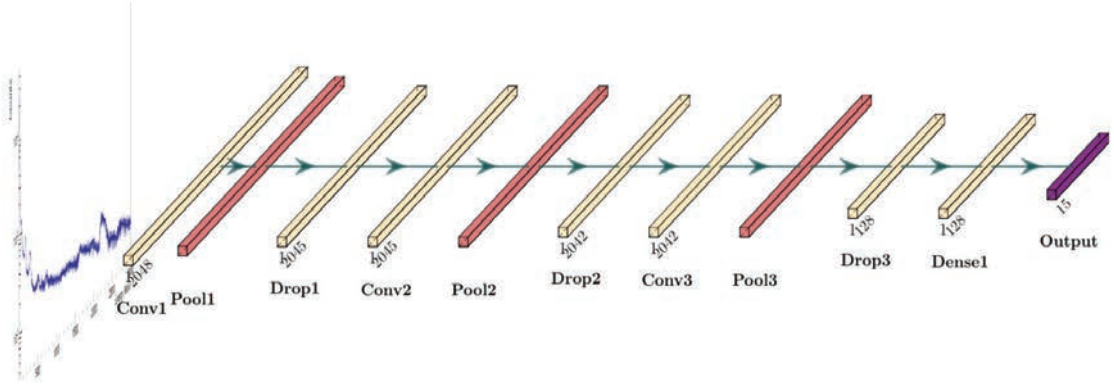


Figure 3 CNN architecture for gamma spectra classification: three convolutional layers (32, 64, 128 filters) with ReLU activation, followed by max pooling layers (window size = 2). Dropout layers reduce overfitting, and a softmax output layer enables classification.

In this study, the CNN was configured with the following architecture, using Keras (Gulli and Pal 2017):

Convolutional Layers (1D): The convolutional layers are responsible for extracting features from the input gamma spectra by applying a series of filters that slide over the data. Each filter learns specific patterns or features, such as peaks or edges, that are important for classification. The configuration of the convolutional layers is as follows:

- The **first convolutional layer** uses 32 filters, a kernel size of 3, a stride of 1, and no padding. This layer captures low-level features from the input spectra.
- The **second convolutional layer** increases the number of filters to 64, with the same kernel size, stride, and no padding. It learns more complex features by building on the patterns identified by the first layer.
- The **third convolutional layer** uses 128 filters, maintaining the kernel size of 3, stride of 1, and no padding. This layer extracts high-level features, capturing intricate details of the input data.

All convolutional layers use the **ReLU (Rectified Linear Unit)** activation function, which outputs the input directly if positive or zero otherwise. This activation introduces non-linearity to the model, enabling it to learn complex relationships in the data while also avoiding the vanishing gradient problem during training.

Pooling Layers: After each convolutional layer, a **max pooling layer** is applied. Pooling layers reduce the dimensionality of the feature maps by selecting the maximum value within a specified window, which helps retain the most important features while reducing computational complexity. Each pooling layer uses a window size of 2, a stride of 1, and no padding. This configuration ensures that relevant features are preserved while progressively reducing the size of the feature maps.

Dropout Layers: Dropout layers are incorporated to prevent overfitting by randomly setting a fraction of the layer's nodes to zero during training. This forces the model to rely on a broader set of features, improving generalization. In this architecture:

- A **dropout layer with a rate of 0.1** follows each pooling layer.
- An additional dropout layer, also with a rate of 0.1, is applied after the dense layer.

Dense Layers: The dense layer serves as a fully connected layer that maps the extracted features into a higher-dimensional representation for classification. In this architecture, the dense layer consists of 128 nodes with **ReLU activation**, enabling the model to capture and represent the complex relationships between the extracted features.

Output Layer: The final layer is the output layer, which assigns probabilities to each material class. This layer uses the **Softmax activation function**, which converts

the raw output values into probabilities that sum to 1. This makes it well-suited for multi-class classification tasks, as it enables the model to determine the most likely class for each input spectrum.

1.3. Training and Validation of the Model

The CNN was trained and validated using the gamma spectra data generated for each material. From the 2000 spectra per material, 60% were used for training, 20% for validation, and 20% for verification. To optimize the model, L1L2 regularization was applied to prevent overfitting, and a batch size of 100 was used during training.

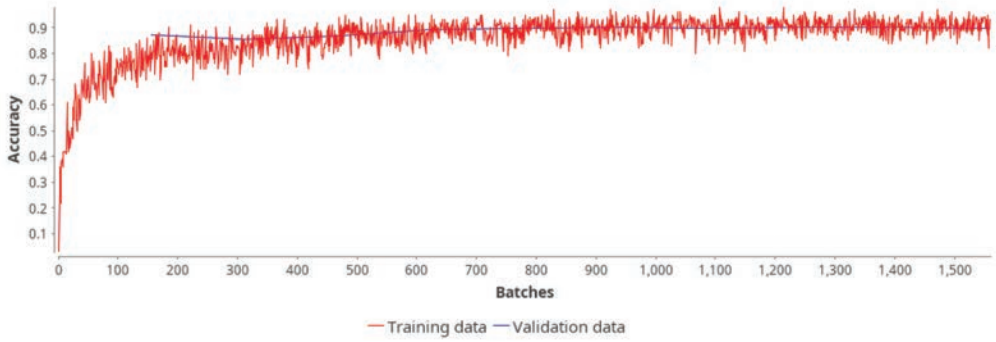


Figure 4 Training and validation accuracy of the CNN model per batch, demonstrating convergence and stability throughout training, with a final accuracy of 0.882 achieved.

The loss function employed was categorical cross-entropy, which measures the difference between the predicted probability distribution and the true distribution. This function is particularly suitable for multi-class classification tasks, as it penalizes incorrect predictions proportionally to their confidence levels.

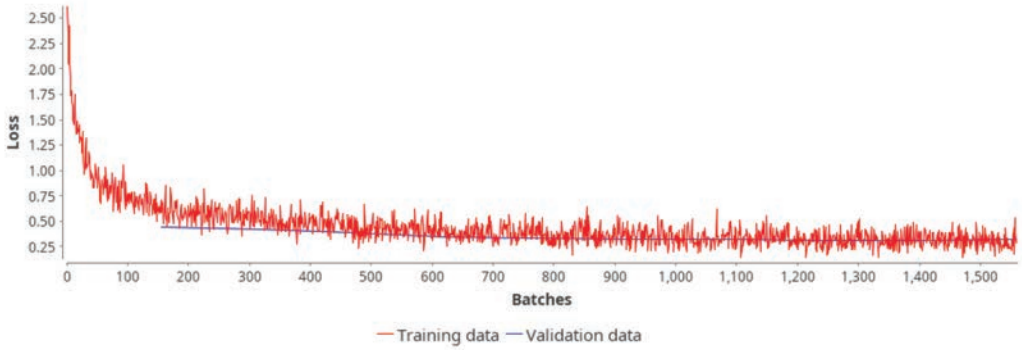


Figure 5 Loss progression during CNN training and validation, showing a steady decrease in categorical cross-entropy loss per batch, with a final loss value of 0.035 achieved.

Training performance was monitored by recording the accuracy and loss values for each batch. The training process achieved an overall accuracy of 0.882 and a final loss of 0.035. Figures 4 and 5 illustrate the training accuracy and loss progression over the batches, respectively, highlighting the model's convergence and reliability.

Results

The CNN model's performance was evaluated using 20% of the original dataset, which was reserved as verification data. The evaluation involved constructing a confusion matrix based on the model's predictions. The confusion matrix (Figure 6), with rows representing the real materials and columns the predicted materials, provides a detailed breakdown of the model's classification performance.

The overall accuracy achieved by the CNN model was 89.615%, reflecting its capability to distinguish between the various materials under study. The model's ability to generalize effectively, despite the limitations of the 3 MeV NaI detector and the constrained energy range, demonstrates the robustness of the proposed approach.

Material \ Prediction	Acrylic	Al	Ammonium_Nitrate	C-4	Cellulose	Cocaine	Fe	Nitroglycerine	Nylon	PAN	Pb	PETN	Polyethylene_nist
Acrylic	295	0	0	0	0	7	0	0	0	122	0	0	4
Al	0	440	0	0	0	0	0	0	0	0	0	0	0
Ammonium_Nitrate	0	0	370	8	0	0	0	21	6	0	0	18	0
C-4	0	0	3	369	0	0	0	0	7	0	0	1	0
Cellulose	0	0	0	0	369	3	0	1	39	0	0	2	0
Cocaine	5	0	0	0	0	377	0	0	0	2	0	0	19
Fe	0	0	0	0	0	0	388	0	0	0	0	0	0
Nitroglycerine	0	0	18	0	0	0	0	335	4	0	0	61	0
Nylon	0	0	2	2	13	4	0	1	300	0	0	3	0
PAN	45	0	0	0	0	5	0	0	0	349	0	0	4
Pb	0	0	0	0	0	0	0	0	0	0	398	0	0
PETN	0	0	18	1	4	0	0	60	7	0	0	297	0
Polyethylene_nist	0	0	0	0	0	19	0	0	0	1	0	0	373

Figure 6 Confusion matrix showing the CNN model's performance in classifying materials. Rows represent the actual material classes, and columns represent the predicted classes.

To evaluate the model's capability in distinguishing between explosive and non-explosive materials, the metrics were grouped accordingly (Table 2).

TABLE NO. 2

Summarized Confusion Matrix

Category/Prediction	Explosive	Non_Explosive
Explosive	1371	28
Non_Explosive	11	3289

By aggregating all classification results for explosive and non-explosive materials, the system's performance can be evaluated using sensitivity, a metric derived from the confusion matrix that measures the ability to correctly identify positive cases.

- Sensitivity for detecting explosives: 0.98, meaning the system accurately identifies 98% of actual explosives, with only 2% of explosives misclassified as non-explosive materials.
- Sensitivity for detecting non-explosives: 0.99, indicating that 99% of benign materials are correctly classified, with only 1% incorrectly flagged as explosives.

These results highlight the model's effectiveness in detecting explosives while maintaining a high level of sensitivity for non-explosive materials. The slight imbalance in performance metrics between the two categories may be attributed to variations in the gamma spectra patterns and overlapping spectral features among certain materials.
The confusion matrix revealed that misclassifications predominantly occurred among materials with similar elemental compositions. These overlaps can be attributed to the inherent limitations of the detector's energy range and resolution, which constrain the availability of distinct spectral features. Despite these challenges, the CNN successfully leveraged subtle spectral patterns to achieve high classification accuracy.

Discussion

This study highlights the potential for low-energy NaI detectors to be employed in explosive detection through advanced computational methods. By leveraging a 3-inch NaI detector and advanced CNN algorithms, the approach demonstrated robust performance despite the detector's energy limitations. The high overall sensitivity of 0.98 for explosives underscores the reliability of this method in accurately identifying explosive materials. The use of Geant4 simulations enabled detailed modelling of neutron interactions and gamma spectra, providing a solid foundation for training and validating the CNN.

One significant finding is the ability of the CNN to compensate for the lack of high-energy gamma photopeaks by recognizing subtle patterns in the lower-energy spectrum. This demonstrates the potential for machine learning to overcome hardware limitations, offering a cost-effective solution for explosive detection. However, the reliance on simulated data necessitates future work involving real-world experiments to validate these findings. Additionally, while the model's performance in detecting non-explosives was strong, slight variations in precision suggest the need for further optimization of the network's architecture and training process.

Future research should focus on expanding the range of tested materials, incorporating real-world noise conditions, and refining machine learning techniques to enhance robustness and generalizability. Furthermore, exploring the integration of this method with complementary detection technologies could provide a comprehensive solution for security applications.

Conclusion

Detecting explosives with a NaI detector limited to 3 MeV is not only feasible but also highly reliable when combined with machine learning techniques. Despite the detector's inherent limitations in capturing high-energy gamma-ray emissions, the

integration of deep learning algorithms, particularly convolutional neural networks (CNNs), enables the accurate classification of explosive materials by analysing the lower-energy gamma spectrum. The achieved overall sensitivity of 0.98 for explosives detection underscores the effectiveness of this approach, making it a promising solution for security screening, border control, and landmine detection.

This method offers a cost-effective alternative to traditional high-energy detectors like high-purity germanium (HPGe) systems, which, while highly precise, are expensive, require cryogenic cooling, and are impractical for large-scale deployment in field applications. By leveraging advanced computational models, this approach compensates for the hardware constraints of NaI detectors, proving that machine learning can bridge the gap between cost and performance.

Moving forward, future research should focus on validating these findings with experimental data, optimizing model robustness under real-world conditions, and expanding the system's applicability to diverse environments, including dynamic security checkpoints, cargo screening facilities, and field-based demining operations. Enhancing the model's adaptability to various background radiation levels and material compositions will further increase its reliability and expand its practical deployment potential.

References

Gulli, A., and S. Pal. 2017. *Deep learning with Keras.* Packt Publishing Ltd.

IAEA. 2012. "NEUTRON GENERATORS FOR ANALYTICAL PURPOSES."

Lou, Tak Pui. 2003. *Compact D-D/D-T Neutron Generators and Their Applications.* UNIVERSITY OF CALIFORNIA, BERKELEY.

Nunes, W.V., A.X. da Silva, V.R. Crispim, and R. Schirru. 2002. "Explosives detection using prompt-gamma neutron activation and neural networks." *Applied Radiation and Isotopes* 56: 937-943.

S. Agostinelli, S, J Allison, K Amako, J Apostolakis, H Araujo, P Arce, M Asai, et al. 2003. "Geant4—a simulation toolkit." *Nuclear Instruments and Methods A* 506: 250-303. doi:10.1016/S0168-9002(03)01368-8.

Whetstone, Z.D., and K.J. Kearfott. 2014. "A review of conventional explosives detection using active neutron interrogation." *Radioanalytical and Nuclear Chemistry* 301: 629-639. doi:10.1007/s10967-014-3260-5.

Zehtabvar, Mehrnaz, Kazem Taghandiki, Nahid Madani, Dariush Sardari, and Bashir Bashiri. 2024. "A Review on the Application of Machine Learning in Gamma Spectroscopy: Challenges and Opportunities." *Spectroscopy Journal* 2: 123-144. doi:10.3390/spectroscj2030008.

Funding Information
The author declares that no funding or financial support was received from any organization, institution, or individual for the research, design, execution, or writing of this work.

Conflict of Interest
The author declares no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Data Availability
The data that support the findings of this study are openly available in the Open Science Framework at https://osf.io/wh8n4

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Analysis of the impact of urban security policies on lone wolf terrorism threats in the European Union

Aris SARJITO*

*Republic of Indonesia Defense University
e-mail: arissarjito@gmail.com

Abstract

This paper examines the effectiveness of urban security policies in countering lone-wolf terrorism threats within the European Union. The research evaluates the implementation and impact of preventive security strategies in major European cities, particularly in response to individual terrorist attacks over the past decade. The study aims to assess how urban security frameworks have adapted to the increasing phenomenon of radicalized individuals acting independently. The analysis is based on case studies from Western European countries, such as France, Germany, and the United Kingdom. It considers policy measures including surveillance systems, counter-radicalization programs, and rapid response units. The findings highlight both the strengths and vulnerabilities of the current urban security structure in mitigating lone-wolf terrorism.

Keywords:
counter-terrorism; European Union; lone wolf terrorism; public safety; radicalization; urban security.

Article info
Received: 15 February 2025; Revised: 3 March 2025; Accepted: 10 March 2025; Available online: 2 April 2025

Citation: Sarjito, A. 2025. "Analysis of the impact of urban security policies on lone wolf terrorism threats in the European Union." *Bulletin of "Carol I" National Defence University*, 14(1): 19-33. https://doi.org/10.53477/2284-9378-25-02

Introduction

The rise of lone-wolf terrorism has posed unique challenges to urban security systems across the European Union. These isolated attackers often evade traditional intelligence networks, exploiting the vulnerabilities of densely populated cities. This paper aims to evaluate the effectiveness of urban security policies in addressing these emerging threats. The research focuses on analysing security strategies implemented in key European cities that have experienced such attacks.

1. Conceptual Framework and Literature Review

1.1. *Defining Lone Wolf Terrorism*

Characteristics and patterns of lone wolf attacks

Lone wolf terrorism involves individuals carrying out violent attacks independently, without direct support from a terrorist group, though they are often inspired by extremist ideologies found online. These attackers frequently struggle with social isolation, mental health issues, or personal grievances, which make them vulnerable to radical content, particularly through social media. (Danzell and Maisonet Montañez 2016; Phillips 2017).

In recent years, lone wolves have shifted towards using simple but deadly methods like vehicle ramming and knife attacks, as seen in the 2016 Nice truck attack and the 2017 London Bridge stabbings. These quick, low-planning assaults often target crowded public spaces, making them difficult to prevent. Authorities try to detect warning signs—like online threats or extremist posts—but distinguishing real danger from online rhetoric remains a major challenge (Spaaij and Hamm 2015; McCauley and Moskalenko 2014).

Distinction from organized terrorist networks

Lone wolf terrorists differ from members of organized groups primarily in their independence—they plan and carry out attacks alone, without support from larger networks. In contrast, groups like Al-Qaeda rely on hierarchy, collective planning, and resources to coordinate large-scale attacks, such as the 2015 Paris attacks and the 2005 London bombings, which are often intercepted through surveillance due to their complexity (Spaaij and Hamm 2015; Kaplan, Lööw, and Malkki 2017).

However, lone actors are often ideologically linked to global extremist movements, drawing inspiration and attack methods from online propaganda by groups like ISIS or far-right networks. While their attacks tend to be smaller, their unpredictability creates widespread fear, making it harder for security agencies to detect and assess (McCauley and Moskalenko 2014; Phillips 2017).

1.2. *Urban Security Policies in the European Union*

Key policy frameworks and national approaches to counterterrorism

The European Union's counterterrorism landscape has evolved significantly over the past decade in response to a series of high-profile attacks, particularly in

Paris (2015) and Brussels (2016). The cornerstone of the EU's approach is the EU Counter-Terrorism Strategy, first adopted in 2005 and revised continuously to address emerging threats. It is built on four pillars: Prevent, Protect, Pursue, and Respond (Council of the European Union 2015). This framework emphasizes the prevention of radicalization, the protection of critical infrastructure, the pursuit of terrorists through legal and operational cooperation, and effective crisis response mechanisms. Recent evaluations highlight improved cross-border cooperation; however, discrepancies in national implementation remain a significant challenge (AMMTC 2018).

Complementing this is the Urban Security Action Plan, which underscores the importance of safeguarding densely populated urban areas. This plan promotes the deployment of advanced surveillance technologies, reinforced law enforcement presence, and community engagement to enhance threat detection capabilities (Cavallini 2021). Real-time data analysis, including the use of AI-powered CCTV systems and social media monitoring, is increasingly employed to monitor potential threats in urban environments (Cadet et al. 2024).

Nevertheless, concerns persist regarding the balance between security and civil liberties. Critics argue that some surveillance-driven policies disproportionately target marginalized communities, fueling distrust and reducing cooperation with law enforcement agencies (RHFV Media 2024).

National Approaches: France's Vigipirate, UK's CONTEST, Germany's Prevention Strategies

France's Vigipirate Plan

France's Vigipirate Plan is a comprehensive national security framework introduced in 1995 and regularly updated, notably after the Charlie Hebdo attacks in 2015. It is designed to maintain high-level preparedness by integrating military patrols, police surveillance, and public awareness campaigns (Yalçınkaya et al. 2022). Following the 2015 attacks, Operation Sentinelle was launched, deploying soldiers to secure public spaces and sensitive sites such as transport hubs, religious buildings, and tourist attractions (Ginkel et al. 2016).

While the presence of military personnel has provided citizens with a sense of security, its effectiveness in deterring attacks is debated. Research suggests that attackers increasingly opt for low-tech methods (e.g., knife attacks, vehicle ramming), which are difficult to prevent through visible patrols alone (Kellner 2017). Furthermore, concerns have been raised about the long-term normalization of militarization in public spaces and its potential to infringe upon citizens' freedoms (Gebrewahd 2019).

UK's CONTEST Strategy

The United Kingdom's CONTEST Strategy, first introduced in 2003 and updated in 2018, is another notable model. It aligns closely with the EU framework, emphasizing Prevent, Pursue, Protect, and Prepare as key pillars (Home Office 2018). The Prevent component is particularly prominent and controversial, focusing

on identifying individuals at risk of radicalization through collaboration between schools, healthcare institutions, and local authorities (Pearson, Winterbotham, and Brown 2021).

While the UK government has lauded Prevent as instrumental in disrupting extremist networks, critics argue it fosters discrimination against Muslim communities and undermines trust in public services (Home Office 2024). Some practitioners have also expressed concerns about the program's impact on free speech, as individuals may avoid discussing political or religious views due to fear of being flagged as extremists (Pearson, Winterbotham, and Brown 2021).

Germany's Prevention Strategies

Germany adopts a preventive and de-radicalization-focused strategy, further strengthened after the 2016 Berlin Christmas market attack. This approach prioritizes early intervention, community resilience, and the reintegration of individuals disengaging from extremist ideologies (Koehler 2021). Programs such as Live Democracy! facilitate partnerships between the state and civil society organizations, fostering grassroots solutions to extremism (Tamang and Professor 2024).

This bottom-up approach is often praised for emphasizing social cohesion and long-term prevention. However, bureaucratic hurdles and inconsistent funding have hindered the program's agility, limiting its effectiveness in addressing rapidly developing threats (Bury 2024). Critics also point out that Germany's approach can sometimes appear overly cautious, lacking the robust enforcement measures seen in France and the UK (Afshcarian and Seeleib-Kaiser 2025).

Cross-national Evaluation and Common Weaknesses

While each European country adapts its counterterrorism approach to its specific security landscape and political culture, they face common challenges: detecting lone actors who evade traditional surveillance designed for organized groups (Shepherd 2021), overcoming delays in intelligence sharing due to institutional fragmentation between agencies (Ginkel et al. 2016), and balancing robust security measures with civil liberties to prevent alienating minority communities (Mathews and McNeil-Willson 2021). Looking ahead, experts suggest that Europe's future counterterrorism strategy will likely combine technology-driven surveillance with community-based prevention to address increasingly complex threats (Bury 2024).

1.3. *Surveillance, Intelligence, and Early Detection*

Surveillance technologies like CCTV, facial recognition, and AI-powered threat detection have become central to counterterrorism in Europe, especially in busy urban spaces. Cities like London and Paris now use systems that analyse behaviour in real-time, spotting potential threats like unattended bags or suspicious movements. Facial recognition helps identify suspects in crowds, while AI scans data for patterns like unusual purchases, but these tools still produce false positives and often misidentify minorities, raising concerns about bias (Asaka and Denham 2023; Singer 2024).

Despite these advances, detecting self-radicalized lone actors remains difficult. These individuals often radicalize privately through online content and show few outward signs, unlike members of organized groups. Surveillance excels at tracking actions but struggles to identify intent—someone buying knives may be a chef, not an attacker. Privacy laws like GDPR also limit online monitoring, and lone actors can radicalize and strike quickly, leaving security services playing catch-up (Kaplan, Lööw, and Malkki 2017; Duncan 2020).

Experts argue that technology alone is not enough; human intelligence and community engagement are still crucial. Family, friends, or neighbours often notice concerning behaviour before authorities do. Combining AI-powered surveillance with trained behavioural assessment teams could improve threat detection, ensuring technology is guided by human judgment to reduce false alarms and better identify genuine risks (Duncan 2020; Park and Pak 2018).

2. Methodology

2.1. *Qualitative Approach*

This study adopts a qualitative research approach using a multiple-case study design. Paris, Berlin, and London were selected as the primary case studies due to their experiences with high-profile terrorist attacks between 2015 and 2017, their significance as political and economic hubs in Europe, and their diverse security responses. This comparative approach enables an evaluation of how different national security frameworks adapt to lone-wolf terrorism threats in densely populated urban settings.

The cases were chosen to reflect varying approaches:

- Paris: Militarized deterrence with the Vigipirate Plan and Operation Sentinelle.
- Berlin: Physical barriers and surveillance upgrades following vehicle ramming.
- London: Community-focused prevention alongside rapid response and intelligence integration.

These cities also exemplify the broader European Union's struggle to balance urban security, public freedoms, and multicultural integration.

2.2. *Data Collection and Analysis*

The research relies on a systematic review of diverse sources to ensure a comprehensive understanding of urban security policies and their effectiveness in addressing lone-wolf terrorist threats:

- **Primary Sources:** National security policies were analysed, including France's Vigipirate Plan (French Government 2017), the UK's CONTEST Strategy (Home Office 2018), and Germany's Prevention Programs (Federal Office for the Protection of the Constitution 2022). European Union-level

policies such as the Schengen Information System (SIS) updates (European Commission 2023) and the Passenger Name Record (PNR) directive (Council of the European Union 2015) were also examined.

- **Institutional Reports:** Europol's *Terrorism Situation and Trend Reports (TE-SAT)* from 2015 to 2024 provided key insights into terrorism patterns and counterterrorism responses across the European Union (Europol 2017; 2023). National security assessments, such as reports by the German Federal Office for the Protection of the Constitution (BfV) (Federal Office for the Protection of the Constitution 2022), further informed the evaluation of security measures.
- **Academic Literature:** Peer-reviewed studies published between 2015 and 2024 were reviewed, focusing on topics such as urban security policies, lone-wolf terrorism, and surveillance technologies. Key works included research on lone-wolf radicalization (Spaaij and Hamm 2015; McCauley and Moskalenko 2014), European counterterrorism strategies (Mathews and McNeil-Willson 2021; Kaunert and Léonard 2020), and the impact of surveillance systems (Coaffee 2021; Blackbourn and Walker 2023).
- **Media Coverage:** Verified news reports were consulted to contextualize the Paris, Berlin, and London attacks and the subsequent policy adjustments. These accounts supplemented official and academic sources, offering real-time details and public reactions to security interventions (Harris 2017; Dearden 2023).

Triangulating these diverse sources—combining official documents, academic analysis, and media reports—allowed for a robust evaluation of both the effectiveness of urban security policies and their broader societal implications.

3. Case Studies: Responses to Lone Wolf Attacks

3.1. *Paris: Vigipirate and Military Patrols*

Visible deterrence, such as uniformed patrols and military deployments, has become a common security measure in European cities after the 2015-2017 attacks. France's *Operation Sentinelle* stationed 10,000 soldiers in public spaces, aiming to reassure citizens and discourage attackers, while armed patrols in the UK and Germany enabled rapid responses during incidents like the 2017 London Bridge attack and the 2016 Berlin truck attack (Samaan and Jacobs 2020; Hufnagel 2020). These measures improved public confidence and reduced casualties in fast-moving attacks but also raised concerns about officer fatigue and the long-term impact on civil life (von Braunschweig 2022).

However, visible patrols struggle to prevent sudden, low-tech attacks like vehicle ramming and stabbings, often carried out by lone actors with minimal planning. Incidents in Nice (2016) and Westminster (2017) showed how attackers can bypass static security using everyday objects as weapons (Lehr 2018; Escalante 2023).

Experts now emphasize combining visible deterrence with intelligence-driven policing and community engagement, as seen in Germany's use of behaviour detection officers and the UK's updated *CONTEST* strategy, which focuses on early intervention and cooperation with local communities to prevent radicalization (Hufnagel 2020; Harris 2017).

3.2. *Berlin: Securing Public Spaces*

The 2016 Berlin Christmas market attack, where Anis Amri drove a hijacked truck into a crowded market, killing 12 and injuring 56, exposed weaknesses in Germany's border security and cooperation between federal and state agencies. It also highlighted the growing threat of vehicle-ramming attacks across Europe, prompting urgent calls for tighter urban security (Schneider 2020; Hufnagel 2020).

In response, Berlin installed permanent anti-vehicle barriers, increased police patrols, and tested facial recognition at Berlin Südkreuz station, reflecting a shift toward technology-driven security. While these measures improved safety, they also restricted public spaces, turning once-open Christmas markets and plazas into heavily monitored zones, raising concerns about over-policing and racial profiling (McIlhatton et al. 2020; Dorreboom and Barry 2022; Ciax and Runkel 2024).

Berlin's experience reflects a broader European challenge—balancing security with public freedom. While barriers and surveillance deter attacks, they risk limiting urban mobility and spontaneous public life. Experts suggest combining flexible security measures with community trust and legal safeguards to protect both safety and democratic values (Coaffee 2021; Mucha 2017).

The urban security policies adopted across Europe after major terrorist attacks reveal both shared patterns and country-specific approaches. France, Germany, and the UK implemented a mix of visible deterrence, surveillance expansion, and community engagement to prevent future attacks. While these measures improved public safety, they also sparked debates over civil liberties and the militarization of public spaces. The table below summarizes key security responses in these countries following the 2015–2017 attacks.

These policy adjustments highlight the tension between strengthening urban security and preserving democratic freedoms. While visible security measures have reassured the public and reduced response times, concerns about racial profiling, restricted mobility, and long-term impacts on community trust remain central to the ongoing evaluation of European counterterrorism strategies.

3.3. *London: Rapid Response and Intelligence Sharing*

The integration of MI5, police forces, and local councils has been central to London's counterterrorism strategy, especially after the 2005 and 2017 attacks. MI5 works closely with the Metropolitan Police's Counter Terrorism Command (SO15), sharing

TABLE NO. 1

Summary of Urban Security Responses in Europe after Terrorist Attacks (2015–2017)

Country	Key Event	Main Security Measures	Positive Impact	Challenges
France	Paris Attacks (2015)	Operation Sentinelle: 10,000 soldiers deployed in public spaces; Vigipirate Plan tightened; Anti-Terrorism Law (2017)	Increased public sense of safety; Faster response times	Militarization of public spaces; Civil liberties concerns
Germany	Berlin Christmas Market Attack (2016)	Anti-vehicle barriers; Expanded CCTV surveillance; Strengthened GTAZ (Joint Counter-Terrorism Centre)	Reduced vehicle-ramming risk; Improved monitoring	Mobility restrictions; Racial profiling concerns
United Kingdom	Westminster, London Bridge, Finsbury Park Attacks (2017)	Expanded armed police patrols; "Run, Hide, Tell" campaign; Updated CONTEST Strategy (2018)	Rapid armed police response; Improved public preparedness	Tensions with Muslim communities; Fear normalization

Source: Compiled by the author (2025).

intelligence and embedding officers within police units to speed up responses. Local councils also play a key role in the *Prevent* strategy, identifying individuals vulnerable to radicalization and working with police and social services to intervene early. However, *Prevent* has faced criticism from Muslim communities, who often feel unfairly targeted, raising concerns about trust and civil liberties (Blackbourn and Walker 2023; Qurashi 2018; Brouillette-Alarie et al. 2022).

The *"Run, Hide, Tell"* public safety campaign, launched in 2015, further strengthened the UK's terrorism preparedness by teaching civilians how to react during attacks. Widely recognized by 2018, the campaign was credited with helping people evacuate safely during the Manchester Arena bombing. The 2017 London Bridge attack highlighted the importance of pairing public awareness with rapid armed response, as police neutralized the attackers within 8 minutes, aided by intelligence coordination through the Joint Terrorism Analysis Centre (JTAC) (Home Office 2018; Dearden 2023).

4. Evaluation of Policy Effectiveness

4.1. *Successes*

Reduced large-scale terrorist plots: shifting trends in European security

Large-scale terrorist attacks like the 2015 Paris attacks and 2004 Madrid bombings

have become rarer in Europe over the past decade. This decline is largely due to better intelligence-sharing systems like the Schengen Information System (SIS) and the Joint Terrorism Analysis Centre (JTAC), the military defeat of ISIS's territorial caliphate in 2019, and proactive security work—MI5 and UK police foiled 31 plots between 2017 and 2023. AI-driven surveillance has also helped detect threats earlier. While lone actors and extremists remain a danger, complex, coordinated bombings have become far less common (Kaunert and Léonard 2020; Nesser, Stenersen, and Oftedal 2016; Dearden 2023; Husain 2021; Pearson, Winterbotham, and Brown 2021).

Enhanced public awareness and cooperation: a critical counterterrorism asset
The rise of low-tech, spontaneous terrorist attacks in Europe has made public vigilance a key part of security efforts. Governments now view citizens as first-line responders who can spot suspicious behaviour and assist with rapid interventions. Campaigns like the UK's *"Run, Hide, Tell"* and *"See it, Say it, Sorted"* have raised public awareness, while France's Vigipirate alerts and Germany's Security Partnership Initiative encourage early reporting and improve situational awareness (Blackbourn and Walker 2023; Pearce et al. 2020; Harris 2017).

Citizen reports have successfully helped prevent attacks, such as a tip-off near Westminster in 2017 and the arrest of a suspect preparing an IED in Birmingham in 2018 (Home Office 2018; Pearce et al. 2020). However, public reporting is not without issues—false alarms can drain security resources, and concerns about racial profiling have damaged trust between police and minority communities. Rural areas and non-English speakers also remain harder to reach through these campaigns (Brouillette-Alarie et al. 2022; Pearson, Winterbotham, and Brown 2021).

Experts emphasize that public vigilance works best when paired with professional security networks. The decline in large-scale attacks shows the success of this cooperation. Systems like the UK's Anti-Terrorism Hotline and France's SAIP app allow rapid information-sharing between the public and law enforcement, enabling faster, more effective responses to potential threats (Kaunert and Léonard 2020; Husain 2021).

4.2. *Shortcomings*
Low-tech terrorist attacks using vehicles, knives, and other everyday objects have emerged as the primary threat across Europe over the past decade. Incidents such as the Nice truck attack (2016), the Berlin Christmas market attack (2016), Westminster (2017), and London Bridge (2017) reveal a critical vulnerability: these rapid, low-planning assaults often bypass surveillance and physical deterrents.

Several systemic weaknesses persist despite security improvements:
Intelligence Gaps and Fragmentation
The Anis Amri case in Germany exemplifies the limitations of intelligence coordination. Although Amri was under surveillance and flagged as a security threat, legal constraints and poor information-sharing between federal and state agencies

allowed him to execute the Berlin attack. Europol's 2023 TE-SAT report highlighted continued delays in cross-border data exchange, with suspects exploiting loopholes within the Schengen zone to evade detection (Europol 2023).

Racial Profiling and Erosion of Trust

Expanded stop-and-search powers in France and the UK's Prevent program have disproportionately targeted Muslim communities. Reports from human rights organizations and scholars (Qurashi 2018; Blackbourn and Walker 2023) suggest that these measures contribute to social alienation, reducing community cooperation with law enforcement, the very cooperation that is crucial for identifying self-radicalized individuals early.

Over-reliance on Surveillance Technologies

While AI-powered CCTV and facial recognition systems in cities like London and Paris have enhanced threat detection, their effectiveness is limited against lone actors with minimal planning. These technologies also exhibit bias, leading to higher rates of misidentification among minority populations (Singer 2024). False positives divert security resources and fuel public resentment.

Militarization and Psychological Impact

Visible security, such as Operation Sentinelle in France, reassures some citizens but also creates a perception of a permanent emergency. Research by Coaffee (2021) argues that militarization can normalize fear, transforming public spaces into zones of suspicion and restricting urban life.

4.3. *Policy Recommendations for Urban Security and Lone Wolf Threats*

Strengthening Intelligence Integration

Building on Europol's current efforts, member states should develop a unified counterterrorism intelligence hub to minimize information silos. Germany's post-Amri reforms, which improved cooperation between federal and regional security bodies, offer a model. Expanding the Joint Counter-Terrorism Centre (GTAZ) concept across Europe could enhance threat assessments and ensure that data flows seamlessly across jurisdictions.

Enhancing Behavioral Risk Assessment

Beyond technological surveillance, frontline officers and community workers should be trained in behavioural threat detection. Programs such as Germany's "Live Democracy!" already emphasize this approach but require broader implementation. Behavioural risk profiling can complement CCTV analysis, identifying subtle pre-attack indicators.

Establishing Independent Oversight of Surveillance Systems

To address privacy concerns, surveillance initiatives must be subjected to rigorous oversight. Independent bodies—comprising legal experts, data scientists, and

community representatives—should review the operation of facial recognition and AI monitoring systems. Periodic audits can ensure that security measures target genuine threats without disproportionately affecting minorities.

Rebuilding Community Trust

Security cannot operate in isolation. Partnerships with local leaders, educators, and mental health professionals can foster early intervention. For instance, revising the UK's Prevent strategy to emphasize voluntary engagement rather than surveillance could repair strained relations with Muslim communities. Establishing Community Liaison Officers across European cities would strengthen dialogue between law enforcement and diverse populations.

Urban Security Design

Flexible security infrastructures such as retractable vehicle barriers and mobile police units—can safeguard public spaces without obstructing urban mobility. Berlin's experiment with temporary barriers during markets demonstrates how security can adapt to city life without permanently altering its landscape.

Conclusions

European cities have become safer in many ways, thanks to stronger security policies put in place after years of facing terrorist threats. Visible patrols, better intelligence sharing, and public safety campaigns have helped prevent attacks and reassure the public. However, lone wolf attacks, especially those using simple weapons like knives or vehicles—remain hard to predict and stop. These threats highlight that security is not just about barriers and cameras; it also depends on trust, cooperation, and strong relationships between authorities and local communities. Moving forward, keeping cities safe will require finding the right balance—protecting people without sacrificing the freedoms that make urban life thrive.

References

Asaka, Jeremiah, and Magdalena Denham. 2023. "New, Old, and Reconfigured: Exploring the U.S. Department of Homeland Security's Path to Climate Security." *Homeland Security Affairs* 19 (May):1–39. https://www.researchgate.net/publication/370837506_New_Old_and_Reconfigured_Exploring_the_US_Department_of_Homeland_Security's_Path_to_Climate_Security.

ASEAN Ministerial Meeting on Transnational Crime (AMMTC). 2018. "ASEAN Plan of Action to Prevent and Counter the Rise of Radicalisation and Violent Extremism (2018–2025)." *ASEAN Secretariat*. https://asean.org/wp-content/uploads/2021/01/Adopted-ASEAN-PoA-to-Prevent-and-Counter-PCVE-1.pdf.

Barbe, Danielle, Lori Pennington-Gray, and Ashley Schroeder. 2018. "Destinations' Response to Terrorism on Twitter." *International Journal of Tourism Cities* 4 (4): 495–512. https://doi.org/10.1108/IJTC-04-2018-0027.

Blackbourn, Jessie, and Clive Walker. 2023. "Tracking in the Interests of Counter-Terrorism." In *Tracking People*, 113–36. Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780367443597-6/tracking-interests-counter-terrorism-jessie-blackbourn-clive-walker.

Braunschweig, B. von. 2022. *The French Approach to Counterterrorism: A Normative Assessment of the Securitisation of Terrorism by France between 2015 and 2017* . [Bachelor's thesis, Leuphana University]. https://pubdata.leuphana.de/bitstream/20.500.14123/861/1/Bachelorarbeit_2022_Braunschweig_von_French.pdf.

Brouillette-Alarie, Sébastien, Ghayda Hassan, Wynnpaul Varela, Sarah Ousman, Deniz Kilinc, Éléa Laetitia Savard, Pablo Madriaza, et al. 2022. "Systematic Review on the Outcomes of Primary and Secondary Prevention Programs 117 Spring," no. 30. https://journals.sfu.ca/jd/index.php/jd/article/download/577/337/1677.

Bury, Patrick. 2024. "Post-Fordism and the Transformation of Transatlantic Counter-Terrorism." *Studies in Conflict & Terrorism* 47 (10): 1261–85. https://doi.org/10.1080/1057610X.2021.2025020.

Cadet, Emmanuel, Olajide Soji Osundare, Harrison Oke Ekpobimi, Zein Samira, and Yodit Wondaferew Weldegeorgise. 2024. "AI-Powered Threat Detection in Surveillance Systems: A Real-Time Data Processing Framework." *Open Access Research Journal of Engineering and Technology* 7 (2): 031–045. https://doi.org/10.53022/oarjet.2024.7.2.0057.

Cavallini, Simona. 2021. *Approaches and Tools to Assess and Measure Security and Safety in Urban Areas*. https://doi.org/10.5281/zenodo.5374605.

Ciax, Katharina, and Simon Runkel. 2024. "Geopolitics of Urban Squares: Atmospheric Securitisation and Counterterrorism in Everyday Urban Spaces in Berlin." *Geopolitics*, 1–24. https://doi.org/10.1080/14650045.2023.2283465.

Coaffee, Jon. 2021. *The War on Terror and the Normalisation of Urban Security*. Routledge. https://doi.org/10.4324/9780429461620.

Council of the European Union. 2015. "Proposal for a Directive of the European Parliament and of the Council on Provisional Legal Aid for Suspects or Accused Persons Deprived of Liberty and Legal Aid in European Arrest Warrant Proceedings (Document 14469/15)." https://data.consilium.europa.eu/doc/document/ST-14469-2015-INIT/en/pdf.

Danzell, Orlandrew E, and Lisandra M Maisonet Montañez. 2016. "Understanding the Lone Wolf Terror Phenomena: Assessing Current Profiles." *Behavioral Sciences of Terrorism and Political Aggression* 8 (2): 135–59. https://doi.org/10.1080/19434472.2015.1070189.

Dearden, Lizzie. 2023. *Plotters: The UK Terrorists Who Failed*. Hurst Publishers. https://www.hurstpublishers.com/.

Dorreboom, Matthew, and Kaya Barry. 2022. "Concrete, Bollards, and Fencing: Exploring the Im/Mobilities of Security at Public Events in Brisbane, Australia." *Annals of Leisure Research* 25 (1): 48–70. https://doi.org/10.1080/11745398.2020.1812411.

Duncan, Kenneth A. 2020. *Role of Intelligence in the Prevention of Terrorism (Early Warning-Early Response)*. International Centre for Counter-Terrorism (ICCT). https://www.icct.nl/.

Escalante, Edwar E. 2023. "A Self-Defense Network against Terrorism and Crime: Evidence from Peru." *Terrorism and Political Violence* 35 (4): 828–45. https://doi.org/10.1080/09546553.2021.1982704.

European Commission. 2023. "Schengen Information System (SIS)." Migration and Home Affairs. 2023. https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/schengen-information-system-sis_en.

Europol. 2017. "European Union Terrorism Situation and Trend Report (TE-SAT)." *European Union Agency for Law Enforcement Cooperation*. The Hague. https://www.europol.europa.eu/publications-events/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017.

___**.** 2023. "TE-SAT: European Union Terrorism Situation and Trend Report 2023 – Executive Summary." European Union Agency for Law Enforcement Cooperation. 2023. https://data.europa.eu/doi/10.2813/376551.

Federal Office for the Protection of the Constitution. 2022. "Brief Summary 2021 Report on the Protection of the Constitution: Facts and Trends." https://www.verfassungsschutz.de/en/public-relations/publications/annual-reports.

French Government. 2017. "Plan Vigipirate: Security Alert System." 2017. https://www.info.gouv.fr/actualite/vigipirate-a-son-niveau-urgence-attentat.

Gebrewahd, Meressa. 2019. "Ethiopia and Eritrea: National Security, Militarization and Normalization Predicaments," December. https://www.researchgate.net/publication/339940002_Ethiopia_and_Eritrea_National_Security_militarization_and_normalization_predicaments.

Ginkel, Bibi, Bérénice Boutin, Grégory Chauzal, Jessica Dorsey, Marjolein Jegerings, Christophe Paulussen, Johanna Pohl, Alastair Reed, and Sofia Zavagli. 2016. "The Foreign Fighters Phenomenon in the European Union. Profiles, Threats & Policies." *Terrorism and Counter-Terrorism Studies* 7 (April). https://doi.org/10.19165/2016.1.02.

Harris, T. 2017. "London's Preparedness to Respond to a Major Terrorist Incident." *Journal of Counter-Terrorism and Homeland Security International* 23 (4): 63–70. https://www.london.gov.uk/mopac-publications/londons-preparedness-respond-major-terrorist-incident.

Home Office. 2018. "The United Kingdom's Strategy for Countering Terrorism." https://assets.publishing.service.gov.uk/media/5b23df8f40f0b634d557b020/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf.

Hufnagel, Saskia. 2020. "Policing Flows in Counter-Terrorism: Barriers to Local and Global Law Enforcement Cooperation." In *Policing Transnational Crime*, 147–65. Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781351132275-9/policing-flows-counter-terrorism-saskia-hufnagel.

Husain, Ed. 2021. *Among the Mosques: A Journey across Muslim Britain*. Bloomsbury Publishing. https://www.bloomsbury.com/uk/among-the-mosques-9781526618672/.

Kaplan, Jeffrey, Heléne Lööw, and Leena Malkki. 2017. *Lone Wolf and Autonomous Cell Terrorism*. Routledge London and New York. https://doi.org/10.4324/9781315724263.

Kaunert, C., and S. Léonard. 2020. *The Collective Securitisation of Terrorism in the European Union. In Supranational Governance in the European Union*. https://www.taylorfrancis.com/chapters/edit/10.4324/9780367853365-3/collective-securitisation-terrorism-european-union-christian-kaunert-sarah-l%C3%A9onard.

Kellner, Anna Maria. 2017. "INTERNATIONAL POLICY ANALYSIS Democracy and Terrorism-Experiences in Coping with Terror Attacks." https://library.fes.de/pdf-files/id/ipa/13552-20171023.pdf.

Koehler, Daniel. 2021. "Deradicalisation in Germany: Preventing and Countering Violent Extremism." https://doi.org/10.24241/rcai.2021.128.2.59/en.

Lehr, Peter. 2018. *Counter-Terrorism Technologies: A Critical Assessment*. Springer. https://link.springer.com/book/10.1007/978-3-319-90924-0.

Mathews, Priya Sara, and Mathews McNeil-Willson. 2021. "Repressive Security and Civil Society in France, Post-9/11." In *Counter-Terrorism and Civil Society*, 127–42. Manchester University Press. https://doi.org/10.7765/9781526157935.

McCauley, Clark, and Sophia Moskalenko. 2014. "Toward a Profile of Lone Wolf Terrorists: What Moves an Individual From Radical Opinion to Radical Action." *Terrorism and Political Violence* 26 (1): 69–85. https://doi.org/10.1080/09546553.2014.849916.

McIlhatton, David, James Berry, David Chapman, Pernille H. Christensen, John Cuddihy, Rachel Monaghan, and Dan Range. 2020. "Protecting Crowded Places from Terrorism: An Analysis of the Current Considerations and Barriers Inhibiting the Adoption of Counterterrorism Protective Security Measures." *Studies in Conflict and Terrorism* 43 (9): 753–74. https://doi.org/10.1080/1057610X.2018.1507311.

Mucha, Witold. 2017. "Polarization, Stigmatization, Radicalization. Counterterrorism and Homeland Security in France and Germany." https://journals.sfu.ca/jd/index.php/jd/article/download/89/79.

Nesser, Petter, Anne Stenersen, and Emilie Oftedal. 2016. "Articles Jihadi Terrorism in Europe: The IS-Effect." https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/617/1409482.pdf.

Park, Paul, and Jung H. Pak. 2018. "Experts Discuss Terrorist Threats Facing Asia, and Ways Forward." Brookings Institution. 2018. https://www.brookings.edu/articles/experts-discuss-terrorist-threats-facing-asia-and-ways-forward/.

Pearce, Julia M, David Parker, Lasse Lindekilde, Noemie Bouhana, and M Brooke Rogers. 2020. "Encouraging Public Reporting of Suspicious Behaviour on Rail Networks." *Policing and Society* 30 (7): 835–53. https://doi.org/10.1080/10439463.2019.1607340.

Pearson, Elizabeth, Emily Winterbotham, and Katherine E Brown. 2021. *Countering Violent Extremism: Making Gender Matter*. Springer. https://link.springer.com/book/10.1007/978-3-030-21962-8.

Phillips, Brian J. 2017. "Deadlier in the U.S.? On Lone Wolves, Terrorist Groups, and Attack Lethality." *Terrorism and Political Violence* 29 (3): 533–49. https://doi.org/10.1080/09546553.2015.1054927.

Qurashi, Fahid. 2018. "The Prevent Strategy and the UK 'War on Terror': Embedding Infrastructures of Surveillance in Muslim Communities." *Palgrave Communications* 4 (1): 17. https://doi.org/10.1057/s41599-017-0061-9.

RHFV Media. 2024. "Balancing Civil Liberties and Security in Counterterrorism Policies." RHFV Media. May 8, 2024. https://rhfv.org/balancing-civil-liberties-counterterrorism/.

Samaan, Jean-Loup, and Andreas Jacobs. 2020. "Countering Jihadist Terrorism: A Comparative Analysis of French and German Experiences." *Terrorism and Political Violence* 32 (2): 401–15. https://doi.org/10.1080/09546553.2017.1415891.

Schneider, Steffen. 2020. "Democracy and Security in Germany before and after Reunification." In *Routledge Handbook of Democracy and Security*, 97–108. Routledge. https://doi.org/10.4324/9781315755724-7.

Shepherd, Alistair J K. 2021. "EU Counterterrorism, Collective Securitization, and the Internal-External Security Nexus." *Global Affairs* 7 (5): 733–49. https://doi.org/10.1080/23340460.2021.2001958.

Singer, Tahel. 2024. "Visual Generative AI in Warfare and Terrorism: Risk Mitigation through Technical Requirements and Regulatory Insights." https://repositum.tuwien.at/handle/20.500.12708/205245.

Spaaij, Ramón, and Mark S Hamm. 2015. "Key Issues and Research Agendas in Lone Wolf Terrorism." *Studies in Conflict & Terrorism* 38 (3): 167–78. https://doi.org/10.1080/1057610X.2014.986979.

Yalçınkaya, Haldun, Richard Warnes, Omi Hodwitz, Arabinda Acharya, Zeynep Sütalan, Jean Pascal Zanders, Stephen Harley, and Petar Marinov. 2022. *GOOD PRACTICES IN COUNTER TERRORISM Edited by Haldun Yalçınkaya COE-DAT Centre of Excellence Defence Against Terrorism Vol. 2.*

ACKNOWLEDGEMENTS

The author gratefully acknowledges the support and guidance from Republic of Indonesia Defense University, which has been instrumental in the completion of this research.

FUNDING INFORMATION

This research received no funding from any institution, organization, or individual.

CONFLICT OF INTEREST STATEMENT

The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

DATA AVAILABILITY STATEMENT

The data supporting this study are derived from publicly available sources and referenced within the article. No additional datasets were generated or analysed specifically for this research.

DECLARATION on AI use

The author confirms that AI tools, including language models such as ChatGPT, were used solely to enhance the writing process, improve readability, and assist with grammar and formatting. All intellectual content, analysis, and critical arguments are the result of the author's original work. The AI tools were not used to generate research findings or substitute independent scholarly work.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

French security management and the integrated approach to national security in the contemporary security environment

Assist. Prof. Vladan M. MIRKOVIĆ, Ph.D.*
* University in Novi Sad, Faculty of Law, Novi Sad, Serbia
e-mail: v.mirkovic@pf.uns.ac.rs

Abstract

France started major reforms in the security sector in 2008 with the White Paper, which contained the guiding principle for numerous changes which occurred from 2008 to 2022. During that period, France suffered several serious terrorist attacks and experienced crises which tested the effectiveness of the French national security system. The National Security Review presented in 2022 reiterates the determination from 2008 and describes six strategic objectives whose coordinated enforcement constitutes an integrated approach to national security. The strategic objectives pointed out in NSR 2022 encompass a plethora of intertwined and complementary military and non-military actions undertaken by numerous holders. Such a massive security system is coordinated by a wide and complex network which enables the integration of multiple actions at horizontal and vertical axes into a single activity under the authority of the President and the Prime Minister. At the same time, the strategic objectives are threatened by hybrid warfare, which is perceived as a strategy of foes (states and non-state actors) who combine military and non-military tools in order to achieve political aims at the expense of the national interests of the Republic. This research aims to test the general hypothesis that the French integrated approach presented in NSR 2022 is well adapted to the contemporary security environment and consistent with and complementary to the EU and NATO security policies while the security system of the French Republic is structured and managed in a way that ensures an integrated approach to national security. The French integrated approach, the structure of the security system and its management were described and explained in order to test the hypothesis.

Keywords:
The Fifth French Republic; the National Security Review; Integrated Approach; Security Management; Hybrid Warfare.

Article info
Received: 23 January 2025; Revised: 22 February 2025; Accepted: 25 February 2025; Available online: 2 April 2025

Citation: Mirković, V.M. 2025. "French security management and the integrated approach to national security in the contemporary security environment". *Bulletin of "Carol I" National Defence University*, 14(1): 34-51. https://doi.org/10.53477/2284-9378-25-03

France presented its National Security Review 2022 (SGDSN 2022) as the result of the strategic shift which happened after the onset of the war in Ukraine. However, it would be wrong to consider the NSR 2022 only from this perspective. The NSR 2022 represents the continuity within the wider process of restructuring the entire security architecture of the Republic, which started in 2008 with the White Paper. From 2008 to 2022, France suffered several serious terrorist attacks (Toulouse 2012, Paris 2015, Nice 2016, Strasbourg 2018) and experienced crises (Migrant crisis 2015, War in Ukraine 2022) which tested the effectiveness of its national security system. The new security architecture was put to the test under the worst circumstances, allowing the security management to identify structural problems and make improvements.

The NSR 2022 contains insight into the security environment. Furthermore, it reiterates security determinations expressed in previous strategic documents (2008, 2013) and the strategic review (2017) and identifies the national strategic objectives whose coordinated enforcement constitutes an integrated approach to national security. Hence, the scientific problems were defined through the following questions:

1. Is the French integrated approach presented in NSR 2022 adapted to the needs of the contemporary security environment and in alignment with the security policies of NATO and the EU?
2. Is the French security system structured and managed in a way that ensures an integrated approach to national security?

The subject of this research is the national security system of the French Republic. More specifically, this research aims to look into the capability of security management to ensure national security in a contemporary security environment. The general hypothesis behind this research is that the integrated approach presented in the NSR 2022 is well adapted to the needs of the contemporary security environment and aligned with the security policies of NATO and the EU. In addition, the security system of the French Republic is structured and managed in a way that ensures an integrated approach to national security. The French security system has structural elements which are responsible for the implementation of its strategic objectives in key domains of the security policy. These elements are managed, coordinated and/or assisted at every level of security management with bodies or individual posts which have adequate competence, enabling the integration of their actions at the horizontal and vertical axis into a single activity under the authority of the highest executive authorities. The scientific goals are to provide a detailed description and analysis of the French security policy, examine its strategic approach and the capability of the French security system to enforce an integrated approach with a particular focus on security management.

Integrated Approach and Countering Hybrid Warfare

Hybrid warfare, hybrid threats and hybrid strategies were presented in the NSR 2022 as threats to national security. According to Robert Walker, who first used this term, hybrid warfare is a combination of conventional and special operations which has the characteristics of both and lies in the interstices between special and conventional warfare, wherefore countering hybrid warfare depends on the existence of hybrid forces which can act in both domains (Walker 1998). However, Franck Hoffman is credited with getting this theory widely used in the security and political discourse. In a similar manner, Hoffman describes hybrid warfare as a unique combination of threats which incorporate a full range of different modes of warfare employed simultaneously and whose significance transcends a blend of regular and irregular tactics (Hoffman 2007, 2009 and 2018). This blend of conventional, unconventional and irregular tactics blurs the line between war and peace and makes the military term "hybrid warfare" and the more neutral term "hybrid threat" equally suitable for this phenomenon.

"Hybrid warfare evolved from an essentially military concept to one that potentially embraced all the instruments of state power" (Wither 2023, 7-8). It tends to exploit societal vulnerabilities and undermine order, peace, normal functioning of the institutions, and trust in the government. Wigell describes this as a *wedge strategy* whose "idea is not to confront the target overtly, but to weaken its resolve by covert means of interference calibrated to undermine its internal cohesion" (Wigell 2019, 262). Hence, Hoffman stated that resiliency is the first step in countering hybrid warfare (Hoffman, Neumeyer and Jensen 2024), whereby resilience is generally understood as "the ability of an entity to overcome adversity" (Jungwirth et al. 2023, 17). The main hurdle in achieving resiliency in case of a hybrid attack is the absence of awareness that one threat (e.g., propaganda) is coordinated with another threat (e.g., terrorism) and that both are a part of a wider action (e.g., political coup). This results in partial and isolated institutional responses or the absence of any response to a threat(s). For that reason, "it is essential that the main security tools work in a fully integrated way" (Pardini 2019, 7) in order to eliminate vulnerabilities at home and provide a coordinated response to any kind of threat that comes from inside or abroad. In the core of such, "comprehensive security thinking is functioning civil-military cooperation as well as other cross-cutting cooperation formats, in particular public-private, political-practitioner, and social science-technology" (Smith 2019, 17).

"EU has increasingly started to emphasize the notion of resilience" (Wigell, Mikkola and Juntunen 2021, 6) as an important element in developing a whole-of-society (WoS) approach to countering hybrid threats. On the Council of EU initiative, in 2016, the European Commission presented the *Joint Framework on countering hybrid threats,* which "encouraged a whole-of-society approach, with 22 areas for action, to help counter hybrid threats and foster the resilience of the EU and the Member States. It enabled a holistic approach to countering threats of a hybrid nature by

creating synergies between all relevant instruments" (European Commission 2016, 3). Hybrid Centre of Excellence was established in 2017 as a non-profit organization promoting a whole-of-government and WoS approach whose participants are EU and NATO members. In 2023, the Comprehensive Resilience Ecosystem (CORE) was developed with the aim of strengthening societal resilience through the interconnection of 13 domains (including military, diplomacy, intelligence, economy, and cyber). In these domains, actors use tools to counter hybrid activities, ensuring the protection of seven key foundations of democratic society (Jungwirth et al. 2023). "In March 2022, the Council of the EU presented the Strategic Compass for Security and Defence in which it announced the establishment of the *EU Hybrid Toolbox,* which should bring together all civilian and military instruments which are suitable for countering hybrid threats. In the Strategic Concept (NATO 2022), NATO announced the enhancement of global awareness and readiness to act across all domains and directions using military and non-military tools in a proportionate, coherent and integrated way to respond to all threats" (Mirković 2024, 98).

NSR 2022 perceives individual threats to national security as elements of adversaries' hybrid strategy which have "shown their impact on multiple theatres" (SGDSN 2022, 12) stating in its introduction that "globalized hybrid warfare" demands an approach to national security which is "consistent with and complementary to" the EU Strategic Compass and Strategic Concept. The French integrated approach to national security has its roots in White Paper 2008, which pointed the "need to define over-arching strategies integrating all the different dimension of security into a single approach" (President of the Republic 2008, 56). That was a guiding principle for numerous changes in the security sector which happened between 2008 and 2022. NSR 2022 just reiterates that determination and describes six strategic objectives whose coordinated enforcement contributes to an integrated approach to national security. These objectives reflect the idea of resiliency since they encompass a plethora of intertwined and complementary military and non-military actions, undertaken at home and abroad, in peacetime, in case of crisis or war, by numerous holders. Strategic objectives are empowered with legal obligations related to national security and defence, which are imposed on almost every executive department, making this approach truly whole-of-government.

According to the NSS 2022, intelligence services should provide a robust information foundation to support the decision-making process of the highest authorities. Moreover, they should serve as support for other executive departments. The Ministry of the Armed Forces is responsible for nuclear weapons. It also directs three intelligence services, advises and assists the civil authorities in the cases of major crises and deploys armed forces abroad in order to support the interests of the Republic. The Ministry of Foreign Affairs presents French interests at an international level and collects information within its competencies in order to inform the highest executive authorities. The Ministry of the Interior is responsible for internal security (civil protection and the protection of public law and order) along with independent

bodies responsible for cybersecurity. The ministers responsible for justice, economy, budget, health, environment, transport, energy, and industry have certain obligations according to the Defence Code (Code de la Défense) related to national security and defence. The coordination of such a massive security system is performed by a wide and complex network which enables the integration of all the mentioned actions at horizontal and vertical axis into a single activity under the authority of the highest executive authorities. In addition, the NSR 2022 insists on the "nation's involvement" and synergy between the people and the officials, making this approach a whole-of-society approach.

The Strategic Level of French Security Management

The 1958 Constitution established the Fifth French Republic as an indivisible, secular, democratic and social Republic, organized on a decentralized basis with the semi-presidential political regime. The French "semi-presidentialism (or dual executive) was based on two old traditions of personal leadership and parliamentarianism" (Appleton 2009, 3). The President ensures due respect for the Constitution, proper functioning of the public authorities, the continuity of the State and guarantees national independence, territorial integrity and due respect for Treaties (Const. Ar. 5). "Article 5 gives the President the right and the duty to intervene in the political process regardless of the composition of the parliamentary majority" (Appleton 2009, 28). "On this basis, he may invoke the extraordinary powers he holds under Article 16" (President of the Republic 2008). Furthermore, the President is the Commander in Chief of the Armed Forces (Const. Ar. 15) and presides over the higher national defence councils, committees (Const. Ar. 15) and the Council of Ministers.

These competencies of the President gave him "a certain margin of interpretation" (David 2004) which led to a presumption of the President's "reserved domain in the areas of national defence and foreign affairs. However, the Constitution is far from categorical on this issue" (Pateman and Geoffroy 2024). Under the influence of De Gaulle and direct suffrage for the post, in the early years of the Fifth Republic, the President imposed his authority as dominant. However, with the White Paper published in 2008 and the series of reform laws and decrees which were passed after 2008, the position of the Prime Minister was strengthened, especially at the expense of what was known as the 'reserved domain' of the President.

The Prime Minister is appointed by the President (Const. Ar. 8) but reports to the Parliament "for the various policies contributing to national security: defence, domestic security and civil security, economic security, foreign policy etc." (President of the Republic 2008, 244). The Prime Minister directs the actions of the Government related to national security; he/she is responsible for national defence and ensures the coordination of the defence activity of all ministerial departments. Furthermore, the Prime Minister prepares and coordinates the actions

of public authorities in the event of a major crisis (Code de la Défense, Ar. L1131-1). Moreover, the Prime Minister makes regulations and appointments to civil and military posts and if the need arises, he/she deputizes for the President as the chair of the Council of Ministers and higher councils and committees (Const. Ar. 21). On his/her proposal, the President appoints the members of the Council of Ministers. The Council of Ministers determines and conducts the policy and has at its disposal the civil services and the armed forces (Const. Ar. 20).

The President and the Prime Minister are supported by the Defence and National Security Council (the Council). The Council was established in 2009 "as a consequence of a strategy in which national strategy is federating and mobilizing objective of government action" (President of the Republic 2008, 242). It is a body at the highest level in which respectable members can address all the aspects of national security and determine priorities and directions in general or in specific domains of national security policy, creating the integrated framework for the decision-making process for the President, the Prime Minister and the Council of Ministers (Code de la Défense, Ar. R*1122-1, Ar. L1111-3). The permanent members of the Council are the President, the Prime Minister, the Minister for the Armed Forces, the Minister of the Interior, the Minister of the Economy, Finance and the Recovery, the Minister Delegate for Public Accounts and the Minister of Foreign Affairs (Code de la Défense, Ar. R*1122-2). The Council of Ministers sets the Composition of the Council.

Within the Council, there are the National Intelligence Council (NIC) and the Nuclear Armaments Council (NAC) (DNSC 2024). The NIC defines strategic directions and priorities in intelligence affairs. Its permanent members are the President, the Prime Minister, the directors of intelligence services and the National Intelligence and Counter Terrorism Coordinator. The NAC defines the strategic orientations of the nuclear deterrence program. Its permanent members are the President, the Prime Minister, the Minister for the Armed Forces, the Armed Forces Chief of Staff, the Delegate General of Armaments and the Director of the Military Applications Directorate at the Alternative Energies and Atomic Energy Commission (Code de la Défense, Ar. R*1122-6, Ar. R*1122-7, Ar. R*1122-9 and Ar. R*1122-10).

The constitutional and political positions of the President and the Prime Minister are complementary and intertwined. However, the French dual executive system produces systemic vulnerability. In situations when the President and the Prime Minister do not belong to the same political majority, a situation called cohabitation arises, and it can lead to 'reciprocal neutralization' or a blockage of the executive power. Nevertheless, the reforms made in the past decade shifted the balance of power in the domain of national security in favour of the Prime Minister and the Council of Ministers, while the President still has a personal influence in the Council, the right to decide on the use of nuclear weapons and the right to dissolve the Parliament and terminate the mandate of the Government.

The Coordinating Level of French Security Management

"The coordinating management is composed of a network of managers whose tasks are to organize, coordinate and control the enforcement of the strategic objectives in a particular administrative area" (Mirković 2024). At the coordinating level of the French security management, the post with the most competencies is the *Secretary General for Defence and National Security* (Secretary General). He "assists the Prime Minister in the exercise of his responsibilities in matters of defence and national security"; chairs and coordinates interministerial bodies; prepares interministerial regulations on national security; contributes to the adaptation of the legal framework relating to intelligence services, etc. (Code de la Défense, Ar. R*1132-3).

The Secretary General has at disposal *the Secretariat General for Defence and National Security* (SGDSN 2024). SGDSN is a robust and complex interministerial body formed in 2009, which was placed under the authority of the Prime Minister with the task to assists in designing and implementing security and defence policies (Code de la Défense, Ar. R*1132-2, D*1131-1; (SGDSN 2024). It has a complex structure with numerous duties, organizational units and attached bodies, whereby some have operational character. SGDSN is the secretariat to the Council and other higher councils and committees (e.g., the Nuclear Policy Council). It prepares the Council's meetings and later "monitors the execution of decisions taken by the Head of State and, to this end, ensures liaison with the relevant ministerial departments" (SGDSN 2024). The Secretary General, accompanied by a small group of associates, performs this SGDSN's role.

Under the authority of the General Secretary there is the *Interministerial Control Group* (GIC) which collects requests for the authorization of use of information gathering techniques from all intelligence services and submits them to the *National Commission for the Control of Intelligence Techniques* (CNCTR) for opinion and later to the Prime Minister for approval (Code de la Sécurité Intérieure, Ar. L821-1). CNCTR is an independent administrative authority created by the French Intelligence Act 2015, which represents the government's reaction to the Charlie Hebdo shooting, as an oversight authority which ensures "that the actions of the French intelligence services across the country comply with legislation" (CNCTR 2024). Furthermore, CNCTR gives opinion to the Council of Ministers whose services, other than the first circle intelligence services, may use information-gathering techniques (Code de la Sécurité Intérieure, Ar. L811-4). CNCTR comprises "two members of the National Assembly, two senators, two members of the Council of Ministers, two senior ranking judges from the Cassation Court and a technical expert specialized in electronic communications" (Mastor 2017, 718).

The National Cybersecurity Authority (ANSSI) is responsible for the enforcement of the national cybersecurity strategy. ANSSI proposes to the Prime Minister the "measures intended to respond to crises affecting the security of information

systems of public authorities and regulated operators. It coordinates Government action and animates the national ecosystem" (SGDSN). ANSSI was founded in 2009 and it is attached to the SGDSN and subordinated to the Secretary General (Décret no. 2009-834, Ar. 2). An *Ethics and Scientific Committee*, also attached to the SGDSN, is responsible for monitoring the activity of the *Vigilance and Protection Service against Foreign Digital Interference* (VIGINUM). VIGINUM is the "technical and operational service of the State responsible for monitoring and protecting against foreign digital interference" (VIGINUM 2024) on digital platforms. Other SGDSN's units and bodies are the Institute of Advanced National Defence Studies (education and science); The Directorate of State Protection and Security (crisis management and data protection); The Department for the International, Strategic and Technological Affairs; The General Administration Service and the High Commissioner for Atomic Energy.

The second most important position at the coordinating level of security management is the *National Intelligence and Counter-Terrorism Coordinator* (CNRLT Coordinator). The CNRLT Coordinator coordinates "the general activities of the intelligence services" (CNRLT Coordinator 2024) and particular intelligence coordination related to counter-terrorism. He performs its duties assisted by "the *National Coordination of Intelligence and the Counter-Terrorism Coordination* and, within it, the *National Counter-Terrorism Center*", which were formed in 2017 and "placed under the authority of the CNRLT Coordinator" (Décret no. 2017-1095). The National Intelligence Coordinator is responsible for the implementation of the national intelligence strategy and serves as the President's adviser on national intelligence matters. As a permanent member of the NIC, he provides a direct link between the President and the security services and vice versa and "transmits the instructions of the President to the ministers responsible for these services and ensures their implementation" (Premier Ministre 2018, 7).

As the National Counter-Terrorism Coordinator, he participates in the process of determining priorities related to the counter-terrorism system and, alone or through the NCTC, coordinates counter-terrorism efforts. NCTC is a task force established in 2017 that is specialised in intelligence sharing between "intelligence services, police and judicial authorities" (Nunez 2021). This unit is under the direct authority of the President, and it "has been created to ensure that the intelligence services truly cooperate" (Jarry 2017). The CNRLT Coordinator is engaged in the inspection of intelligence services, which are conducted by the *Intelligence Inspectorate* (ISR). ISR is under the direct authority of the Prime Minister, who appoints its members after consulting the CNRLT Coordinator. For each inspection, the Prime Minister determines the mandate and the composition of the team responsible for carrying out the inspection. The Secretary General of the ISR proposes the mandate and the composition to the Prime Minister after consulting the CNRLT Coordinator (Décret no. 2014-833).

The Operating Level of French Security Management

The Ministry of the Armed Forces

The Minister of Armed Forces, as the head of the Ministry, is at the operational level of security management. He is "responsible within the Government for defence policy for which he is accountable to Parliament, along with the Prime Minister" (President of the Republic 2008, 243). The Minister has at his disposal the Armed Forces (Army, Navy, Air and Space forces), the National Gendarmerie and three intelligence services. Armed Forces are subordinated to the Chief of Staff of the Armed Forces, who assists the Minister in his duties related to the use of forces and serves as the military advisor to the Government. He is responsible for the operational use of forces and ensures the command of military operations. The Chief of Staff has the authority over the Chiefs of Staff of the Army, Navy, and Air and Space Forces who prepare units for operational use (Code de la Défense, Ar. R*3121-1 and Ar. R*3121-3). The National Gendarmerie is an autonomous armed force, and its General Director in military competences of the Gendarmeries is subordinated to the Minister of Armed Forces.

In case of an interruption of the regular functioning of public authorities which leads to the simultaneous vacancy of the Presidency, the Presidency of the Senate and the functions of Prime Minister, the responsibility and powers of defence are automatically and successively devolved to the Minister of Armed Forces and, should that fail, to the other ministers in the order indicated by the decree establishing the composition of the Government (Code de la Défense, Ar. L1131-4).

The territorial organization of national defence is based on Defence and Security Zones (DSZ), which serve as a framework for civil and military defence coordination (Code de la Défense, Ar. R*1211-1), which enables its integration. All Departments as administrative districts of the Republic are organized into six DSZs along with the Paris DSZ (Ministere des Armées 2024). The DSZ are also established for overseas territories (Code de la Défense, Articles from R*1211-1 to D1212-16). The Prefect of the DSZ is the prefect of the Department where the capital of the DSZ is located. He/she is a delegate of the Minister and serves as a civilian authority that is responsible for the organization and coordination of all non-military tasks and missions related to defence and civil protection. Each DSZ also has a General Officer who exercises the responsibilities of a military advisor to the Prefect of the DSZ and coordinates military efforts in the DSZ. The General Officer is placed under the direct authority of the Chief of Staff, and in case of an armed attack, by the decision of the Prime Minister, he becomes the supreme commander (operational commander) of either the entire DSZ or part of it. The General Officer has a military representative in each Department who serves as a military advisor to the prefect of the Department for the exercise of his/her defence responsibilities. The National Gendarmerie has its own territorial organization. However, its commanders in their respective regions assist the Prefect of the DSZ and departmental prefects in all matters concerning the

civil defence missions. Furthermore, the Gendarmerie provides a specialized unit (Nuclear Weapons Security Gendarmerie) for ensuring governmental control over nuclear weapons.

The Ministry of the Interior

The Minister of the Interior, as the head of the Ministry of the Interior, is at the operational level of security management. The Ministry of the Interior "is responsible for preparing and implementing internal security and civil security policies that contribute to national defence and security and, as such, is responsible for public order, the protection of people and property, and the safeguarding of installations and resources of general interest within the territory of the Republic" (Code de la Défense, Ar. L1142-2; Code de la Sécurité Intérieure, Ar. L111-1). The Minister has available joined units, such as the intelligence service (DGSI), which is directly subordinated to the Minister, and organizational units of the Ministry such as the Secretariat General, the National Police, the National Gendarmerie and the Prefecture of Police.

The Secretariat-General is headed by the Secretary General – Senior Defence Official, who is the first assistant of the Minister in managing the Ministry. He is the general manager who coordinates and leads the action of all services, except for those falling under the management of the National Police and the National Gendarmerie. He/she is in charge of the protection of national defence secrets and ensures the security of information systems (Décret n. 2013-728, Ar. 3). The National Police is responsible for police missions and tasks which are prescribed in the Code de la Sécurité Intérieure, Ar. R411-2. It is headed by the General Director, who is directly subordinate to the Minister. In performing police duties, the National Gendarmerie is under the authority of the Minister of the Interior. As a police service, it is supposed to ensure public safety and order in rural and peri-urban areas. It contributes to the intelligence mission of public authorities, the fight against terrorism, and the protection of the population and it also performs the duties of the judicial police (Code de la Sécurité Intérieure, Ar. L421-1). The Command of the Ministry of the Interior in Cyberspace as a service with national jurisdiction is attached to the Director General of the National Gendarmerie (Décret n. 2013-728, Ar. 7).

The Prefecture of Police, headed by the Prefect of Police, is formed under the authority of the Minister for the territory of Paris and three more departments. The President, on the proposal of the Prime Minister and the Minister for the Interior, appoints prefects as the State's representatives in the Departments (Décret n. 2022-491, Ar. 1). The Prefect of Police and departmental Prefects lead and coordinate the entire internal security system in the Prefecture/Department. Furthermore, the Prefect of Police is responsible for the security of the three airports in Paris and performs the function of the Prefect of the Paris DSZ (Code de la Sécurité Intérieure, Ar. L121-1 and Ar. L122-5). The mayors, within their competences, may entrust the municipal police officers with duties in matters of prevention and monitoring of

good order, tranquillity, security and public health (Code de la Sécurité Intérieure, Ar. L511-1).

Other departments with responsibilities in defence matters

National security and defence are considered to be an intergovernmental effort, with the Minister of the Armed Forces and the Minister of the Interior as leading powers at the operational level. Nevertheless, the Code de la Défense prescribed the obligations for other ministers in terms of preparation and execution of national defence and security measures. The Minister in charge of the economy takes the measures which guarantee the continuity of economic activity in the event of a major crisis and ensures the protection of the economic interests of the Republic. The Minister responsible for the budget manages and coordinates services which perform customs control, providing constant revenues to the budget. The Minister of Foreign Affairs, both individually and through the network of diplomatic services, presents the priorities of the security and defence policy at the European and international level, secures allies and partners and leads defence and security cooperation. The Minister of Justice ensures the continuity of judicial affairs and international judicial assistance, especially in cases of criminal offences against the fundamental interests of the Republic. The Minister of Health is responsible for the resilient health system, the protection of the population against health threats, as well as the care for victims. The ministers in charge of the environment, transport, energy and industry are each responsible within their competences for controlling natural and technological risks, transport, energy production and supplies, and infrastructure, meeting the needs of defence and national security and, in all circumstances, ensuring the continuity of services (Code de la Défense, Ar. L1131-1; L1142-3; L1142-4; L1142-6; L1142-7).

The first circle of French intelligence services

Intelligence activities are performed by the intelligence services, which act under the authority of the Government and in accordance with the guidelines determined by the NIC (Code de la Sécurité Intérieure, Ar. L811-2). Six intelligence services represent the first circle of the French intelligence and together with the CNRLT Coordinator and the Intelligence Academy they constitute the French intelligence community (Code de la Défense, Ar. R*1122-8). These services are subordinated to the ministers of the respective executive departments, while the CNRLT Coordinator is responsible for their coordination, having the same function as the director of intelligence community in the US.

The Directorate–General for External Security (DGSE) was established in 1982 and attached to the Minister of the Armed Forces. Its internal organization was set by the Order from 12 July 2022. Its core mission is the collection of information related to national security abroad in order to inform the highest executive authorities. It is under the control of the Director – General who defines the strategy of the DGSE which is in line with the guidelines of the NIC and the instructions he/she receives from the President, the Prime Minister, the Ministry of the Armed Forces

and some other members of the Government (DGSE 2024). *The Military Intelligence Directorate* (DRM) is established within the Ministry of the Armed Forces in order to meet intelligence needs of the Chief of Staff and other authorities, agencies and commands of the Ministry as well as the needs of the other relevant government authorities and agencies (Décret no. 92-523, Ar. 1-2). DRM functionally coordinates the intelligence resources of the Army, Navy, and Air and Space Forces (Ministere des Armées 2024). Its internal organization was set by the Order from 30 March 2021. *The Directorate of Intelligence and Defence Security* (DRSD) is a counterintelligence agency established in 2016 which was "placed at the disposal of the Minister of the Armed Forces to exercise his/her responsibilities for the security of the personnel, information, equipment and sensitive sites" (Code de la Défense, Ar. D3126). It acts home and abroad in order to protect the forces (force counter-intelligence), the defence industry (economic counter-intelligence) and cybersecurity from any kind of hostile interference (Ministere des Armées 2024).

The Directorate–General for Internal Security (DGSI) was established in 2014 by Décret No. 2014-445 as an active unit of the National Police under the authority of the Minister (DGSI 2024). It is an intelligence service with general competencies which performs its missions on the territory of the Republic. "The DGSI's missions consist of combating all activities that could constitute an attack on the fundamental interests of the Republic. It is responsible for preventing and suppressing activities inspired, initiated or supported by foreign powers or organizations and likely to threaten the security of the Republic" (Premier Ministre 2018, 15). The Counter-Terrorism Coordination Unit, which ensured the counter-terrorism collaboration of all services and police units, became in 2009 a department inside the DGSI (Olech 2022, 72). The DGSI also exercises judicial police tasks under the conditions laid down in Article 15-1 of the Code of Criminal Procedure (Décret No. 2014-445).

The Financial Intelligence Service (Tracfin) was established by the Décret in 1990 as a coordination unit of the General Directorate of Costumes and Indirect Taxes (DGDDI) which is "responsible for processing intelligence and taking action against clandestine financial circuits" (Décret 1990, Ar. 1). Through time, Tracfin has become an independent financial-intelligence unit headed by the Director and attached to the Minister of Finance (Code Monétaire et Financier, Ar. D561-33) with primary obligations related to the fight against money laundering and the financing of terrorism (Code Monétaire et Financier, Titre VI, Chapitre Ier). *The National Directorate of Intelligence and Customs Investigations* (DNRED) is the only intelligence service established by the minister's Order. It is a national authority attached to the DGDDI within the Ministry of Finance (Arrêté du 29 octobre 2007, Ar. 1). "The DNRED implements the DGDDI's policy of intelligence, controls and the fight against major customs fraud. The investigations carried out and the files produced in these areas constitute important sources of intelligence, some of which can be opportunely used in the fight against terrorism and radicalization" (Premier Ministre 2018, 21). It operates through the network of internal organizational units,

departments across the Republic and French customs attachés whose expertise covers nearly 60 countries.

Operational management in the cyber domain

Security in the cyber domain was highlighted in the NSR 2022 as an important aspect of national security. Except for the organizational units in the ministries and intelligence services, there are bodies at the operational level which are responsible for general or specific aspects of cybersecurity. ANSSI is a national cybersecurity authority which performs its mission through sub-directorates for operations, expertise, strategy, and administration. One part of the Sub-Directorate for Operations is CSIRT-FR as a technical and operational body which deals with cyber incidents, manages and coordinates all of the sub-directorate's activities related to cyber incidents and defines the CERT-FR development strategy. VIGINUM was established by the Décret No. 2021-922 and attached to SGDSN in order to provide the Secretary-General with powers "enabling him to identify foreign digital interference operations on digital platforms which are likely to harm the fundamental interests of the Republic, to analyse their effects and to lead and coordinate at the interministerial level the protection of the State against such operations" (Décret No. 2021-922). In other words, VIGINUM is established in order to suppress psychological-propaganda activities on the Internet. The head of the VIGINUM is appointed by the decree of the Prime Minister on the proposal of the Secretary-General (Décret No. 2021-922, Ar. 4). *Classified Interministerial Information Systems Operator* was established by Décret no. 2020-445 and attached to SGDSN. "Its main mission is to develop and deploy in an optimal manner, in all places and at all times, the classified means of communication necessary for the President of the Republic and the Government, as well as between the President of the Republic and foreign heads of state or government" (SGDSN).

Conclusion

France started major reforms in the security sector in 2008 with the White Paper, which paved the way for a comprehensive and integrated approach to security which meets the requirements of the rule of law on one hand and the demands of the contemporary security environment on the other. The NSR 2022 reiterates strategic determinations expressed in previous strategic documents and identifies the national strategic objectives which should be achieved through an integrated approach to national security. In the introduction of the NSR 2022, the President identified "globalized hybrid warfare" as a major security challenge to freedom and emphasized the need for a national approach that is consistent with and complementary to the EU and NATO security policies. Both the EU and NATO announced readiness to act across all domains and directions using military and non-military tools in a proportionate, coherent and integrated way to counter hybrid warfare as a wedge strategy whose idea is to weaken and undermine the internal cohesion of the society.

This is the reason why resiliency should be the first step in countering hybrid warfare, and it is also why the main security tools must work in a fully integrated way in order to eliminate vulnerabilities at home and provide a coordinated answer to any kind of threat that comes from inside or abroad.

The French integrated approach presented in the NSR 2022 has its roots in White Paper 2008 which pointed out the need for the integration of all the different dimensions of security into a single approach. NSR 2022 describes six strategic objectives whose coordinated enforcement contributes to an integrated approach to national security. These objectives reflect the idea of resiliency because their achievement encompasses a plethora of intertwined and complementary military and non-military actions, at home and abroad, in peacetime, in case of crisis or war, by numerous holders. Strategic objectives are strengthened by legal obligations related to national security, which are imposed on almost every executive department, making this approach truly whole-of-government. In addition, the NSR 2022 insists on the nation's involvement and the synergy between the people and the officials, making this approach a whole-of-society approach. The results of the research confirmed that the French integrated approach presented in NSR 2022 is well adapted to the needs of the contemporary security environment and is in alignment with the security policies of NATO and the EU.

In the second part of the research, the French security system was analysed in order to provide an answer to the question of whether it is structured and managed in a way that ensures an integrated approach to national security. The national security and defence policy of the Republic is determined at the strategic level. The Council determines the priorities and directions in general while NIC and NAC do so in specific domains of the national security policy, creating a framework for the decision-making process for the President, the Prime Minister and the Council of Ministers. The implementation of strategic objectives and tasks is performed by intelligence services, the Ministry of the Armed Forces, the Ministry of Foreign Affairs, the Ministry of the Interior and ministries responsible for justice, economy, budget, health, environment, transport, energy and industry which have obligations related to national security and defence in accordance with the Code de la Défense.

The coordination of such a massive security system is performed by a wide and complex network which enables the integration of all of the mentioned actions at horizontal and vertical axis into a single activity under the authority of the President and the Prime Minister. At the coordinating level, the entities with the most competences are the Secretary General, as a general coordinator because he assists the Prime Minister in the exercise of his responsibilities in matters of defence and national security, and the CNRLT Coordinator who has a special coordination function due to which he performs his coordination function only in intelligence and counter-terrorism matters and also serves as the President's advisor in these matters. Based on the research results, it was concluded that the security system of the French

Republic is structured and managed in a way that ensures an integrated approach to national security. Thus, the general hypothesis of the research was confirmed.

Conflict of Interest Statement

The author declares no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Appleton, Andrew M. 2009. "France the Unexceptional." In *The French Fifth Republic at Fifty: Beyond Stereotypes*, by Sylvain Brouard, Andrew M. Appleton and Amy Gale Mazur, 1-22. London: Palgrave Macmillan.

CNCTR. 2024. *National Commission for the Control of Intelligence Techniques.* https://www.cnctr.fr/en.

CNRLT Coordinator. 2024. *National Intelligence and Counter-Terrorism Coordination.* https://www.elysee.fr/en/national-intelligence-and-counter-terrorism-coordination.

David, Franck. 2004. "Le Président de la République, garant de la cohésion sociale." *Revue française de droit constitutionnel* pp. 533-566. www.cairn.info/revue-francaise-de-droit-constitutionnel-2004-3-page-533.htm.

DGSE. 2024. *The Directorate – General for External Security.* https://www.dgse.gouv.fr/en/get-to-know-us/who-are-we.

DGSI. 2024. *10 ans de la Direction Générale de la Sécurité Intérieure.* https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/directrice-generale.

DNSC. 2024. *Defence and National Security Council.* https://www.elysee.fr/en/french-presidency/defence-and-national-security-council.

European Commission. 2016. *Joint Communication – Joint Framework on Countering Hybrid Threats JOIN (2016) 18 final.* Brussels: European Union.

Hoffman, Frank G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington: Potomac Institute for Policy Studies. https://apps.dtic.mil/sti/pdfs/ADA496471.pdf.

___. 2009. "Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict." *Strategic Forum* no. 240: 1-8.

___. 2018. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges." *PRISM* Volume 7 (no. 4): 30-47. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1983462/.

Hoffman, Frank G., Matt Neumeyer, and Benjamin Jensen. 2024. "The Future of Hybrid Warfare." *Center for Strategic and International Studies.* https://www.csis.org/analysis/future-hybrid-warfare.

Jarry, Emmanuel. 2017. "France creates new counter-terrorism task force, Notre Dame attacker identified." *Reuters.* https://www.reuters.com/article/us-europe-attacks-france-idUSKBN18Y12T/.

Jungwirth, Reiner, H. Smith, E. Willkomm, J. Savolainen, M. Alonso Villota, M. Lebrun, A. Aho, and G. Giannopoulos. 2023. *Hybrid threats: a comprehensive resilience ecosystem.* Luxembourg: Publications Office of the European Union. doi:10.2760/37899.

Mastor, Wanda. 2017. "The French Intelligence Act : "The French Surveillance." *European Public Law* 23 (4): 707-722.

Ministere des Armées. 2024. *Etat-major des armés.* https://www.defense.gouv.fr/ema.

Mirković, Vladan. 2024. "Security Management of the Italian Republic in the Contemporary Security Environment." *SCIENCE International Journal* 3 (3): 97–103. https://doi.org/10.35120/sciencej0303097m.

NATO. 2022. "NATO 2022 Strategic Concept." NATO Summit. https://www.nato.int/strategic-concept/.

Nunez, Laurent, interview by Mathew Levitt. 2021. *Contending with New and Old Threats:A French Perspective on Counterterrorism.* https://www.washingtoninstitute.org/policy-analysis/contending-new-and-old-threats-french-perspective-counterterrorism.

Olech, Aleksander. 2022. *French and Polish fight against terrorism.* Poznań: Kontekst Publishing House.

Pardini, Gérard. 2019. "La sécurité nationale: Un concept à enraciner." *Cahiers de la sécurité et de la justice* (no. 45): 4-9. www.ihemi.fr/sites/default/files/articles/files/2020-01/article_csj45_pardini_securite_nationale.pdf.

Pateman, Lili, and Romain Geoffroy. 2024. "What's a cohabitation in French politics and what are the precedents?" *Le Monde.* https://www.lemonde.fr/en/les-decodeurs/article/2024/06/17/what-s-a-cohabitation-in-french-politics-and-what-are-the-precedents_6674967_8.html.

Premier Ministre. 2018. "Academie-renseignement." *La Communaute française du renseignement.* https://www.academie-renseignement.gouv.fr/files/plaquette-presentation-comrens.pdf.

President of the Republic. 2008. *The French White Paper on Defence and National Security.* Security and Defence Strategy, New York: Odile Jacob Publishing Corporation.

SGDSN, Secrétariat général de la défense et de la sécurité nationale. 2022. *National strategic review.* Paris: Security and Defence Strategy Review. https://www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf.

SGDSN, Secretariat General for Defence and National Security. 2024. *SGDSN in English.* https://www.sgdsn.gouv.fr/sgdsn-english.

Smith, Hanna. 2019. *NATO and the EU - Countering hybrid threats.* Rome: NATO Defense College. https://www.jstor.org/stable/pdf/resrep19964.7.pdf.

VIGINUM. 2024. *Welcome to Jungle.* https://www.welcometothejungle.com/fr/companies/viginum.

Walker, Robert G. 1998. *Spec Fi: The United States Marine Corps and Special Operations* . Monterey: Naval Postgraduate School. https://archive.org/details/specfiunitedstat109458989.

Wigell, Mikael. 2019. "Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy." *International Affairs* 255–275. doi:10.1093/ia/iiz018.

Wigell, Mikael, Harri Mikkola, and Tapio Juntunen. 2021. *Best Practices in the whole – of – society approach in countering hybrid threats.* Strasbourg: European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf.

Wither, James K. 2023. "Hybrid Warfare Revisited: A Battle of 'Buzzwords." *Connections: The Quarterly Journal* (no. 1): 7-27. https://doi.org/10.11610/Connections.22.1.02.

Legal acts

Arrêté du 29 octobre 2007 portant création d'un service à compétence nationale dénommé " direction nationale du renseignement et des enquêtes douanières. https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006076055.

Constitution of October 4, 1958. https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/anglais/constiution_anglais_oct2009.pdf.

Code de la Défense, Version en vigueur au 27 septembre 2024. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071307/LEGISCTA000006096399/#LEGISCTA000006096399.

Code de la Sécurité Intérieure, Version en vigueur au 27 septembre 2024. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000025503132/.

Code monétaire et financier. Version en vigueur au 27 septembre 2024. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072026/.

Décret no 2022-491 du 6 avril 2022 relatif aux emplois de préfet et de sous-préfet. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045522798.

Décret no 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé "service de vigilance et de protection contre les ingérences numériques étrangères". https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361.

Décret no 2020-455 du 21 avril 2020 portant création d'un service à compétence nationale dénommé opérateur des systèmes d'information interministériels classifies. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000041814396/2020-10-05/.

Décret no 2017-1095 du 14 juin 2017 relatif au coordonnateur national du renseignement et de la lutte contre le terrorisme, à la coordination nationale du renseignement et de la lutte contre le terrorisme et au centre national de contre-terrorisme. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034938469/.

Décret no 2014-833 du 24 juillet 2014 relatif à l'inspection des services de renseignement. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029290787.

Décret no 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028887486.

Décret no 2013-728 du 12 août 2013 portant organisation de l'administration centrale du ministère de l'intérieur et du ministère des outre-mer. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000027838041/.

Décret no 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé Agence nationale de la sécurité des systèmes d'information. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000020828212.

Décret no 92-523 du 16 juin 1992 portant création de la direction du renseignement militaire. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000357733.

Décret du 9 mai 1990 portant création d'une cellule de coordination chargée du traitement du renseignement et de l'action contre les circuits financiers clandestins (TRACFIN). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000714950.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Conventional Arms Control in the Baltic Sea: A Montreux for the North

William LIPPERT, Ph.D. Candidate*

*Institute of Security and Global Affairs, Leiden University, Netherlands
e-mail: lippertwe@gmail.com; w.e.lippert@fgga.leidenuniv.nl
https://orcid.org/0000-0001-6546-6109

Abstract

A conventional arms control (CAC) agreement for the Baltic Sea could help stabilize the security relationship, reduce arms racing, and improve diplomatic relations between Russia and the North Atlantic Treaty Organization (NATO). Similar to the Montreux Convention, which governs the passage of naval forces through the Turkish Straits, a CAC agreement focused on the Danish Straits could set limits on the size, type, number, and total tonnage of naval ships that pass through the straits. Additionally, or alternatively, an agreement could set limits on naval vessels based in the Baltic Sea, based on a combination of ratios, ship types, and capabilities. Any agreement could be implemented and managed by the state parties themselves or delegated to an agreement executor, such as an international organization.

Keywords:
Conventional arms control; Baltic Sea; Montreux Convention; Danish Straits.

Article info
Received: 11 December 2024; Revised: 2 February 2025; Accepted: 26 February 2025; Available online: 2 April 2025

Citation: Lippert, W. 2025. "Conventional Arms Control in the Baltic Sea: A Montreux for the North." *Bulletin of "Carol I" National Defence University*, 14(1): 52-73. https://doi.org/10.53477/2284-9378-25-04

Though the Russo-Ukraine War rages without any certain end in sight, attempts to prevent another conventional conflict in Europe should still be considered. Future agreements and policies should be based on the notion that the Russo-Ukraine War was caused in large part by the Russia-North Atlantic Treaty Organization (NATO) rivalry, which itself was amplified by the deterioration of conventional arms control (CAC) and failure to establish a new CAC regime adapted to the significantly altered European security landscape than that which existed in 1992 when the Conventional Armed Forces in Europe (CFE) Treaty entered into force (Kühn 2020; Lippert 2024b; Nelson and Twardowski 2022).

A broad, Europe-wide CAC agreement from the Atlantic to the Urals (ATTU) might be called for – essentially an updated CFE Treaty that includes all NATO and European Union (EU) members[1], Ukraine, Russia, Belarus, and potentially other states in eastern Europe but not necessarily those in central Asia. Such an agreement may be necessary to offer a comprehensive, stable arms control regime that both prevents a surprise attack and offers all parties a sense of "indivisible security" (Kvartalnov 2021; Perrin de Brichambaut 2010). Alternatively, or in combination with a broad agreement, a narrow, geographic demilitarization agreement can contribute to crisis stability, stabilize an aspect of the EU/NATO-Russia relationship, and improve diplomatic relations to pave the way or build upon other CAC agreements[2]. With the complete suspension of the CFE Treaty, only minimal application of the Open Skies Treaty (OST) (NATO 2021), and Russia's non-compliance with the Vienna Document (Rosa-Hernández 2023), there are currently no Europe-wide arms control measures or significant CSBMs that temper the EU/NATO - Russia security rivalry.

This article discusses options and issues concerning a "Montreux Convention for the Baltic Sea," which could include naval limits on Baltic Sea states for forces based in the Baltic Sea, controls and rules on access to the Baltic Sea through the Danish Straits for all naval vessels, and limits placed on naval forces permitted in the Baltic Sea for non-Baltic Sea states. Such an agreement could help stabilize the great-power rivalry between NATO and Russia (Mazarr et al. 2021) that contributed to the Russo-Ukraine War through the development and implementation of a specific CAC agreement[3]. This agreement can offer all parties benefits at minimal costs. For the EU/NATO, it could improve relations with Russia and prevent or halt arms racing in the Baltic Sea. For Russia, it could offer increased security compared to an unchecked increase in NATO naval capability in the Baltic Sea. Addressing Russia's security concerns and geopolitical ambitions is more necessary now than in the past, given that Moscow is unilaterally looking to alter existing borders (AP News 2024). What confronts Baltic Sea states and EU/NATO members more broadly today is whether they

[1] The EU has not been extensively involved in major arms controls agreements, but there is a need for their future involvement. See Portela (2021) and Lippert (2023b).

[2] Burns and Urquidi (1968) offer a detailed discussion of the differences between geographic demilitarization and broader, arms limitations.

[3] See, for example, Charap et al. (2020) for concrete, CAC recommendations made prior to the Russo-Ukraine War.

want to retain a confrontational approach with Russia or seek (eventually) a more cooperative relationship (Claeys and Williams 2022).

Previous discussions about arms control in the Baltic region have focused on land forces and/or only offered vague recommendations for CAC in the Baltic Sea (Engvall et al. 2018; Kacprzyk and Kulesa 2020; Richter 2016; Zellner, Oliker, and Pifer 2020). Buzhinskiy and Shakirov (2019) briefly discuss naval CAC in the Baltic region but dismiss it as infeasible. This article offers an original set of detailed proposals and discussion focused on the Baltic Sea.

One of the EU/NATO's main goals would be to offer Russia assurances and a diplomatic and security gain both to improve diplomatic relations overall, and potentially as part of a broader diplomatic or CAC agreement. For Russia, any offer to establish limits on NATO naval forces in the Baltic Sea should be welcomed, given the substantial imbalance of naval forces it faces with Sweden and Finland's accession to NATO (Dahlstrand 2024; Dyer 2023; Kayali 2023; Newsweek 2023).

The Montreux Convention

The 1936 Montreux Convention for the Turkish Straits, officially entitled the *Convention Regarding the Regime of The Straits*, was an evolution of an earlier agreement, the 1923 *Convention Relating to the Regime of the Straits and Turkey* (Lausanne Treaty). At the end of the First World War, the newly independent state of Turkey (now Türkiye) was established from the break-up of the Ottoman Empire and the new state's borders contained in their entirety the Bosporus, Dardanelles, and the Sea of Marmara – collectively referred to as the Turkish Straits *(see map 1)*. Negotiations between interested states about control of the straits resulted in the Lausanne Treaty, which gave Türkiye control of the straits but prohibited Türkiye from placing weapons and fortifications along the strait's coastlines. Additional rules applied to naval forces passing through the Straits, in part based on a compromise between Soviet Russia in particular which sought to restrict all naval ships from passing through the straits and global seapowers such as the United Kingdom which sought to retain freedom of navigation to and within the Black Sea (Seydi 2010). The basis of maintaining the Turkish Straits as an international waterway was based on historical custom and existing international law (Ünlü 2002).
Türkiye, however, was dissatisfied with the limits imposed on its military, which prohibited fortifications and other military capabilities along the straits, and in 1936, it successfully negotiated a revision that was signed by state parties in Montreux, Switzerland.

The Montreux Convention removed any restrictions on Türkiye concerning its own military and also removed the limited roles of the League of Nations and the Straits

Commission in monitoring compliance. The Montreux Convention's CAC elements include limits on the ship tonnage of non-Black Sea states that can transit the straits; the number of naval ships that may pass through the straits at any one time; the total tonnage that any non-Black Sea state may have in the sea at any one time; and the duration that a non-Black Sea naval vessel may stay in the sea. While in times of peace, the straits are open to all navies; in times of war, belligerent Black Sea states may only transit the straits if the ship is returning to its home port (either entering or exiting the Black Sea). A non-Black Sea state at war (in principle *anywhere* in the world) cannot transit the straits[4].

The treaty's application was soon tested during World War Two, when both sides sought to use the straits to move military supplies and naval ships back and forth between the Black Sea and the Mediterranean. While there were instances of deceit and some inconsistent application of the rules, by and large, Türkiye upheld the Montreux Convention while remaining neutral and applied it equally to all belligerents (Seydi and Morewood 2005). The belligerents themselves did not seek to openly violate the rules openly, as doing so might have offered Türkiye a justification to lift rules applied to the other side. Arguably, the establishment of naval passage through the straits and their fair application decreased the incentive of belligerents to attempt a (possibly expensive) seizure of the straits. This phenomenon finds similarities in other geographic demilitarization efforts, such as Norway's Spitsbergen and Finland's Åland Islands, which prohibit the presence of *any* military forces in times of peace. This phenomenon of an arms control agreement in which the absence of possession by all parties resolves a security dilemma reminiscent of Schelling's (1975) notion of an "IFF" preference. In his framework, he was referring to a weapon system, with an IFF framework referring to the notion that a state would only want to possess a weapon system *if and only if* its adversaries possessed it. The correspondence between Schelling's IFF and agreements such as the Montreux Convention is that both sides may accept that, first, they do not need to control the straits as long as an adversary does not; and second, that they do not need substantial foreign naval reinforcements if the other side does not have them.

The Convention is still in force and was applied by Ankara soon after Russia invaded Ukraine in February 2022. The impact on Russia is likely significant – it cannot easily reinforce its Black Sea fleet or quickly replace losses (Axe 2023) (most of its navy's larger surface vessels and submarines are homeported outside of the Black Sea (Office of Naval Intelligence 2015; "Chapter Five: Russia and Eurasia" 2022). The impact on Ukraine is less certain. On the one hand, Ukraine's surface combat fleet prior to Russia's full-scale invasion was relatively small ("Chapter Five: Russia and Eurasia" 2022).

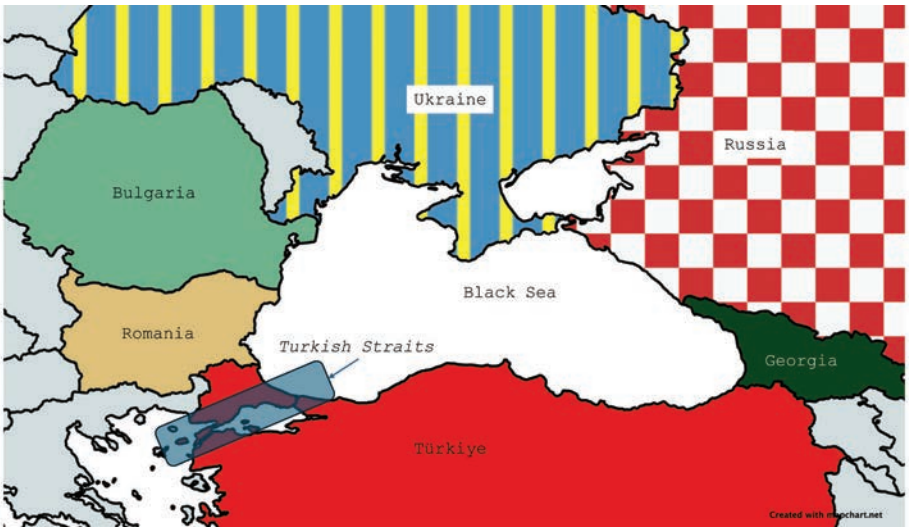
[4] While applying Montreux Convention limitations to states involved in a conflict involving Black Sea states is relatively straightforward – such as the Russo-Ukraine War, determining that states are at war elsewhere in the world with no immediate impact on the Black Sea and its littoral states may be more complicated. This issue arose, for example, when the US sought to send a warship into the Black Sea during the Vietnam conflict. The Soviet Union objected, claiming that the US was a belligerent state, but Turkey determined that the conflict was not a war (Ünlü 2002, 90).

But on the other, Türkiye's policy of prohibiting *any* naval ships' passage through the straits reduces Ukraine's ability to obtain naval vessels for Black Sea operations (Reuters 2024), or for NATO to provide any assistance, for example, escorting grain shipments (Isachenko 2023; Overfield 2022). The absence of naval reinforcements reduces Ukraine's ability to defend its coastline, including its air defense, and clear waterways of mines, which is important for Ukraine's maritime trade[5].

[5] It remains to be seen to what extent other Black Sea states can reduce this threat (see, for example, (Kucukgocmen and Hayatsever 2024) – and if this will be sufficient if they do not remove mines from Ukrainian waters.

The Montreux Convention serves as a useful template for any CAC agreement for the Baltic Sea due to similarities such as rival states sharing a large sea with limited access, although a substantial difference is that the Black Sea is composed of non-NATO states, NATO members, and Russia so that Turkey remain – as is currently the case – neutral while two non-NATO Black Sea states are at war. This means that Ankara can impartially implement the Montreux Convention as a non-belligerent state. However, excepting the near-term improbability of two Baltic Sea NATO states engaging in conflict with one another, any conflict between Russia and another Baltic Sea state would minimize Sweden and Denmark's neutrality due to all Baltic Sea states other than Russia belonging to NATO.

Map 1 - Black Sea



The Baltic Sea

The Baltic Sea's primary access route that can accommodate ships of all sizes runs from the Kattegat Strait between Sweden and Denmark, and then through the relatively narrow Oresund, Little Belt and Great Belt into the Baltic Sea. While the Kattegat flows through Swedish and Danish territorial waters, the Belts are wholly within Danish territory. The Oresund separates Denmark and Sweden and is wider and deeper than the Little and Great Belts and handles more traffic (Helsinki Commission, n.d.). Collectively, these are

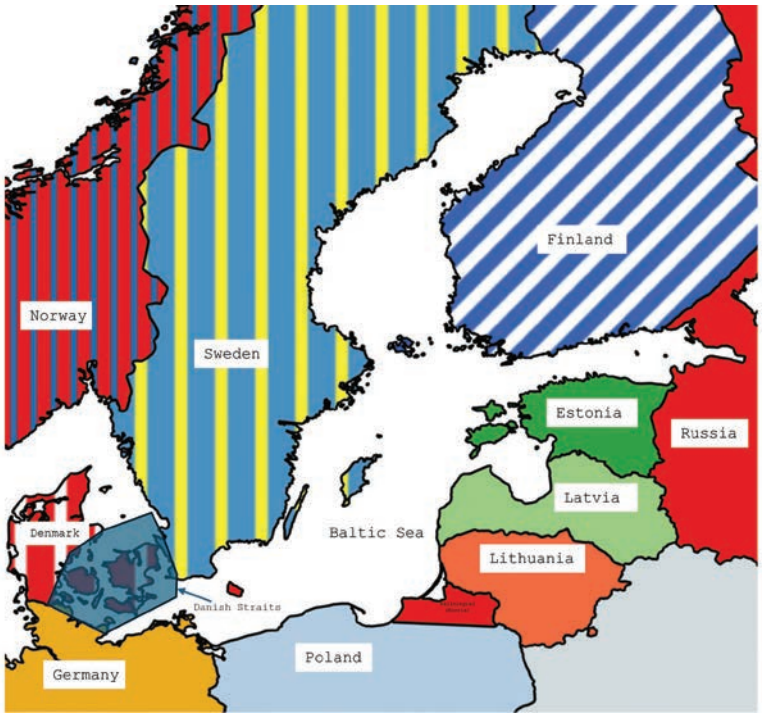
referred to as the Danish Straits and are considered international waterways and thus as a matter of maritime law naval vessels by default have a right to transit them with some rules applied for reasons of safety (such as the requirement for submarines to surface while transiting) and security, such as limits on the number of warships that may pass the Danish Straits together (Denmark 1999; Sweden 1966) *(see map 2)*.

The Kiel Canal connects the North and Baltic Seas within German territory, cutting across northern Germany south of Denmark. Due to a combination of international customs and German laws, the waterway is subject to German government approval for the passage of naval vessels[6]. On the eastern end of the Baltic Sea, the White Sea- Baltic Canal and the Volga- Baltic Waterway are minor, artificial sets of canals that lead to the North, Black, and Caspian Seas (Deaton 1975; Swistek and Paul 2023). While the Russian canals offer Moscow some flexibility regarding the way to access the Baltic Sea, due to their shallow depth and narrow width, the canals are neither an efficient route nor can they support larger vessels (Savitz and Winston 2024).

Perhaps the most significant difference between the Baltic and Black Seas is that the former is entirely NATO dominated, with Russia only retaining a narrow coastline along the Baltic Sea, and its navy is much smaller than NATO's collective naval forces in the Baltic Sea. Among the strategically important Russian areas that border the Black Sea are the exclave of Kaliningrad and Saint Petersburg.

[6] The Kiel canal management has indicated that permission from the German government is likely required for passage of Russian naval vessels (UCA Kiel 2023). Another document indicates that Russian-flagged vessels are unable to use the canal due to EU sanctions ("Notification Requirements," n.d.). These indicators suggest that the Kiel canal is subject to more restrictions and sovereign control than the Danish or Turkish Straits.

Map 2 - Baltic Sea



Potential CAC in the Baltic Sea

Russia would have an interest in seeing any Baltic Sea naval restrictions. Although it can freely move its own naval forces in and out of the Baltic Sea in times of peace, Moscow faces comparative disadvantages. First, the overall size of NATO's navies – especially due to the US's naval fleet – dwarves that of Russia's. Thus, without limits, NATO naval forces can threaten Russia far more than Russia can threaten NATO. Second, NATO's industrial and defense capacity outstrips Russia's so that, if unchecked, the Baltic Sea NATO states will produce far more ships than Russia. Access and/or national limits could at least stabilize Russia's disadvantage. Third, it might be possible for Sweden and Denmark to prevent the passage of Russian warships in times of crisis, leading to escalation and potential conflict. A legally binding agreement would establish the precise conditions in which the Danish straits could be closed to Russian naval vessels. Table 1 contrasts and compares the Turkish Straits agreements with potential Danish Straits and Baltic Sea CAC agreements.

Russia should be especially concerned about NATO's overall growing coastal and naval activities in the Baltic Sea area, such as NATO naval exercises (Reuters 2023; Brooks 2022). NATO established Baltic Sentry in early 2025 in response to underwater communications cable damage and to generally deter Russian naval activities and presence (Shape.Nato.Int 2025). Baltic Sea NATO members plan continued upgrades and expansions of their naval capabilities (Livermore 2024).

Access Control

One aspect of a Baltic Sea CAC regime could be the establishment and implementation of naval vessel access controls. These already exist to a limited extent according to Danish and Swedish laws, limiting the number of naval vessels that may transit the Danish Straits simultaneously and the requirement for submarines to transit surfaced. The former likely reflects, even if not explicitly, fears of attack by sea. For example, the German invasion of Norway by sea included the passage of a German fleet through the Danish Straits. Nothing in international or national laws, however, prohibit Denmark or Sweden from permitting larger fleets from transiting their waters through the Danish Straits in peacetime – a notable difference from the Montreux Convention which limits the aggregate number (to include non-Black Sea naval vessels already in the Black Sea) and size of non-Black Sea state naval vessels[7].

Aside from fears of enemy action, Sweden and Denmark impose reasonable maritime safety measures due to the Danish Straits' narrowness and high

[7] The Montreux Convention Article 21 permits Turkey to impose unilateral control over the straits when it might "consider herself to be threatened with imminent danger of war".

TABLE NO. 1

	Lausanne	Montreux	Current Danish Straits Restrictions	Danish Straits Potential Limitations	Potential Baltic CSBM	Potential Baltic Medium Limits	Potential Baltic Deep Limits
Area of Application	The Turkish Straits, its shorelines, and entry/exit areas.	Turkish Straits.	Danish Straits (Sweden and Denmark territorial waters).	Danish Straits (Sweden and Denmark territorial waters).	Baltic Sea.	Baltic Sea.	Baltic Sea.
Tonnage restrictions	No individual ship shall exceed 10,000 tons.	The maximum aggregate tonnage of all foreign naval forces which may be in course of transit through the Straits shall not exceed 15,000 tons; the aggregate tonnage which non-Black Sea Powers may have in that sea in time of peace shall not exceed 30,000 tons.	None.	Other than Sweden and Denmark, a limitation of 15,000 tons for one ship, maximum of three ships.	Reporting of naval ships over 1500 tons entering or departing the Baltic Sea, to include production within.	Limit of a certain number of ships total for each side (not necessarily even number), above a certain tonnage, in part based on class. For example, for "destroyers" a ratio of 5:3; for cruisers 1:1; etc.	Only a small number of ships permitted between certain tonnages (real numbers at a ratio), for example 10,000-20,000. Above a certain number, 20,000, no military vessels permitted. Prohibition of amphibious assault ships.
Rule differentiation based on geography	None.	Black Sea Powers may send through the Straits capital ships greater than 15,000 tons, on condition that these vessels pass through the Straits singly, escorted by not more than two destroyers. Other definitions of ships based on gun calibre.	None (excluding Danish/Swedish sovereignty).	No single tonnage limitation for Baltic Sea states, but no more than three ships totaling 45,000 tons at any one time.	Reporting would not apply to ships *not* in, entering, or departing the Baltic even if the state is a Baltic sea state (ie the ships are outside of the Baltic Sea).	Non-Baltic Sea states are permitted up to five naval vessels totally 50,000 tons per state.	Non-Baltic Sea NATO states are only permitted up to three naval vessels combined totalling 30,000 tons in the Baltic Sea at any one time. Amphibious assault ships and submarines from non-Baltic Sea states are prohibited.
Firepower restrictions	None.	For auxilliary vessels, 105 mm anti-surface guns, and 75 mm anti-air guns.	None.	None.	Above a certain firepower, perhaps defined by number of missiles or missile tubes (excluding small missiles) could be reported. This might account for small boats armed with anti-ship missiles.	Limitation on the number and a fixed ratio of VLS/missile tubes.	Limitation on the number and a fixed ratio of VLS/missile tubes (lower ceiling compared to medium limits).
Aircraft restrictions	Freedom to fly over a strip of territory of five kilometres on each side of the narrow parts of the Straits;	Vessels of war in transit through the Straits shall in no circumstances make use of any aircraft which they may be carrying. No other mention of military aircraft.	Denmark: restrictions on activities; Sweden: no restrictions in a narrow corridor. A bit unclear however, although some sources say it is sovereign airspace subject to permissions (and specifically in contrast to sea vessels).	No change.	Reporting of planned military aircraft activities above a certain threshold and/or in a certain international area.	A specified area might be prohibited to armed military aircraft.	A specified area might be prohibited from armed military aircraft (lower ceiling and/or larger area, compared to medium limits).
Fortifications	Demilitarization (military forces and fortifications) along the Straits shorelines.	None.	None.	None.	None.	None.	None.
Quantitative restrictions	Based on the total Black Sea fleet size of	The maximum aggregate tonnage of all foreign	Sweden: Not more than three naval vessels of the same	Maximum of three naval vessels (except for	Not applicable.	Limit of a certain number of ships total for each side	Only a small number of ships permitted between
	the most powerful fleet; and not more than three ships of which none shall exceed 10,000 tons. Limit of 12,000 soldiers in Constantinople.	naval forces which may be in course of transit through the Straits shall not exceed 15,000 tons, except in certain cases and not more than nine vessels. In the Black Sea itself, the aggregate tonnage which non-Black Sea Powers may have in that sea in time of peace shall not exceed 30,000-45,000 tons depending on the tonnage of the largest Black Sea fleet.	belligerent Power, or of allied belligerent Powers, may be within Swedish territory at the same time. A naval vessel of a belligerent Power shall be admitted to pass through the territorial sea for a maximum period of 24 consecutive hours. A naval vessel of a belligerent Power shall not stop or anchor or otherwise interrupt its voyage within Swedish territory unless this is necessary for the safety of the vessel. Unclear what new rules will apply to NATO members. No clear limits imposed by Denmark.	Denmark/Sweden) for any one nation or alliance.		(not necessarily equal ratio), above a certain tonnage, in part based on class. For example, for "destroyers" a ratio of 5:3; for cruisers 1:1; etc.	certain tonnages (real numbers at a ratio), for example 10,000-20,000. Above a certain number, 20,000, no military vessels permitted. Prohibition of amphibious assault ships.
Monitoring and verification	Straits Commission on-site inspections	Unilateral and national means.	None (unilateral).	Joint NATO-Russia Commission.	OSCE.	Joint NATO-Russia Commission or OSCE.	New Baltic Sea-Specific International Organization.
International Organization role	Straits Commission, composed of state representatives.	None.	None (unilateral).	Joint NATO-Russia Commission.	OSCE.	Joint NATO-Russia Commission or OSCE.	New Baltic Sea-Specific International Organization.
Exemptions	Right of Turkey to move forces through the Straits; Turkey and Greece could move forces through the demilitarized areas.	None; Tükiye is not subject to limitations.	Denmark/Sweden are not subject to limitations.	Denmark/Sweden are not subject to limitations.	Ships not in the Baltic Sea, even if belonging to a Baltic Sea state.	Emergency humanitarian operations, as informed and monitored.	Emergency humanitarian operations, as informed and monitored.
Dispute adjudication	Council of the League of Nations.	Bilateral/diplomatic.	Bilateral.	Joint NATO-Russia Commission, OSCE, and United Nations.	Joint NATO-Russia Commission, OSCE, and United Nations.	Joint NATO-Russia Comission, OSCE.	Joint NATO-Russia Comission, OSCE. Possibily New Baltic Sea-Specific International Organization.
Other	No violations of Turkish neutrality (attacking enemy forces within the Straits). No passage for states at war, unless Turkey is at war then the Convention does not apply.	Vessels of war belonging to non-Black Sea Powers shall not remain in the Black Sea more than twenty-one days, whatever be the object of their presence there.	Submarines must transit surfaced. Prohibitions on various activities such as espionage and taking scientific measurements.	Denmark and Sweden may close the Straits to belligerent states at war with another state in the Baltic Sea, if Denmark/Sweden are non-belligerent parties. That is, a non-Baltic Sea state at war with a Baltic Sea state would not be permitted to transit the Straits; and a Baltic Sea state vs. another Baltic Sea state in which case no Baltic Sea state at war may transit.	Additional protocols involving long-range weapon firing, and exercises in the Baltic Sea over a certain quantity, such as a 10 vessels and 30 aircraft.	Vessels flagged by Baltic Sea states that are not present and/or based in the Baltic Sea will not count towards any totals and limitations.	Vessels flagged by Baltic Sea states that are not present and/or based in the Baltic Sea will not count towards any totals and limitations.

traffic. Even in the best of circumstances, ships can collide in busy seaways and naval ships may be more vulnerable to accidents due to combinations of radar and visibility reductions (modern naval vessels often incorporate radar signature reduction designs and due to their often matte gray paint, they are less visible compared to commercial and civilian vessels), potentially higher speeds, and possibility of turning off identifying, navigation radio signals (Labrenz 2023). The requirement for submarines to travel surfaced is an obvious question of safety, as submerged submarines are difficult to detect and, should they surface in constricted waterways, may easily collide with other ships[8].

The Montreux Convention imposes a variety of access controls which might be transferrable to the Danish Straits. First, there may be limits on the size (tonnage) of naval vessels. Ship tonnage is a fairly straightforward measure of a ship's capability, with larger vessels being more capable because more systems and weapons fit in it[9]. This comparison is restricted to ships of the same technological generation; an 8000-ton modern destroyer arguably has much more anti-ship capability than a World War Two-era 65,000-ton battleship because the former is equipped with accurate, long-range anti-ship missiles.

The Montreux Convention also specifically prohibits the transit of non-Black Sea states' capital ships, as defined by tonnage and/or firepower, and submarines. Additionally, though not specified in the Convention, the Turkish government prohibits the passage of all aircraft carriers ("Implementation of the Montreux Convention", n.d.).

Ship tonnage and quantity are two approaches to limit access to the Baltic Sea through the Danish Straits. First, there may be a universal limit on ship types based on tonnage and firepower. Before the age of missiles, firepower was easily determined by barrel caliber and the number of large guns. Today, however, guns are irrelevant to naval surface warfare, having been replaced by missiles. Assessing ship firepower in the missile age is much more difficult than in the gun age because missile capabilities vary significantly due to technology, design, and tactics. Moreover, ships carry missiles for a variety of missions such as anti-ship, anti-submarine, surface strike, and air defense. Despite the challenges of measuring naval firepower, as most naval ships today are equipped with vertical launch systems (VLS), the quantity of these can be used as a measure of a ship's firepower.

Tonnage-based limitations could hedge against states attempting to circumvent firepower limits and might otherwise offer a means to anticipate changes in naval ship design and warfare. Moreover, a tonnage limit can help prevent ships from circumventing any restrictions based on ship class designations. While broad ship classes may exist for naval vessels, many

[8] See, for example, the collision of a surfacing Japanese submarine with a commercial ship (Ogura 2021).
[9] See, for example, Peck's (2019) discussion about battlecruisers being less capable than battleships due to less armor (less mass).

ships can fall between or within several categories. For example, any restrictions on aircraft carriers will be frustrated by a lack of a universal definition of such ships. Some fixed-wing aircraft-carrying ships also conduct other missions, such as amphibious assault. Two examples of these gray areas are the Soviet *Kiev* and *Kuznetsov* aircraft-carrying cruisers and the US amphibious assault ships that double as fixed-wing aircraft carriers. Both these types of ships displace significantly more mass than a modern cruiser or destroyer.

A universal tonnage and firepower restriction would offer Russia an increased sense of security as it would decrease its fear of a sea-based attack in the Baltic Sea. This would reduce arms racing and contribute to confidence building. While some states might object to what would amount to *de facto* national limits if their entire coastline falls within the Baltic Sea, it is unclear that they require the restricted vessels or, if they do, that these cannot be based in the ports of other NATO members. Foreign-basing of naval vessels is widely practiced by the United States, with other countries operating primarily foreign naval support facilities without permanently assigned ships. This approach may in part suggest a more alliance-wide approach to defense planning, basing, and deployments for NATO – one that treats NATO's entire geographic space as a single, continuous zone or at least substantial areas and blocs of states as a single zone for CAC purposes, much as Russia seeks be considered as a single zone (west of the Urals) instead of it being partitioned into CAC zones which restrict internal movement – but this is beyond this article's scope.

Another approach, which the Montreux Convention also incorporates, is the placement of certain limits on non-Baltic Sea states and different restrictions (or no restrictions) on Baltic Sea states. The Montreux Convention sets limits on aggregate tonnage of all non-Black Sea state naval vessels combined, the aggregate tonnage for any one non-Black Sea state, and the duration in which they may remain in the Black Sea. The latter varies from most of the other Convention's stipulations as the limit goes beyond transiting; that is, once a vessel has passed through the Turkish Straits, it is unclear how Türkiye could compel a state to withdraw the vessel other than through diplomatic means and by refusing entry of the violator's other naval vessels.

Baltic Sea limitations that apply only to non-Baltic Sea states could still reduce arms racing and build confidence and security, but without Russia seeing limits imposed on its navy. On the other hand, the limits would not (in this approach) apply to the Baltic Sea NATO states, thus it might not go far in increasing Russia's sense of security although restrictions placed on NATO's top three naval powers – the US, UK, and France –in the Baltic Sea (as non-Baltic Sea states) should improve Russia's perception of security.

National and Bloc Limits

The national naval limits of Baltic Sea states represent another approach that could be adopted to CAC in the Baltic Sea. This would be a substantial variation

of the Montreux Convention, which did not impose limits on the size or composition of Black Sea naval fleet sizes – limits rather applied primarily to transiting the Turkish Straits and *de facto* limits. Rather, national naval limits would build on an established history of national, military capability CAC agreements. Among these are the 1922 Washington Naval Treaty which set limits on capital ships amongst five major naval powers and the 1990 Conventional Armed Forces in Europe (CFE) Treaty which set limits on five categories of land-based weapon systems from the North Atlantic to the Ural Mountains (often referred to as the Atlantic to the Urals (ATTU)).

While the CFE Treaty set equal limits for NATO and the Warsaw Pact, the Washington Naval Treaty established a ratio of naval forces between five states. Measured in tonnage, the ratio was 5:5:3:1.67:1.67 ratio of tonnage for the United Kingdom, the US, Japan, France and Italy, respectively. This ratio was established based on a combination of existing naval power and perceived naval force requirements with the US and UK, for example, having by agreement a greater need for a larger navy compared to other state parties. Importantly and relevant to today, the CFE and Washington Naval Treaties were signed during times of peace between the signatories, albeit the proxy war that NATO and Russia find themselves in Ukraine creates a much more challenging atmosphere for agreement as well as casting into question bases for any ratios. Another agreement of interest is the 1817-1818 Rush-Bagot Treaty between the US and Canada, which sets (it is still in force despite the two states' close alliance) limitations on fortifications and naval vessels in and around the Great Lakes (Bagot and Rush 1817; O'Neill 1991).

The issue of whether an agreement is signed during peace or war (or soon after) is important because peace agreements often require extensive bargaining and discussions, as each side has the capacity to refuse the agreement with minimal consequences. In contrast, a conflict or post-conflict agreement, such as the post-World War treaties, permits the victor to impose CAC limits and measures on the defeated state(s) without accepting any limits on their own military forces[10]. It is unclear if post-Russo-Ukraine War agreements between Russia and NATO are likely to lean towards peacetime or discriminatory post-conflict agreements, but currently, a Baltic Sea agreement is more likely to reflect a peacetime agreement due to neither side having the capacity to impose a discriminatory agreement on the other (Lippert 2024a).

Currently, available information from the 2025 IISS Military Balance and other sources suggest that Baltic Sea NATO tonnage far surpasses Russia's by a ratio of 85:15, or 217,000 metric tons to 40,000[11]. Thus, realistically, Russia is unable to compete with NATO's current Baltic Sea fleet, even

[10] One exception to this was the peacetime, 1920 Russia-Finnish agreement signed in Tartu/Dorpat which imposed substantial limits, particularly naval, on Finland. Finland was newly independent from imperial Russia, but newly-established.

[11] For this calculation, all of Germany's fleet is counted for simplicity, although its ships can be based in the North Atlantic rather than the Baltic Sea. The calculations are based on various open sources, such as The Military Balance ("Chapter Three: Europe" 2025; "Chapter Four: Russia and Eurasia" 2025), and count combat ships of 20 tons and higher, excluding, for example, inflatable boats. Russia's calculations are an estimate based on multiple sources of what it may have in the Baltic Sea at any given time, and likely overestimates actual holdings.

excluding NATO reinforcements from outside of the Baltic Sea. For example, a ten percent increase in tonnage offers Russia a modest 4000 tons, which is approximately one frigate. NATO, on the other hand, would gain 22,000 tons with a ten percent increase – or the equivalent of five frigates.

Though the CFE Treaty and its additional protocols specify national limits in five TLE categories, the treaty established equal limits for NATO and the Warsaw Pact collectively. A similar approach could be done with a Baltic Sea limitation treaty. NATO and Russia could agree on a broad ratio and limitations, and then work backwards to define national limits. Alternatively, the two sides might agree on an overall NATO ceiling, reflecting Russia as a single-entity, then NATO could manage the ceiling internally[12].

[12] When the Soviet Union was dissolved, the newly independent states divided CFE Treaty TLE limits amongst themselves.

The ratio approach still leaves open several questions and choices. First, should there be reductions in TLE or should Baltic Sea fleets be subject to a ceiling that is either at or higher than current inventories? The CFE Treaty mandated the destruction of a significant amount of TLE by both blocs, although the Warsaw Pact had a heavier destruction burden as they had more TLE than NATO at the time of CFE signature and entry into force. TLE limits or reductions reduce the capability of conducting a surprise attack – which was one of the CFE Treaty's main goals.

Another question would be whether to only count tonnage or to also include counts for specific ship types. For example, a strong case can be made that 20 ships of just 1000 tons each (a large patrol vessel) are not as capable as 5 ships of 4000 tons each (approximately a frigate). This is because small ships lack capabilities that larger ships have, such as advanced radar and sonar systems as well as helicopter-carrying capacity. Thus, limits could be both on total tonnage and per ship class and type. This would be in line with previous naval agreements, including the Washington Naval Treaty and the Montreux Convention, which established ship class definitions and limits specific to each class. Prohibitions on specific ship classes or ships above a certain size could also be considered, such as cruisers, large amphibious assault ships, and aircraft carriers.

Another, and perhaps the most important and difficult question to resolve, is the allocation of limit ratios. Russia might seek (and certainly prefer) an even ratio of 1:1 or even a ratio in its favor. However, there is no historical justification for this, as CAC agreements often reflect the military balance at the time of agreement[13]; that is, NATO is unlikely to give up a substantial advantage *unless* the agreement is closely tied to a broader ATTU agreement and/or to ending the Russo-Ukraine War. If a substantial reduction in the gap between NATO and Russian Baltic Sea capabilities is not likely, this still leaves open the possibility that the gap can be narrowed – or even

[13] Reference CSP article.

broadened – but to an extent that reduces the potential, long-term gap. Concerning the latter option, if Russia faces a potential tonnage ratio of 95:5 in fifteen years, it might be willing to accept a limitation which locks in a ratio at 90:10 – worse than the current ratio of 85:15 – but better than 95:5.

NATO, in the interests of stability, confidence building, and improved diplomatic relations might be willing to sacrifice some of its advantages in the Baltic Sea, especially as it is unclear if such overwhelming naval capabilities are essential to offense or defense given advantages in airpower, strategic depth, and difficulties Russia might face in conducting amphibious operations (Baev 2023; Gapiński, Kulesza, and Muzyka 2023). Thus, NATO might reasonably tolerate a 66:33 ratio, for example.

Implementation and Delegation

Two important aspects of implementation are verification and implementation management. Verification measures include a combination of national intelligence collection, on-site inspections, state reporting, and remote monitoring. There are three broad approaches to monitoring and verification: state-based "good faith", state-based multilateral intrusive inspections, and delegated implementation. In the first, which was the approach adopted for the interwar naval agreements, states did not establish a formal system of inspection. Rather, they relied on espionage, open sources, and good faith. After the Second World War, intrusive measures became more commonplace, with state parties sending inspectors to one another's military facilities. The management of the arms control treaties, however, was by the state parties themselves. In the case of several agreements, a coordinative body was created (such as the CFE Treaty's Joint Consultative Group (JCG)). This body was legally established as part of the agreement, but it was composed of national representatives who met to discuss administrative, technical and coordinative issues. Disputes could be raised in the JCG, but the JCG itself did not conduct monitoring or verification activities and did not assess compliance.

Other agreements, such as the Organization for Security and Cooperation in Europe's (OSCE) role in implementing the 2015 Minsk Agreements for the reduction in hostilities in Ukraine, involved a neutral, third-party implementer. The OSCE was charged with a full range of monitoring and verification functions, which included over 1000 staff members, many of whom were based in Ukraine on both sides of the line of contract (OSCE 2021). The OSCE issued compliance reports but did not have an enforcement mandate.

The Lausanne Treaty for the Straits established the Straits Commission which was charged with collecting information about naval vessels in the Black Sea, sharing this information with all states concerned, and "to see that the provisions relating to the passage of warships and military aircraft are carried out," ("The Convention

Relating To The Regime Of The Straits And Turkey" 1923, art. 15). The agreement also established a commission to verify defortification along the Turkish Straits. In practice, the commissions were only minimally active, perhaps due to a lack of violations and because of Türkiye's desire to be in control of the straits. With the Montreux Convention's entry into force, the commissions were dissolved, and Türkiye assumed full responsibilities for monitoring, verification, and enforcement.

A notable difference between the Montreux Convention and other CAC agreements is that Türkiye has substantial capabilities to enforce the agreement due to the straits running through its territory. In contrast, most CAC agreement violations occur in opposing states' national territory, outside of the control of the state(s) making any accusations of violations. For example, the US had no means to enforce Russian compliance with the INF Treaty when Washington accused Russia of testing a prohibited conventional land-based cruise missile. The US's only means of compelling enforcement was through diplomacy.

An important caveat on CAC agreement enforcement, however, is necessary. States or their supranational agreement implementors may be able to enforce discriminatory, post-conflict agreements when the victorious states occupy the defeated states or are otherwise willing to use force to enforce the agreements. One of the clearest examples of this are the post-World War Two Allied Control Councils and Commissions (ACCs) set up in the defeated Axis states. These had the backings of the occupation armies to ensure compliance with agreements. In the case of the much narrower agreement that ended the 1999 Kosovo conflict, the agreement authorized NATO to enforce the demilitarized zone by force.

The geography of the Turkish Straits permits, and the Montreux Convention implicitly authorizes Türkiye to enforce rules concerning the passage of the Straits. As recently demonstrated due to the Russo-Ukraine War, Türkiye unilaterally decides which naval vessels are and are not permitted to pass through the straits. Aside from diplomatic costs, violators risk military action in an extremely tactically disadvantageous position. Of course, for Türkiye to attack a state with whom they are otherwise not at war would be extreme. But other measures could be undertaken, including the non-provision of a pilot and non-cooperation from traffic control authorities. The Straits, which may have difficult navigational natural, marine, and man-made obstacles, might be risky to pass through if authorities erect non-destructive barriers such as obstacles or do not offer navigational assistance ("Note on the Turkish Straits," n.d.).

The agreement execution body options available for a Baltic Sea agreement can be any of the three approaches mentioned above. A purely state-based approach with no agreement executor would likely disadvantage Russia as Russia has no control over the Danish Straits, and they (as well as other states) would face the complicated factor that the straits run through two states instead of one. With Sweden and Denmark

being NATO members, Russia may not trust their objectivity in implementing the agreement. While Türkiye is also a NATO member, perceptions of it being a fair custodian of the straits going back to Türkiye's foundation likely alleviate concerns about Türkiye's objectivity. Russia might have less faith in Denmark and Sweden's goodwill. This approach, however, ruffles the least sovereignty feathers. States engage in traditional bilateral and multilateral diplomacy without the perceived interference of a treaty executor, however weak.

Still, a weak agreement executor is not without its advantages, which the JCG demonstrated. As a standing forum, it can efficiently coordinate information exchange, deal with disputes to some extent, and resolve technical questions in a way that can be accepted by all state parties. A standing body would develop institutional knowledge, experience, and norms especially if the same group of experts regularly assemble (Finnemore 1993).

A strong agreement executor and neutral body such as the OSCE or United Nations (UN) (which was charged with implementing weapons of destruction disarmament in Iraq, for example) has the advantage of being perceived as *relatively* fair and objective (compared to an adversaries' state organs or alliances performing inspections and assessments). Depending on its mandate and how it is structured, it may also be endowed with considerable resources, as in the case of the OSCE Special Monitoring Mission (SMM) in Ukraine or the European Union Monitoring Mission (EUMM) in Georgia, to execute the agreement's mission.

One advantage of an empowered, delegated treaty executor is that it is likely more adaptable – if the agreement is written to incorporate adaptability – than either of the other two approaches, which are more likely to require a whole renegotiation of the agreement. CAC agreements can only, at best, reflect military capabilities and technologies at the time of signature, but military capabilities evolve continuously. In the case of the Montreux Convention, for example, it had not anticipated armed, converted merchant vessels (Seydi and Morewood 2005). Similarly, some of the limits are based on gun caliber, which is no longer relevant to modern surface combatants. Türkiye's monopoly over the Montreux Convention's enforcement – a relatively unique situation amongst CAC agreements – likely facilitates agreement adaptability and evolution.

An agreement implementer could be charged with adapting the agreement based on changes in military technologies and geopolitical changes such as alliance memberships (Lippert 2023a). Indeed, agreement adaptation potential may be an important component of agreement survivability. Agreements that do not adapt to technological or geopolitical changes – both of which occur over the lifetime of CAC agreements – may easily become irrelevant. This irrelevance may be because they are no longer effective in addressing the problem they were designed to address, such the CFE Treaty's relevancy struggles following the dissolution of the Warsaw Pact when the

agreement had been conceived specifically to prevent a NATO-Warsaw Pact conflict; or because one or several parties no longer view the agreement as in their interests, such as the Russian perception of the INF Treaty's limitations on conventional, land-based, medium-range missiles due to perceptions of overwhelming NATO long-range precision strike capability (Kühn and Péczeli 2017).

Kühn (2015) emphasizes that adaptability is one of the three main factors of institutional success in arms control agreements (the other two being courtesy and clarity). Debre and Dijkstra (2021) note, for example, that international organizations – which conceptually include CAC agreement executors, though these are not specifically mentioned in their study – are more survivable when they are larger and more flexible. On the other hand, international organizations with very narrow mandates – which may characterize some CAC agreement executors – may be unable to adapt. This would suggest that an organization such as the OSCE is more survivable and adaptable compared to a narrow CAC body such as the CFE Treaty's JCG – which is largely borne out by the fact that the OSCE continues to function (albeit with substantial handicaps due to NATO-Russian rivalries (Hill 2023) while the JCG is *de facto* disbanded due to most state parties having suspended participation (Alberque 2023).

Conclusion

This article's underlying theme is that another war in Europe should be prevented and that preventing wars is about creating the conditions in which states view war as more costly than beneficial (Hausken 2016). CAC accomplishes this by stabilizing the military balance and reducing, if not eliminating, arms racing (Baliga and Sjöström 2004; Downs, Rocke, and Siverson 1985; Gray 1971). CAC also offers a forum for improving diplomatic relations, both through the process of negotiating agreements and in implementing the agreement. A successful CAC agreement helps to build trust and confidence between rivals and, ideally, removes some sources of dispute that can lead to conflict.

This article suggests that an effective CAC regime in the Baltic Sea can accomplish these goals. The article offers several approaches, indicating some of their advantages, disadvantages, and impacts. There is no singular approach to CAC agreements that assures success or failure. Over the past 100 years, CAC agreements have been varied and have met different levels of success. However, the relative success of the Lausanne and Montreux agreements, which have collectively surpassed 100 years of implementation, suggests that a similar approach to the Baltic Sea might be successful. The Lausanne/Montreux agreements survived several major historical periods: the interwar years, World War Two, the Cold War, and the post-Cold War decades – and still function amidst the Russo-Ukraine War. Surviving through these periods demonstrates that even if the agreement was intended for a certain

geopolitical situation, it retained its relevance despite significant changes in Europe. A Baltic Sea agreement designed for a second Cold War might similarly maintain relevance and durability.

A Baltic Sea CAC agreement, whether it imposes access controls, establishes naval inventory and capability limits, or both, is unlikely to do more harm than good for all the state parties. Russia finds itself significantly outnumbered, out-tonned, and out-missiled by NATO. Thus, they should welcome any opportunity to limit NATO naval forces, whether this is by locking in a fixed ratio of Russian and NATO navy ships and/or reducing non-Baltic Sea naval capabilities from entering the Baltic.

NATO's Baltic Sea CAC interest lies in preventing arms racing, which, even if it could prevail, would still require funds that might otherwise be better spent, and in improving diplomatic relations with Russia. The Russo-Ukraine War has shattered mutual trust. A Baltic Sea CAC agreement could be one brick in rebuilding a stable security foundation. Even if such an agreement might only slightly contribute to preventing another large-scale European conflict, the costs of the war in Ukraine suggest that all efforts should be undertaken to avoid a second 21st-century European war.

The author did not receive any funding for this study.

References

Alberque, William. 2023. "NATO Allies Fully Suspend Implementation of the CFE Treaty." IISS. https://www.iiss.org/online-analysis/online-analysis/2023/10/nato-allies-fully-suspend-implementation-of-the-cfe-treaty/#.

AP News. 2024. "Baltic Sea Nations React Warily to a Reported Russian Proposal to Revise Its Maritime Border." https://apnews.com/article/baltic-sea-russia-security-border-fb9849dd556fa166f1135172c6935c9d.

Axe, David. 2023. "Ukrainian Bombers Just Blew Up Another Russian Warship. 'Russia's Fleet Is Getting Smaller And Smaller!'" Forbes. https://www.forbes.com/sites/davidaxe/2023/12/26/ukrainian-bombers-just-blew-up-another-russian-warship-russias-fleet-is-getting-smaller-and-smaller/.

Baev, Pavel. 2023. "Russia's New Challenges in the Baltic/Northern European Theater." Notes de L'Ifri 130. Russie.Eurasie.Visions. Paris: French Institute of International Relations (Ifri).

Bagot, Charles, and Richard Rush. 1817. "British-American Diplomacy : Exchange of Notes Relative to Naval Forces on the American Lakes." The Avalon Project. https://avalon.law.yale.edu/19th_century/conv1817.asp.

Baliga, Sandeep, and Tomas Sjöström. 2004. "Arms Races and Negotiations." *Review of Economic Studies* 71:351–69.

Brooks, James. 2022. "Swedish, US Troops Drill on Remilitarized Baltic Sea Island." Military Times. https://www.militarytimes.com/news/your-military/2022/06/12/swedish-us-troops-drill-on-remilitarized-baltic-sea-island/.

Burns, Richard Dean, and Donald Urquidi. 1968. *Disarmament in Perspective: Volume 4: Conclusions*. Vol. 4. Los Angeles: California State College at Los Angeles Foundation.

Buzhinskiy, Evgeny, and Oleg Shakirov. 2019. *Outlines for Future Conventional Arms Control in Europe: A Sub-Regional Regime in the Baltics*. London, UK: European Leadership Network (ELN).

"Chapter Five: Russia and Eurasia." 2022. *The Military Balance* 122 (1): 164–217. https://doi.org/10.1080/04597222.2022.2022930.

"Chapter Four: Russia and Eurasia." 2025. *The Military Balance* 125 (1): 152–205. https://doi.org/10.1080/04597222.2025.2445476.

"Chapter Three: Europe." 2025. *The Military Balance* 125 (1): 52–151. https://doi.org/10.1080/04597222.2025.2445475.

Charap, Samuel, Alice Lynch, John Drennan, Dara Massicot, and Giacomo Persi Paoli. 2020. *A New Approach to Conventional Arms Control in Europe: Addressing the Security Challenges of the 21st Century*. RAND Corporation. https://doi.org/10.7249/RR4346.

Claeys, Suzanne, and Heather W. Williams. 2022. "War and Arms Control: When to Pursue Cooperation." *Survival* 64 (6): 137–52. https://doi.org/10.1080/00396338.2022.2150432.

Dahlstrand, Katherine E. 2024. "Achieving the Promise of NATO's New Northeast Quadrant." Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/12/achieving-the-promise-of-natos-new-northeast-quadrant?lang=en.

Deaton, James Paul. 1975. *The Significance of International Straits to Soviet Naval Operations*. Monterey: Naval Postgraduate School.

Debre, Maria Josepha, and Hylke Dijkstra. 2021. "Institutional Design for a Post-Liberal Order: Why Some International Organizations Live Longer than Others." *European Journal of International Relations* 27 (1): 311–39. https://doi.org/10.1177/1354066120962183.

Denmark. 1999. "Ordinance Governing the Admission of Foreign Warships and Military Aircraft to Danish Territory in Time of Peace."

Downs, George W, David M Rocke, and Randolph M. Siverson. 1985. "Arms Races and Cooperation." *World Politics* 38 (1): 118–46.

Dyer, Evan. 2023. "NATO's Latest Moves Could Bottle up Much of Russia's Naval Power." CBC. July 20, 2023. https://www.cbc.ca/news/politics/russia-ukraine-black-sea-baltic-naval-1.6911530.

Engvall, Johan, Gudrun Persson, Robert Dalsjö, Mike Winnerstig, and Carolina Vendil Pallin. 2018. *Conventional Arms Control - A Way Forward or Wishful Thinking?* FOI.

Finnemore, Martha. 1993. "International Organizations as Teachers of Norms: The United Nations Educational, Scientific, and Cultural Organization and Science Policy." *International Organization* 47 (4): 565–97. https://doi.org/10.1017/S0020818300028101.

Gapiński, Miłosz, Ireneusz Kulesza, and Konrad Muzyka. 2023. "Ocean Shield 2023: The Baltic Fleet's Perspective." Rochan Consulting.

Gray, Colin S. 1971. "The Arms Race Phenomenon." *World Politics* 24 (1): 39–79. https://doi.org/10.2307/2009706.

Hausken, Kjell. 2016. "Cost Benefit Analysis of War." *International Journal of Conflict Management* 27 (4): 454–69. https://doi.org/10.1108/IJCMA-04-2015-0023.

Helsinki Commission. n.d. *Report on Shipping Accidents in the Baltic Sea Area for the Year 2008*.

Hill, William H. 2023. "The OSCE Approaching Fifty: Does the Organization Have a Future?" In *OSCE Insights 2022*, edited by Institute for Peace Research and Security Policy at the University of Hamburg, 1–10. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748933625-01.

"Implementation of the Montreux Convention." n.d. Republic of Türkiye Ministry of Foreign Affairs. Accessed July 24, 2023. https://www.mfa.gov.tr/implementation-of-the-montreux-convention.en.mfa.

Isachenko, Daria. 2023. *Turkey in the Black Sea Region: Ankara's Reactions to the War in Ukraine against the Background of Regional Dynamics and Global Confrontation*. Vol. SWP Research Paper 12. Berlin: Stiftung Wissenschaft und Politik: German Institute for International and Security Affairs. https://www.swp-berlin.org/10.18449/2023RP12/.

Kacprzyk, Artur, and Łukasz Kulesa. 2020. *Dilemmas of Arms Control: Meeting the Interests of NATO's North-Eastern Flank*. Tallinn, Estonia: International Centre for Defence and Security.

Kayali, Laura. 2023. "Sorry Russia, the Baltic Sea Is NATO's Lake Now." *POLITICO* (blog). https://www.politico.eu/article/nato-lake-what-sweden-and-finland-will-change-in-the-baltics-russia-ukraine-war/.

Kucukgocmen, Ali, and Huseyin Hayatsever. 2024. "Turkey, Romania, Bulgaria Sign Deal to Clear Floating Black Sea Mines | Reuters." Reuters. https://www.reuters.com/world/turkey-romania-bulgaria-ink-deal-clear-floating-black-sea-mines-2024-01-11/.

Kühn, Ulrich. 2015. "Institutional Resilience, Deterrence and the Transition to Zero Nuclear Weapons." *Security and Human Rights* 26 (2–4): 262–80. https://doi.org/10.1163/18750230-02602002.

———. 2020. *The Rise and Fall of Cooperative Arms Control in Europe*. 1st ed. Demokratie, Sicherheit, Frieden. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748903239.

Kühn, Ulrich, and Anna Péczeli. 2017. "Russia, NATO and the INF Treaty." *Strategic Studies Quarterly* 11 (1): 66–99.

Kvartalnov, Artem. 2021. "Indivisible Security and Collective Security Concepts: Implications for Russia's Relations with the West." *Central European Journal of International and Security Studies* 15 (3): 4–29. https://doi.org/10.51870/CEJISS.A150301.

Labrenz, Robert. 2023. "Drill Emission Control as a Main Battery." *U.S. Naval Institute* 149 (6). https://www.usni.org/magazines/proceedings/2023/june/drill-emission-control-main-battery.

Lippert, William. 2023a. "A European Military Balance Organization and Dynamic Conventional Arms Control." *Bulletin of "Carol I" National Defense University* 12 (3): 41–59. https://doi.org/10.53477/2284-9378-23-31.

———. 2023b. "The Role Of The European Union In Future Conventional Arms Control In Europe." Presented at the EUACADEMY Conference "European Security: Challenges And Policies," Dublin, Ireland, December 15.

———. 2024a. "Conventional Arms Control and Ending the Russo-Ukrainian War." War on the Rocks. https://warontherocks.com/2024/10/conventional-arms-control-and-ending-the-russo-ukrainian-war/.

———. 2024b. "How Conventional Arms Control Failures Caused the Russo-Ukraine War." *Defense & Security Analysis*, January, 1–23. https://doi.org/10.1080/14751798.2024.2300889.

Livermore, Doug. 2024. "NATO's Baltic Build-Up." CEPA. https://cepa.org/article/natos-baltic-build-up/.

Mazarr, Michael J., Samuel Charap, Abigail Casey, Irina A. Chindea, Christian Curriden, Alyssa Demus, Bryan Frederick, et al. 2021. *Stabilizing Great-Power Rivalries*. Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/RR-A456-1.

NATO. 2021. "Statement by the North Atlantic Council on the Treaty on Open Skies." NATO. June 18, 2021. http://www.nato.int/cps/en/natohq/news_184840.htm.

Nelson, Amy J., and Adam Twardowski. 2022. "How the Demise of an Arms Control Treaty Foreshadowed Russia's Aggression against Ukraine." *Bulletin of the Atomic Scientists* (blog). https://thebulletin.org/2022/02/how-the-demise-of-an-arms-control-treaty-foreshadowed-russias-aggression-against-ukraine/.

Newsweek. 2023. "Sweden Joining NATO Is a Nightmare for Russia's Baltic Sea Fleet." https://www.newsweek.com/russia-nato-sweden-baltic-sea-finland-1812526.

"Note on the Turkish Straits." n.d. Republic of Türkiye Ministry of Foreign Affairs. Accessed January 22, 2024. https://www.mfa.gov.tr/the-turkish-straits.en.mfa#.

"Notification Requirements." n.d. Deutsche Flagge. Accessed January 21, 2024. https://www.deutsche-flagge.de/en/pscen/notification.

Office of Naval Intelligence. 2015. *The Russian Navy: A Historic Transition*. Suitland, MD: US Navy.

Ogura, Junko. 2021. "Japanese Submarine Collides with Commercial Ship While Surfacing in Pacific." CNN. https://www.cnn.com/2021/02/08/asia/japan-submarine-collision-intl-hnk-scli/index.html.

O'Neill, Barry. 1991. "Rush-Bagot and the Upkeep of Arms Treaties." *Arms Control Today* 21 (7): 20–23. http://www.jstor.org/stable/23624556.

OSCE. 2021. *A Peaceful Presence - The First Five Years of the OSCE Special Monitoring Mission to Ukraine*. Vienna: OSCE Conflict Prevention Centre. https://www.osce.org/secretariat/491220.

Overfield, Cornell. 2022. "Turkey Must Close the Turkish Straits Only to Russian and Ukrainian Warships." Lawfare. https://www.lawfaremedia.org/article/turkey-must-close-turkish-straits-only-russian-and-ukrainian-warships.

Peck, Michael. 2019. "Why a Battlecruiser Is No Battleship: High Speed and Firepower, but No Armor." Text. The National Interest. The Center for the National Interest. https://nationalinterest.org/blog/buzz/why-battlecruiser-no-battleship-high-speed-and-firepower-no-armor-82871.

Perrin de Brichambaut, Marc. 2010. "The Indivisibility of Euro-Atlantic Security." OSCE.

Portela, Clara. 2021. *The EU's Arms Control Challenge: Bridging Nuclear Divides*. Chaillot Paper, 166 (April). Paris: European Union Institute for Security Studies (EUISS). https://doi.org/10.2815/601066.

Reuters. 2023. "Baltic Sea Drills to Focus for First Time on Repelling Russian Attack." https://www.reuters.com/world/europe/baltic-sea-drills-focus-first-time-repelling-russian-attack-2023-09-01/.

———. 2024. "Turkey to Block Minehunter Ships Intended for Ukraine." https://www.reuters.com/world/middle-east/turkey-block-uk-minehunter-ships-intended-ukraine-2024-01-02/.

Richter, Wolfgang. 2016. *Sub-Regional Arms Control for the Baltics: What Is Desirable? What Is Feasible?* Deep Cuts Working Paper 8. Hamburg, Germany: Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH).

Rosa-Hernández, Gabriela. 2023. "How Russia's Retreat from the Vienna Document Information Exchange Undermines European Security." *Bulletin of the Atomic Scientists* (blog). https://thebulletin.org/2023/03/how-russias-retreat-from-the-vienna-document-information-exchange-undermines-european-security/.

Savitz, Scott, and Isabelle Winston. 2024. "A Brief Naval Overview of the Baltic Sea Region." Expert Insights. Santa Monica, CA: RAND Corporation.

Schelling, Thomas C. 1975. "A Framework for the Evaluation of Arms-Control Proposals." *Daedalus* 104 (3): 187–200.

Seydi, Süleyman. 2010. *The Turkish Straits and the Great Powers : From the Montreux Convention to the Early Cold War, 1936-1947*. Analecta Isisiana: Ottoman and Turkish Studies. Piscataway, NJ: Gorgias Press. https://doi.org/10.31826/9781463225506.

Seydi, Süleyman, and Steven Morewood. 2005. "Turkey's Application of the Montreux Convention in the Second World War." *Middle Eastern Studies* 41 (1): 79–101. https://doi.org/10.1080/0026320042000322725.

Shape.Nato.Int. 2025. "Baltic Sentry to Enhance NATO's Presence in the Baltic Sea." https://shape.nato.int/news-releases/baltic-sentry-to-enhance-natos-presence-in-the-baltic-sea.aspx.

Sweden. 1966. "Proclamation of 3 June 1966 Concerning the Admission to Swedish Territory of Foreign Naval Vessels and Military Aircraft."

Swistek, Göran, and Michael Paul. 2023. "Geopolitics in the Baltic Sea Region: The 'Zeitenwende' in the Context of Critical Maritime Infrastructure, Escalation Threats and the German Willingness to Lead." 9. SWP Comment. Berlin: Stiftung Wissenschaft und Politik: German Institute for International and Security Affairs.

"The Convention Relating To The Regime Of The Straits And Turkey." 1923. Lausanne.

UCA Kiel. 2023. "Kiel Canal." https://www.kiel-canal.de/.

Ünlü, Nihan. 2002. *The Legal Regime of the Turkish Straits*. Brill | Nijhoff. https://doi.org/10.1163/9789004481343.

Zellner, Wolfgang, Olga Oliker, and Steven Pifer. 2020. "A Little of the Old, a Little of the New: A Fresh Approach to Conventional Arms Control in Europe." 11. Deep Cuts Issue Brief. Hamburg, Germany: Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH).

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

NATO opportunities in the MENA region in the context of the Russian threat

Teodora-Ioana MORARU, Master Student*

* "Mihai Viteazul" National Intelligence Academy, Bucharest
e-mail: banu.teodora@animv.eu

Abstract

The Middle East and North Africa (MENA) region represents a geopolitical space marked by instability, strategic competition and the influence of global actors, including the Russian Federation, which has strengthened its presence through economic and military partnerships, as well as information influence campaigns. In this context, the North Atlantic Treaty Organization (NATO) can adopt new strategies to expand its engagement in the region, aiming to counter these dynamics and reduce Russia's ability to destabilize Euro-Atlantic security.

This study employs prospective analysis methods, specifically the RVAP-O framework (Risks, Vulnerabilities, Threats and Opportunities) to identify the main challenges and possible courses of action in the MENA region and the environmental scanning/horizon scanning (ES/HS) method to assess their short-term impact. Thus, the research examines the extent to which NATO's involvement in MENA can alter the balance of power and reshape the Russian Federation's strategic priorities, thereby limiting its operational capabilities in the Euro-Atlantic space.

Keywords:
NATO; MENA; Russian Federation; Euro-Atlantic security; prospective study.

Article info
Received: 10 February 2025; Revised: 28 February 2025; Accepted: 4 March 2025; Available online: 2 April 2025

Citation: Moraru, T.I. 2025. "NATO opportunities in the MENA region in the context of the Russian threat". *Bulletin of "Carol I" National Defence University*, 14(1): 74-89. https://doi.org/10.53477/2284-9378-25-05

The Middle East and North Africa (MENA) represent an epicentre of global geopolitical dynamics, characterized by high strategic complexity and multiple challenges to international security. The region is marked by phenomena such as the expansion of extremist ideologies, the transnational terrorist threat, drug trafficking and risks associated with weapons of mass destruction. Simultaneously, political instability and internal fragmentation affect numerous states, such as Iraq and Afghanistan, while others, including Pakistan and Lebanon, are exposed to internal tensions that could escalate into civil conflicts. Even in states considered relatively stable, the persistence of ethnic and sectarian divisions constitutes vulnerability factors with destabilizing potential.

Against this backdrop, MENA remains a space where strategic competition among global powers such as the United States of America (USA), Russia and China is particularly intense, with each seeking to strengthen its influence in the region. The North Atlantic Treaty Organization (NATO), as a fundamental actor in the Euro-Atlantic security architecture, maintains its interest in regional stability, especially as the Russian threat to the European continent necessitates a reassessment of strategic priorities.

In this context, the present research aims to identify the opportunities that NATO can leverage in the MENA region, considering the evolution of security risks and challenges, as well as their impact on European security. The study employs qualitative analysis methods, specifically the RVAP-O framework (Risks, Vulnerabilities, Threats, Dangers and Opportunities), which enables a systematic assessment of regional security dynamics and the environmental scanning/horizon scanning (ES/HS) method, which explores the potential impact of NATO's actions in the region. This methodological approach will facilitate not only a deeper understanding of emerging risks but also the identification of possible strategic courses of action for NATO in MENA.

1. Geopolitical context

During the Cold War, various dominant political and ideological movements in the Arab world significantly contributed to shaping a negative perception of NATO among the states and populations of the region (Liteanu, Degeratu and Toma 2007, 162-167). The Arab nationalist movement, the Arab socialist movement, leftist and communist groups, along with Islamist organizations, have historically been and continue to be political forces strongly opposed to the West and, by extension, to NATO. Additionally, many of these groups developed ideological affinities with the former Union of Soviet Socialist Republics (USSR) and the member states of the Warsaw Pact, which were perceived as a counterbalance to Western influence in the region. These sympathies materialized through diplomatic, economic and military support provided by the Soviet Union to certain Arab regimes, including Gamal

Abdel Nasser's government in Egypt, Hafez al-Assad's administration in Syria and Ahmed Ben Bella's leadership in Algeria, as well as through the adoption of socialist-oriented policies in Arab states such as Iraq, Libya and Sudan.

Although NATO established itself as an organization with both political and military dimensions, its image during the Cold War was largely associated with Western interventions in former European colonies. For example, the Suez Crisis of 1956 (US Department of State 2017b), in which France and the United Kingdom, alongside Israel, launched a military intervention in Egypt to regain control of the Suez Canal, nationalized by Nasser's regime, was perceived in the Arab world as an imperialist action, despite NATO as an organization not being directly involved. Additionally, Western support for Israel in the Arab-Israeli conflicts, particularly during the Six-Day War in 1967 (Lorch 2008, 1-8), reinforced the perception that NATO and its member states supported Western hegemony in the Middle East to the detriment of Arab states. This perception was further amplified by the propaganda of socialist states and pan-Arab movements, which portrayed NATO as an instrument of Western imperialism and neocolonialism (Droin, et al. 2024).

During the Cold War, NATO focused primarily on defending the Euro-Atlantic territory and deterring the USSR, without significant involvement in strategic communication campaigns in Arab states. As a result, the Alliance's perception in the MENA region was shaped by external factors, and its image was often influenced by nationalist and anti-Western rhetoric (Baban 2018, 351–357) promoted by certain regimes and ideological movements.

Subsequently, NATO placed public diplomacy among its priorities, particularly after the September 11, 2001 attacks, amid intensified efforts to counter radicalization and negative perceptions associated with Western presence in the Middle East and North Africa. In this regard, the Alliance launched initiatives such as the Mediterranean Dialogue in 1994 (NATO 2024b) and the Istanbul Cooperation Initiative in 2004 (NATO 2024a), aimed at strengthening relations with countries in the region and fostering a better understanding of its strategic objectives. However, the impact of these initiatives remained limited, primarily due to the sensitive political context and persistent suspicions toward Western interventions in the Arab world.

NATO's perception in the MENA region is shaped by historical and geopolitical factors, often being associated with the strategic interests of the West, particularly those of the USA. Unlike other international alliances, where decisions are frequently dominated by the most powerful members, NATO operates through a collective decision-making mechanism, involving all its allies in the development of security policies and strategies (NATO 2023). However, in the Arab world, the perception persists that NATO serves as a tool for projecting American power, a viewpoint reinforced by the role the United States has played in military interventions in the region.

This perception is not exclusive to the MENA region but is also present within public opinion, where debates persist regarding the predominant influence of the USA over NATO's decision-making process (Ivanov 2011, 242). In Arab states, this view is further amplified by a climate of scepticism and a tendency to interpret international events through the lens of conspiracy theories.

Although ten member states of the Arab League have joined NATO's cooperation initiatives with the MENA region, their objectives and impact remain insufficiently understood both at the level of political elites and among the Arab public. The Mediterranean Dialogue, launched in 1994, includes seven partner states, six of which are members of the Arab League: Algeria, Egypt, Jordan, Mauritania, Morocco and Tunisia (NATO 2024b). The Istanbul Cooperation Initiative, launched in 2004, was adopted by four Gulf Cooperation Council states: Bahrain, Kuwait, Qatar and the United Arab Emirates (NATO 2024a). Despite this formal commitment, NATO has not managed to clearly communicate the tangible benefits of these partnerships (Zara 2006, 146-148), reinforcing the perception that the Alliance's involvement in the region remains limited and lacks a well-defined strategic direction.

NATO's lack of a clear direction in the MENA region generates uncertainty regarding its role and its ability to influence political and security developments. Additionally, concepts such as "dialogue," "initiative," and "partnership" are often perceived as vague in the absence of concrete results that demonstrate the impact of these collaborations on regional security. In this context, the European Union (EU) enjoys a more favourable perception among regional actors (EEAS 2021), due to its diplomatic approach and involvement in strategic negotiations, without being directly associated with military interventions. A relevant example is the EU's role in managing the Iranian nuclear dossier, where it acted as a mediator in the negotiations that led to the Joint Comprehensive Plan of Action (JCPOA), signed in 2015 between Iran and the five permanent members of the United Nations Security Council (US Department of State 2017a).

In this process, the EU facilitated dialogue, implemented and later eased the economic sanctions imposed on Iran, while also monitoring compliance with the agreement alongside the International Atomic Energy Agency (IAEA). Following the USA's withdrawal from the JCPOA in 2018, the EU sought to maintain the agreement through alternative mechanisms, such as the Instrument in Support of Trade Exchanges (INSTEX) (European Parliament 2023), designed to facilitate trade with Iran without relying on the US dollar.

A key aspect of the research documentation is that the Gulf Cooperation Council states that have joined the Istanbul Cooperation Initiative – Bahrain (Bureau of Near Eastern Affairs 2022), Kuwait (US Embassy in Kuwait 2025), Qatar (Bureau of Near Eastern Affairs 2020a) and the United Arab Emirates (Bureau of Near Eastern Affairs 2020b) – already benefit from institutionalized security partnerships and

military cooperation with the USA. These bilateral agreements cover areas such as counterterrorism, the prevention of weapons of mass destruction proliferation, defence planning assistance, military training and exercises, border security and critical infrastructure protection. Given the overlap between these commitments and NATO's objectives in the region, the general perception is that the Alliance has yet to define a distinct and autonomous role in relation to US initiatives.

2. Methodological approach

The purpose of this research is to identify the opportunities that NATO can leverage in the MENA region in the context of the threat posed by the Russian Federation to Euro-Atlantic security and, subsequently, to assess its potential impact on the security landscape.
Therefore, the main research objective is *determining the optimal course of action for NATO to strengthen its strategic position in MENA in order to counter the Russian threat to Euro-Atlantic security*.

This objective is supported by two specific research objectives:

- *Identifying the opportunities that NATO can exploit in MENA to consolidate its influence*;
- *Establishing the optimal course of action for NATO in MENA to counter the threat posed by the Russian Federation in the Euro-Atlantic space, while maintaining stable relations with regional partners*.

The research objectives will be addressed through the following research questions:

- *What opportunities can NATO leverage in the MENA region to expand its influence?*
- *What is the optimal course of action for NATO in the MENA region to limit Russia's capacity to project strategic influence in the Euro-Atlantic space?*

In this context, the research aims to identify the opportunities that NATO can leverage in the MENA region, considering the evolution of security risks and challenges, as well as the short-term impact on European security. The study employs qualitative analysis methods, specifically the RVAP-O framework (Risks, Vulnerabilities, Threats, Dangers and Opportunities), which will allow for a systematic assessment of regional security dynamics, and the environmental scanning method, which will explore the potential impact of NATO's actions in the region.

From a data collection standpoint, the analysis relies on official sources and institutionally validated strategic documents, including reports produced by NATO, the EU, and the US on emerging global trends and recent geopolitical developments in the MENA region. For a comprehensive perspective on the geostrategic context, these sources were complemented by academic analyses and open-source materials,

such as specialized articles and media reports, used strictly for contextualization and for verifying data correlations. To ensure that research remains relevant, the timeframe under examination is limited to the past five years (2019–2024), thus allowing for an assessment of recent trends and the short-term impact of NATO's strategies in the region.
The analysis of the relationship between MENA states and NATO or Russia is conducted across three dimensions: diplomatic, military, and economic. Each dimension is examined through a set of specific variables tied to relevant indicators.

Within the diplomatic dimension, the targeted indicator is the relation between MENA states and NATO or Russia, analyzed through two variables. The first variable, the effectiveness of regional cooperation mechanisms, is reflected in the capacity of regional structures to manage crises, the influence of internal rivalries on decision-making processes, and the coherence of regional organizations in relation to global actors. The second variable, the institutional relation with NATO and Russia, is analyzed in terms of the consistency of security commitments made to these two actors, the impact of foreign policy changes on how MENA states position themselves, and the general trends in their strategic orientation.

Within the military dimension, the targeted indicator is the dependence of MENA states on NATO or Russia for ensuring security and defence, examined through two variables. The first, the role of arms imports in defining strategic partnerships, considers the predominant direction of military equipment acquisitions, patterns of military cooperation, and technological transfer between MENA states and NATO or Russia. The second variable, the link between non-state actors and external military support, analyzes how the actions of these groups influence MENA states' reliance on external military assistance, as well as the support tendencies provided by NATO or Russia in contexts involving non-state actors.

From an economic standpoint, the targeted indicator is the degree of stability of internal economic markets in MENA states, assessed through two variables. The first, the level of economic dependence includes an examination of the structure of national economies in relation to key resources and dominant economic sectors, vulnerability to global economic factors, and the role of oil and gas resources in the economic framework of producer states. The second variable, economic support from NATO or Russia, addresses how reliance on external backing influences internal economic policies and considers the effects of strategic investments on the stability of local markets.

Building on the research methods employed, the analysis will be structured around two main directions. The first research direction focuses on the strategic assessment of the opportunities that NATO can leverage in the MENA region in the diplomatic, military and economic domains, based on the RVAP-O analytical framework developed by Deac and Grigoraș (2014, 62-70). This approach involves identifying

the key advantages that NATO can exploit to strengthen its position in relation to regional partners and to limit Russia's ability to maintain or expand its influence. In this context, the risks, vulnerabilities, threats and dangers stemming from the current status quo in the MENA region will be identified, followed by the determination of potential courses of action for NATO.

The second research direction aims to determine the optimal course of action for NATO in the MENA region, based on the environmental scanning method, with the goal of assessing the potential impact of different strategies adopted by the Alliance. This approach will allow for an analysis of how NATO can engage in MENA while maintaining relations with regional partners and avoiding the escalation of geopolitical tensions, with the ultimate objective of countering the Russian Federation's influence in the Euro-Atlantic space and enhancing deterrence. Based on the identified opportunities, action plans will be developed, serving as potential events. Subsequently, possible consequences and their impact on the geopolitical landscape will be assessed.

The RVAP-O analytical framework (Deac and Grigoraș 2014, 62-70) was developed to provide a coherent analytical structure for the concept of national security strategy. Thus, after identifying risks, vulnerabilities, threats and dangers, the authors propose establishing action opportunities, a key aspect that can facilitate the mitigation of the previously identified challenges. This instrument has proven effective in analyzing conflict dynamics and strategic planning, offering valuable insights for anticipating potential outcomes.

The environmental scanning method can be defined as "a process of collecting data and information about specific events and causal relationships that may influence the future of an organization" (Grigoraș 2022, 38). It is classified as a prospective estimation method, with viable applicability in the short term (up to five years). Initially, this method was used in strategic planning (Renfro 1993) to identify indicators of change. Thus, after assessing the initial results (courses of action), key determinant factors can be developed to support planning processes.

The research approach is based on a theoretical framework grounded in the concepts adopted by the Romanian state regarding vulnerabilities, risks, threats and dangers, as defined in the National Defense Strategy Guide for the 2015-2019 period (Administrația Prezidențială 2015, 7).

3. Assessing strategic opportunities

In this chapter, vulnerabilities, risks, threats and dangers in the MENA region will be analyzed from the diplomatic, military and economic perspectives. This analysis will be followed by a synthesis in tabular form, summarizing the main findings,

including NATO's potential opportunities, which could negatively impact Russia's ability to project power in the Euro-Atlantic space.

3.1. Vulnerabilities in the MENA Region

From a diplomatic perspective, the lack of an effective coordination mechanism undermines the diplomatic stability of MENA states. In the absence of functional cooperation structures, countries in the region fail to adopt unified positions in crisis management and their engagement with international actors (Trobbiani 2017, 25-30). Strategic orientations vary significantly, with some Gulf states maintaining close relations with the USA, while Algeria and Syria strengthen their partnerships with Russia and China, thereby weakening the effectiveness of regional diplomatic initiatives.

From a military perspective, the vulnerabilities of MENA states are shaped by their dependence on arms imports and limited domestic production capabilities. While Saudi Arabia and the United Arab Emirates continue to invest in the modernization of their armed forces, countries such as Libya, Yemen and Syria remain affected by prolonged conflicts, which have significantly weakened their autonomous defence capabilities (van den Bosch and Lindstaedt 2024, 376).

From an economic perspective, MENA states are vulnerable to fluctuations in oil and gas prices due to their dependence on hydrocarbon exports (Mezni and Nesrine 2022, 7-10). Gulf states, despite their vast resources, are striving to diversify their economies to mitigate exposure to energy market shocks, North African countries, such as Algeria and Egypt, face persistent economic challenges driven by population growth and political instability.

3.2. Risks in the MENA Region

From a diplomatic perspective, the increase in interstate tensions represents a significant risk in the MENA region. Political and strategic divergences between states such as Saudi Arabia and Qatar or Turkey and Egypt fuel regional competition and hinder the establishment of functional cooperation frameworks (Quero 2023, 114-116). These tensions weaken diplomatic mechanisms and heighten the risk of conflict escalation in the region.

From a military perspective, the arms race is an escalating trend in the MENA region, increasing the risk of conflict escalation. Gulf states, such as Saudi Arabia and the United Arab Emirates, have significantly increased their acquisitions of advanced weaponry (Vieira and Eslami 2023), while Iran continues to develop ballistic missile capabilities and electronic warfare systems.

Another significant military risk is the dependence on non-state actors in regional conflicts. Groups such as Hezbollah in Lebanon, the Houthi movement in Yemen and paramilitary forces in Libya are used as instruments of influence by states engaged in conflict (National Intelligence Council 2021, 86), and this weakens

central governments' control over internal security and facilitates the prolongation of conflicts.

From an economic perspective, the region faces significant risks, particularly due to its high dependence on external loans (Rustamov, Ozatac and Taspinar 2024, 107). The increasing pressure on national budgets restricts the ability of states to invest in development and security, which may further exacerbate social instability.

Another emerging risk is the instability of financial and commercial markets in the region, driven by regulatory fragmentation and political uncertainties. Foreign investors are reluctant to engage in long-term projects in countries such as Libya, Iraq and Syria (Muhamad and Khayyat 2024, 77-80), which hinders economic recovery and limits improvements in living standards in these states.

3.3. Threats in the MENA Region

From a diplomatic perspective, a significant threat is the intervention of major powers in the internal affairs of MENA states, which generates diplomatic instability (Ipsos 2023, 117). USA, Russia and China are strengthening their influence by supporting rival regimes or groups, undermining the sovereignty of states in the region and intensifying the polarization of international alliances.

From a military perspective, the proliferation of weapons of mass destruction still represents a major threat in the MENA region (National Intelligence Council 2008, 61-63). The expansion of nuclear capabilities and the development of armament programs by states such as Iran and Israel, along with the potential dissemination of nuclear technologies to non-state actors, escalate large-scale armed confrontation.

Additionally, the threat posed by extremist and paramilitary groups remains high. Dawla al-Islamiya fi al-Iraq wa al-Sham (Daesh), Hezbollah, the Houthi movement and other insurgent organizations continue to adapt (National Intelligence Council 2021, 107), utilizing modern technologies to carry out attacks and maintain control over unstable territories. The support provided to these groups further exacerbates conflicts and complicates their long-term resolution.

From an economic perspective, the threat posed by global competition for resources is increasing, driven by the involvement of major actors such as the Russian Federation, China and India, which are expanding their influence through the acquisition of strategic assets and investments in the region's energy infrastructure (Muhamad and Khayyat 2024, 75). This competition leads to market reconfiguration and economic pressure on MENA's producing states.

3.4. Dangers in the MENA Region

From a diplomatic perspective, a major danger is the increase in the number of unresolved conflicts (Moosa, Yasmin and Tamer 2024, 132), which hinders the

establishment of cooperation mechanisms and sustains diplomatic instability. As the Arab League and the Gulf Cooperation Council remain affected by internal rivalries and external powers intensify their influence, the region's ability to act in a unified manner is severely compromised.

From a military perspective, the escalation of indirect confrontations represents a major danger in the MENA region (Vieira and Eslami 2023, 369). State rivalries are intensified by competition for military superiority and the dependence on non-state actors to project influence. Amid the expansion of nuclear capabilities and the development of armament programs by states such as Iran and Israel, indirect confrontations are becoming increasingly difficult to control.

From an economic perspective, a significant danger is the intensification of economic and humanitarian crises caused by reduced access to resources (National Intelligence Council 2021, 71). Egypt, Sudan, and Algeria are experiencing severe economic deterioration, driven by limited access to food and water, which exacerbates migration and intensifies resource control disputes.

TABEL NO. 1

RVAP-O analysis results

	Intent	Non-intent	**Domain**
Internal environment	**RISKS**	**VULNERABILITIES**	
	- increasing interstate tensions	- lack of an effective coordination mechanism	Diplomatic
	- arms race - dependence on non-state actors in regional conflicts	- dependence on arms imports	Military
	- dependence on external loans - financial market instability	- dependence on hydrocarbon exports for producer states	Economic
	OPPORTUNITIES		
	- strengthening strategic partnerships through multilateral cooperation initiatives - enhancing strategic communication through a digital platform in Arabic, building on the precedent of protecting Muslim communities - strengthening cooperation in nuclear security and non-proliferation		
External environment	**THREATS**	**DANGERS**	
	- intervention of major powers	- increasing number of unresolved conflicts	Diplomatic
	- proliferation of weapons of mass destruction - intensification of extremist and paramilitary group activities	- escalation of indirect confrontations	Military
	- global competition for resources	- intensification of economic and humanitarian crises	Economic

As a result of the identified factors (see Table no. 1), one of the opportunities that NATO can leverage in MENA is strengthening strategic partnerships through multilateral cooperation initiatives, using the Mediterranean Dialogue and the Istanbul Cooperation Initiative as main platforms. Given the fragmentation of regional alliances and the inability of MENA states to adopt unified positions in the face of regional crises, NATO can facilitate dialogue between Arab states and its global partners, providing a stable framework for coordinating diplomatic and security initiatives. The Alliance could expand the role of these platforms by organizing periodic diplomatic forums, where NATO member states and those in MENA collaborate to address regional issues, such as counterterrorism, conflict management, or maritime security cooperation. In this way, NATO not only consolidates its influence in the region but also contributes to reducing the influence of other actors, such as the Russian Federation, which is trying to expand its strategic partnerships in MENA.

Another opportunity that NATO can leverage in the MENA region is enhancing strategic communication to consolidate its diplomatic position and counter the influence of global competitors. The creation of an official digital platform in Arabic, which would provide clear information about the Alliance's missions and objectives, would allow NATO to combat misinformation and correct negative perceptions, especially in a context where the Russian Federation is intensifying its efforts to influence public opinion in the region. By promoting a clear and transparent message, this initiative would facilitate dialogue with academic elites, security experts, and the media in MENA, contributing to the creation of a favourable framework for diplomatic cooperation. Strengthening NATO's presence in the regional information space could reduce the influence of other powers and support the consolidation of strategic partnerships.

Another opportunity that NATO can leverage in the MENA region is strengthening cooperation in nuclear security and non-proliferation, given the danger of the expansion of weapons of mass destruction programs and the risk of the dissemination of nuclear technologies to non-state actors. By enhancing monitoring and control mechanisms for nuclear materials and collaborating with regional partners, using the necessity of protecting Muslim communities as a favourable precedent – demonstrated through interventions in Bosnia-Herzegovina, Kosovo province, the Former Yugoslav Republic of Macedonia, and Afghanistan – NATO could contribute to reducing emerging threats. These initiatives would diminish the Russian Federation's influence over Arab states, reducing their dependence on Russia in terms of security and military technology, thereby reinforcing NATO's position as a strategic partner in the region.

4. Evaluation of strategies' impact

According to the second research direction, this chapter will evaluate the short-term impact of the implemented strategies and the opportunities previously identified using the RVAP-O framework.

The first step in evaluating the impact of NATO's strategies in the MENA region is identifying potential events, which, in this analysis, are represented by the strategic opportunities identified. This process is crucial for environmental scanning, as it allows the formulation of realistic scenarios based on the actions the Alliance might implement. In this regard, three major directions are identified as having significant potential for NATO's influence in the region.

Strengthening strategic partnerships through the Mediterranean Dialogue and the Istanbul Cooperation Initiative could facilitate a more effective consultation mechanism between MENA states and NATO, offering an alternative to their dependence on external actors such as the Russian Federation. In the short term, such an initiative could encourage certain Arab states to explore security options aligned with NATO, thereby reducing the need for military and technological support from Moscow. This would force Russia to intensify its efforts to maintain influence in MENA, potentially diminishing its ability to focus resources on projecting power in the Euro-Atlantic space. However, this strategy may face opposition from certain NATO member states, particularly the USA, which could view an expanded NATO engagement in MENA as conflicting with its own bilateral security partnerships, especially with Gulf states. In this scenario, the success of this strategy would depend on the balance between European support for an extended engagement in MENA and any reservations expressed by Washington, which might prefer maintaining direct control over its relationships with regional partners.

Improving strategic communication through a NATO digital platform in Arabic could have an immediate impact on the Alliance's perception in the region, helping to combat misinformation and build a more balanced image. Direct access to verified information about NATO's objectives and commitments could limit the effect of the information campaigns carried out by the Russian Federation and reduce the influence exerted by Moscow in the regional environment. In the short term, this initiative could prompt Russia to reorient its strategic resources towards maintaining influence in MENA, thereby reducing its ability to project power in the Euro-Atlantic space. However, such a project might be met with scepticism by some NATO member states, which could perceive the initiative as likely to provoke hostile reactions from MENA state actors with close ties to the Russian Federation.

Strengthening cooperation in nuclear security and non-proliferation of weapons of mass destruction could contribute to limiting non-state actors' access to nuclear technologies and reducing emerging risks associated with the development of autonomous strategic capabilities by states in the MENA region. This initiative could compel Russia to intensify its efforts to maintain influence over states seeking technological support in this field, which could benefit Euro-Atlantic security. However, the success of this initiative would depend not only on the receptiveness of MENA states to such cooperation but also on the position of certain NATO members, who may view extensive involvement in this area as posing significant

diplomatic risks. For example, Turkey, which has expressed interest in developing its own nuclear program and is collaborating with Russia on the construction of the Akkuyu Nuclear Power Plant (Nuclear Regulatory Authority 2024), may demonstrate reluctance.

Evaluating the impact of NATO's strategies in MENA cannot be done without considering the balance between the costs and benefits of these initiatives for Euro-Atlantic security. If these strategies lead the Russian Federation to reorient its resources towards maintaining its influence in MENA, instead of focusing on expanding its presence in the Euro-Atlantic area, this could be considered a strategic advantage. In this scenario, NATO could gain an indirect benefit by reducing Russia's ability to exert pressure on the eastern flank of the Alliance, which could be one of the positive effects of these strategies in the short term.

Of the three scenarios analyzed, the most beneficial strategy for NATO is enhancing strategic communication through a digital NATO platform in Arabic.
This scenario offers the advantage of maximizing NATO's influence in MENA without direct military involvement, reducing the Russian Federation's ability to control public discourse and consolidate its influence in the region. Such an initiative would allow NATO to combat Russian propaganda, clarify its commitments, and support regional partnerships by creating a direct, accessible communication channel for both the local population and decision-makers. Furthermore, this strategy would not generate significant opposition within NATO member states, as it is a non-military approach that does not interfere with US bilateral interests in the region or the positions of other members.

The most important aspect of this scenario is its impact on the Russian Federation's influence in the region. Russia actively employs disinformation strategies in MENA to strengthen its geopolitical position, undermine trust in Western partnerships, and maintain access to arms and energy markets. By implementing a NATO digital platform in Arabic, the Alliance could reduce the region's informational dependence on Russian sources, thereby forcing Moscow to redirect its resources to maintain dominance over the strategic discourse in MENA. This effort would implicitly reduce Russia's capacity to focus its attention on the Euro-Atlantic space, representing a strategic gain for NATO's security.

To implement this strategy, NATO must adopt a set of concrete measures. In this regard, the first course of action involves creating and launching a NATO digital platform in Arabic, which will provide updated information about the Alliance's commitments in MENA and clarify its positions in relation to regional partners. The platform could be managed by a specialized strategic communication centre, composed of regional policy experts and specialists in combating disinformation, ensuring that the messages are tailored to the cultural and political context of the target audience.

A second essential element of the strategy is the establishment of a partnership with local experts and academic institutions in MENA states, to enhance the platform's credibility and integrate it into the regional information landscape. Involving local personnel would help reduce the perception that this initiative is an external influence tool and would facilitate the acceptance of NATO's messages among decision-makers.

For this initiative to achieve its objectives, it is necessary to combat misinformation through a proactive strategy, which includes the constant monitoring of influence campaigns carried out by the Russian Federation and the development of counter-narratives based on verified information. Integrating interactive approaches, such as detailed analyses of geopolitical events and Q&A sessions with NATO experts, could facilitate the understanding of the Alliance's positions and counter hostile messages.

Another course of action focuses on integrating the platform into a broader framework of regional cooperation so that it can support the Mediterranean Dialogue and the Istanbul Cooperation Initiative. In this way, the platform would not only serve as an informative tool, but also as a complementary mechanism for strengthening NATO's relationships with MENA states in the field of security.

To ensure the effectiveness of this strategy, it is essential to evaluate the impact of the platform on NATO's perception in the region through periodic surveys and data analysis, so that messages can be adjusted based on public reactions and geopolitical dynamics. Constant monitoring would allow for the adaptation of content to regional developments and more precise calibration of messages in relation to the specific interests of MENA states.

Conclusions

In conclusion, NATO's involvement in MENA should be observed not just as a regional strategy, but as a crucial tool for diminishing the Russian Federation's ability to project power in the Euro-Atlantic space. Reducing Moscow's influence in the region could require the redistribution of Russian strategic resources, thus limiting the pressure on NATO's eastern flank and strengthening regional security.

Of the scenarios analyzed, improving strategic communication through a NATO digital platform in Arabic emerges as the most feasible short-term solution, with the potential to counter Russian disinformation and offer MENA states a credible alternative in terms of security. By implementing this strategy, NATO can weaken the Russian Federation's influence without generating significant internal opposition within the Alliance, making it a viable and sustainable option.

Therefore, strengthening NATO's presence in MENA not only improves relations with regional partners but also directly contributes to balancing the power dynamics between the Alliance and the Russian Federation, reducing strategic pressure on Europe and granting NATO more freedom of action in addressing Euro-Atlantic security challenges.

References

Administrația Prezidențială. 2015. *Ghidul Strategiei Naționale De Apărare A Țării Pentru Perioada 2015-2019*. București: Administrația Prezidențială.

Baban, Feyzi. 2018. "Nationalism and the crisis of community in the Middle East." *Dialect Anthropol* 42: 351–357. doi:10.1007/s10624-018-9534-5.

Bureau of Near Eastern Affairs. 2020a. "U.S. Relations With Qatar." https://www.state.gov/u-s-relations-with-qatar/.

___. 2020b. "U.S. Relations With United Arab Emirates." https://www.state.gov/u-s-relations-with-united-arab-emirates/.

___. 2022. "U.S. Relations With Bahrain." https://www.state.gov/u-s-relations-with-bahrain/.

Deac, Ioan, and Răzvan Grigoraș. 2014. "Modelarea autopoietică a Strategiei de Securitate Națională." *Impact strategic* 50 (1): 62-70.

Droin, Mathieu, Carlota G. Encina, Cameron Hudson, and Selin Uysal. 2024. "Critical Questions." https://www.csis.org/analysis/nato-and-its-south-redefining-terms.

EEAS. 2021. "League of Arab States (LAS) and the EU." https://www.eeas.europa.eu/eeas/league-arab-states-las-and-eu_en.

European Parliament. 2023. "The collapse of the controversial INSTEX mechanism and the motivations behind the EU's wrong policy towards the Islamic Republic of Iran." https://www.europarl.europa.eu/doceo/document/E-9-2023-001509_EN.html.

Grigoraș, Răzvan. 2022. *Metode științifice prospective în securitatea națională.* București: Top Form.

Ipsos. 2023. *Global Trends 2023.* Washington: Ipsos Publishing.

Ivanov, Dinev. 2011. *Transforming NATO: New Allies, Missions, and Capabilities.* USA: Rowman & Littlefield Publishing Group.

Liteanu, Traian, Constantin Degeratu, and Gheorghe Toma. 2007. *Evoluția Arhitecturilor de Securitate sub Impactul Globalizării.* București: ANI.

Lorch, Netanel. 2008. "The Arab-Israeli Wars." Report, Online: Ministry of Foreign Affairs. https://publikationen.ub.uni-frankfurt.de/opus4/frontdoor/deliver/index/docId/11317/file/The_Arab_Israeli_Wars.pdf.

Mezni, Mohamed, and Djebali Nesrine. 2022. "External Debt and Human Development Index: MENA Region Case." *Research Square* 1-18. doi:10.21203/rs.3.rs-1650276/v1.

Moosa, Elayah, Bashir Yasmin, and Qarmout Tamer. 2024. "Navigating Conflict: The Dynamics of Palestinian Civil Society Organizations amidst Internal Divisions." In *Conflicts in the Middle East and Africa*, by Elayah Moosa and Alzandi Bakeel, 121-133. New York: Routledge.

Muhamad, Goran, and Nabaz Khayyat. 2024. *Resource Management Performance: A Sectoral Analysis in the Post-Conflict Kurdistan Region of Iraq.* Singapore: Springer Nature.

National Intelligence Council. 2008. *Global Trends 2025: A Transformed World.* US Government Printing Office. www.dni.gov/nic/NIC_2025_project.html.

___. 2021. *Global Trends 2040.* Online: Office of the Directorate of National Intelligence. www.dni.gov/nic/globaltrends.

NATO. 2023. "The consultation process and Article 4." https://www.nato.int/cps/bu/natohq/topics_49187.htm.

2024a. "Istanbul Cooperation Initiative." https://www.nato.int/cps/en/natohq/topics_52956.htm.

___. 2024b. "Mediterranean Dialogue." https://www.nato.int/cps/en/natohq/topics_52927.htm.

Nuclear Regulatory Authority. 2024. "Licensing of Akkuyu Nuclear Power Plant. Authorization of Nuclear Facilities." https://www.ndk.gov.tr/en-US/licensing-of-akkuyu-nuclear-power-plant.

Quero, Jordi. 2023. *Overlapping Regional Orders in the Middle East and North Africa.* New York: Routledge.

Renfro, William. 1993. *Issues Management in Strategic Planning.* Westport: Quorum Books.

Rustamov, Bezhan, Nesrin Ozatac, and Nigar Taspinar. 2024. "Sustainable Development in Banking and Finance." *7th International Conference on Banking and Finance Perspectives, Famagusta, Northern Cyprus* (Springer Nature).

Trobbiani, Riccardo. 2017. *EU Cultural Diplomacy in the MENA Region: A Qualitative Mapping of Initiatives Promoting Regional Cooperation.* EL-CSID Working Paper 2017 - 2, Bruges: UNU Institute on Comparative Regional Integration Studies.

US Department of State. 2017a. "Joint Comprehensive Plan of Action." https://2009-2017.state.gov/e/eb/tfs/spi/iran/jcpoa/.

___. 2017b. "The Suez Crisis, 1956." https://history.state.gov/milestones/1953-1960/suez.

US Embassy in Kuwait. 2025. "U.S. - Kuwait Relations." https://kw.usembassy.gov/policy-history/#Assistance.

van den Bosch, Jeroen, and Natasha Lindstaedt. 2024. *Research Handbook on Authoritarianism.* United Kingdom: Edward Elgar Publishing.

Vieira, Alena, and Mohammad Eslami. 2023. *The Arms Race in the Middle East.* Switzerland: Springer.

Zara, Ion. 2006. *Europa – Qvo Vadis?* Constanţa: Ex-ponto.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Weaponization of data: the role of data in modern warfare

Dorcus Phanice OLASYA, Ph.D. Candidate*
Anita KIAMBA, Ph.D.**

*Department of Diplomacy and International Studies, University of Nairobi, Kenya
e-mail: dolasya@students.uonbi.ac.ke
**Department of Diplomacy and International Studies, University of Nairobi, Kenya
e-mail: akiamba@uonbi.ac.ke

Abstract

The 21st century is swamped with innumerable technologies distributed across different fields. Consequently, loads of data is being generated, transforming it into a tactical forte. Using appropriate tools and procedures, data can be appraised to generate enhanced insights into facts vital in decision-making for governments and businesses alike. However, despite its significance in strategic security, little attention has been paid to this concept. Accordingly, this article analyses ways in which data has influenced modern warfare and ways in which its potential misuse can be mitigated upon. Specifically, it highlights the aspect of power dissemination abetted by data availability, its influence in military strategies and procedures, and the role it plays in tactical intelligence and surveillance as well as military decision-making. The study adopts a qualitative and analytical research design as it comes with fewer ethical considerations. Secondary data is gathered from existing records, journals, reports, internet sources, policy papers, presented papers and books. Using the case study of Russia and Ukraine, the findings indicate that data has been transformative in present-day conflicts. Through open source data, actionable intelligence has been realized. Further, technologies such as remote sensing have been valuable to tactical intelligence, while the documentation of war crimes provided situational awareness in Ukraine as well. For ethical purposes, therefore, the use of data in the battlefield calls for sufficient regulations to oversee its use. This will also ensure caution during its deployment for the preservation of human rights as stipulated in the International Humanitarian Law.

Keywords:
data; warfare; cyber war; battlefield; military.

Article info
Received: 14 February 2025; Revised: 28 February 2025; Accepted: 5 March 2025; Available online: 2 April 2025

Citation: Olasya, D.P. and Anita Kiamba. 2025. "Weaponization of data: the role of data in modern warfare." *Bulletin of "Carol I" National Defence University*, 14(1): 90-107. https://doi.org/10.53477/2284-9378-25-06

Cyber-space, through its ability to connect the world, has been fundamental in redesigning the global security perspective. The extensive use of technology has provoked the online administration of countless businesses, hence growing the amount of data generated. In 2023, for instance, a report by Global Data projected a 26% increase in the total amount of data produced for the periods between 2017 and 2022, with mobile traffic taking up 9% of the internet traffic (Army Technology 2023). At present, approximately 8.55 billion searches are made daily using Google (Shewale 2024), and approximately 402.74 million terabytes of data are being created daily, with the figure expected to hit 181 zettabytes by the end of 2025 (Duarte 2024). Given the current emerging economic space, data has gained some sort of additional economic value. Alec Ross, a US technology-policy expert, labelled it the "raw material" of the new Industrial Revolution (Manning 2020), with other analysts referring to it as the new oil of the 21st Century, a phrase coined by the famous British mathematician and entrepreneur Clive Humby (Wilbik 2024).

As more sectors integrate technology into their daily operations, the collection of data intensifies. Just as corporate entities, Netflix for instance, have made use of data from their subscribers to understand and predict their habits (Marr 2016), governments especially in the Global South could leverage on a centralized data system (Offiong, Nta, and Etim Bassey 2021) in addition to big data generated from technologies such as the GPS systems (Nwanga et al. 2014) to combat insecurity and acts of terrorism. To note, however, is that data has the potential to be misused as was the case in Xinjiang, where the Chinese government is accused of using the IJOP app to surveil and collect data on its residents (Human Rights Watch 2019).

In the military, data can be valuable in the enhancement of situational awareness and weaponized during wars to earmark the opponents (Hammond-Errey 2022). In Liverpool for instance, during the COVID 19 pandemic in 2020, Professor Iain Buchan together with the members of the 8 Engineer Brigade, tapped into a data linkage and AI-automated intelligence system dubbed the Combined Intelligence for Population Health Action (CIPHA) to help combat the virus, classified then as a threat to the civil society (King 2024). By the same token, Ukraine, along with its allies, have made use of open source data such as satellite images to identify and attack its opponents (King 2024). With the help of a private technology company, Ukraine has benefitted immensely in the area of targeting (Farnell and Kira 2024). Data has, therefore, ceased being a mere facet in understanding the battlefield frontiers to a frontier in itself. In order to gain tactical advantage on this new characteristic of war, therefore, states require massive investment in data gathering and analysis capabilities.

Data can be described as the raw material making up any given information (Räsänen and Nyce 2013). They are recorded facts (Michael 2017) that can be logicalized and processed to come up with valuable information (Gu 2023). Data can also be viewed in terms of facts with reference to occurrences (Davenport and Prusak 1998). Herian (2021) broadly looks at it as known or supposed facts that,

if processed, could generate knowledge defining policies and also explain specific behavior. It is made up of structured and unstructured facts represented in the form of numeric, alphabets, photos, videos and audios, collected from sources such as social media, transactions, surveys just to mention but a few. It operates as a tool for dissemination in the economic process, hence crucial towards any critical decision-making process. Through data, actionable insights are realized making it an intermediary of experience and an undisputable source of truth (Herian 2021).

The use of data within the armed forces has gained traction, especially in the Global North. During the 2018 NATO Science and Technology Organization's Specialists meeting held in France, Roberto Guerrero, an official, resonated that for NATO to enhance and maximize its force, digitizing the battlefield by making use of big data is paramount (Poland 2018). Through sufficient data, Guerrero added, rational and insightful decisions on smart operations will be made. To bring this to perspective, he highlighted findings on how the inclusion of data brought about a deeper understanding of the effects of flight planning to fighters, allowing the Air Force leadership to come up with informed decisions in support of the respective operations (Poland 2018).

For the effective use of data on the battlefield, an enhanced comprehension of the problem at hand is paramount. Dawson and Matthew, therefore, propose examining it as ammunition. They argue that viewing it from this perspective will unveil its weaponry-like attributes, making it possible to understand its capabilities and enabling the defense forces to appreciate this major shift in the character of war (Dawson and Matthew 2024). Furthermore, with this concept, it will be possible to conceptualize the potential risk data poses, enlightening leaders on its threats to individuals as well as the armed forces (Dawson and Matthew 2024). To note, however, unlike physical ammunition that becomes unserviceable over a period of time, once data is stored, its value and form remain intact. Similarly, with numerous claims of data exploitation and massive violations of human rights by both state and non-state actors in the Global South, Mone et al. (2024a) propose the concept of data warfare. Data warfare in this case means the use of information and communication technologies (ICTs) by states to manipulate data systems of other states or entities for political or economic advantage (Mone et al. 2024a). This can be executed through hacking or malware attacks leading to insecurities at the national level, in addition to interfering with human rights. This concept has widely been adopted by a number of states to advance their agendas. China, for instance, has been accused by the US several times of attacking its key research facilities to steal data on its key innovations to enable its foreign influence campaigns (Farivar 2023).

As the role of data across numerous fields grows rapidly, challenges on the international legal frame to manage its malicious use have come to light. At present, the basic principles that govern personal data are being violated on purpose in favor of military operations while defying the International Humanitarian Law

(IHL) (Mone et al. 2024b). Therefore, concerns have been raised on the application of the IHL to military operations such as targeting and surveillance that majorly leverage data, considering that its operationalization is merely considered an act of espionage and hence falls under domestic rather than international law (Mone et al. 2024a). Further, due to the act of attribution, it is almost impossible for states to take responsibility for their actions. A case in point is the recent allegation of the hacking and intrusion of Kenya's key ministries and government departments by the Chinese government, allegations that have since been denied (Reuters 2023).

This article, therefore, contributes to the ongoing debate on the use of data in the modern battlefield by demonstrating its influence in the current transformation in power distributions, as well as its role in key military strategies and procedures, military decision making, in addition to tactical intelligence and surveillance. The study is anchored on two key objectives: first, to highlight the ways in which data has influenced modern warfare, and second, to discuss ways in which the potential misuse of data can be mitigated now that its incorporation in modern warfare is inevitable. The case study of the Russian - Ukraine war intends to bring to perspective the specific areas in which data has been transformative in present-day conflicts and how it has influenced major decisions on how wars are fought.

Methodology

This study seeks to highlight the role of data in modern warfare. Under the numerous activities conducted online, a lot of data is being produced. Using appropriate tools and procedures, therefore, data has been transformed to a tactical forte in key military strategies. Currently, states are not the only collectors of data; non-state actors are scrambling for its collection, analysis and exploitation to gain a niche in their respective areas. With this, data has been translated to one of the most valuable commodities not only to governments but also to non-state actors. Using the case study of the Russian – Ukrainian war, this study seeks to answer the following research questions:

1. How has data influenced modern warfare?
2. How can the potential misuse of data, especially in warfare situations, be mitigated?

The study adopts a qualitative and analytical research design as it comes with less ethical considerations while providing for the opportunity to maintain neutrality, objectivity and credibility of the data sets. Secondary data used is gathered from existing records, journals, reports, internet sources, policy papers, presented research papers and books. The findings and conclusions are drawn from the analysis of the available empirical data used.

Literature Review

Ubiquity of Data

The fourth industrial revolution is characterized by the proliferation of technologies, such as mobile phones and social media platforms, that have enhanced connectivity and communication among individuals and groups. Through these technologies, people across all divides can benefit from equal access to information and communication systems. Owing to the fact that the computing powers of cellphones today exceed organizational resources owned by institutions in the past, users, at the comfort of their cell phones, have the capabilities to access and process numerous online data sets. The processing power currently possessed by cell phones and other easily accessible devices have therefore made data ubiquitous and readily available to everyone for access and processing.

Ubiquitous data elucidates unstructured and decentralized data, sourced from different, possibly contradicting or overlapping sources (Hotho, Pedersen, and Wurst 2010), the social bookmarking systems being a typical example. Since the establishment of the social web in the late 1990s, content generated by users through the various social media sites became central to the internet culture. Through smartphones, users are able to create, upload and share content instantly from anywhere across the globe. This has created a web of interconnected networked devices, acting as information collection points publicly sharing its findings on social media. The outcome has been the proliferation of information with possible operational and intelligence value.

The accessibility of information, some of which may contain operational and intelligence value, has opened up opportunities to civilian organizations to carry out accurate intelligence analysis away from state intelligence organizations. For instance, in 2014, the covert activities of Russian soldiers in Ukraine were unfolded by the Atlantic Council and Vice News, following the combatants' activities on social media (Allen 2020). On the same note, the Global Investigative Journalism Network has been able to carry out high-caliber investigations on divergent issues by merely using readily available open-source intelligence, which is mostly generated from social media platforms (Allen 2020). Further, during the COVID-19 pandemic, using phone data, a private geospatial analytics company was able to point out the fact that several arms industries in Russia were decelerating their production, despite the government depicting very little effects of the pandemic within the country (Tucker 2020). Coincidentally, days after the report emerged, members of the forces were prohibited from carrying any digital device likely to record or store data to work (RFE/RL 2020).

Presently, content devoid of credibility is disseminated at a supersonic speed to audiences sitting in different corners of the world. Data on individual citizens and their patterns of life, likes, and preferences are easily collected, collated and analyzed by commercial

entities as well as malicious actors, using readily available tools and methodologies (Motupalli 2017). Additionally, the ubiquity of data has not only enhanced the global production chain but has also accelerated trade and investment flow. Making use of big data, companies have come up with new services, such as customer relations management, in addition to revamping their management strategies and exploring novel market domains. In a nutshell, through available data, commercial services have been transformed, directly impacting the respective economies (Ülgen 2016).

Data and Global Power Shift

For a long time, power within the international system has been discussed in the form of a state's military strength (Nye 1990). At present, however, this notion is diminishing as other factors, such as economic interdependence and the spread of technology, are diffusing power away from the traditionally great powers to private actors as well as perceived small states (Nye 2023). Additionally, along with modernization, increased communication being experienced in developing countries has also contributed to the diffusion of power from governments to private entities (Nye 2023). As information becomes powerful, the ability to respond to new information promptly becomes supreme.

Wang and Nye (2022) highlight two categories of power shifts being experienced in the current information age. First is the power shift from the west to east, that is, from Europe and the Atlantic to the Pacific and Asia, and power shifts from governments to non-governmental and transnational actors, with the second category being majorly driven by technology. Hence, power is slowly diminishing from being defined in terms of capital wealth to being defined in terms of the quantity of information one has access to (Nye 2023). With its massive cross-border distribution, therefore, information in the form of data has become a component of globalization, with data flow registering over a 100% increase between 2008 and 2020 (McCormick and Slaughter 2021).

Data is key in devising new ideas. Therefore, its unlimited flow provides economic potential because of its nonrival nature. Nonrival means that its consumption does not diminish its value, and hence it is still available for use by others (McCormick and Slaughter 2021). Because of this, innovation and, consequently, economic power depend on the quality and quantity of data accessible by states and corporations (McCormick and Slaughter 2021). Hence, tech companies, as the main collectors of data, through their newly acquired power, are taking part in foreign policies independent of their home states. A case in point is the relationship between Google and China, which contradicts American foreign policy. Further, reports have emerged of American tech companies still engaging with Huawei, completely disregarding its blacklisting by the U.S government (Apostolicas 2019).

Besides policy formulation, tech companies are rapidly investing and acquiring military technologies and capabilities that could highly impact cyber warfare.

Examining a 2018 Cybersecurity Accord, tech companies, such as Microsoft, agreed to refrain from any current or future cyber wars (Apostolicas 2019), meaning that while they do have these capabilities in place, they chose to refrain from using them. Through computer capabilities such as Quantum computing, spearheaded by private tech companies such as IBM and Intel, the current encryption methods could be unraveled. Although this is unlikely to be used in wars, it certainly would be one of the deadliest cyber-weapons globally not in the hands of government entities.

Data in Military Strategies and Decision Making

The current digital age has seen the military increasingly take advantage of data science for enhanced capabilities. By analyzing historical and real-time data, the armed forces have been able to identify trends, patterns and anomalies, thereby pointing out threats while forecasting the outcomes of upcoming military operations (Jang 2023). Through an extensive analysis of a wide range of data, it is possible to identify high-risk activities and, hence, allocate resources accordingly. Consequently, data has been able to enhance situational awareness while providing a comprehensive understanding of the operational environment, such as the weather conditions and the terrain in question (Jang 2023). Through war-gaming and simulation, available data can be used to create scenarios allowing the forces to refine their strategies. During the 2004 battle in Fallujah, for instance, war gaming was used to showcase the anticipated damage in view of classifying the reconstruction process (Mcwilliams and Schlosser 2004).

Military strategy is a critical element in military affairs, and it captures the planning phase and the execution of wars. Kofman *et al.* define military strategy as a set of guidelines states and top military officials adopt for defense and the management of war on the battlefield (Kofman et al. 2021). Through strategic decision-making, the military is able to come up with effective courses of action regarding specific situations (Zabala-López et al. 2024). This process first identifies a problem, then collects and carries out an analysis on the available data, after which the possible approach is identified, weighing its pros and cons. Depending on the specific ideologies, the decision is passed to the command and control for execution (Zabala-López et al. 2024). Military strategic decision-making is mainly carried out to deal with issues emanating from the various military domains and threatening the sovereignty and security of states.

For a successful military operation, decisions need to be prompt and accurate. Treiblmaier (2022), therefore, proposes the use of a data-driven decision-making strategy to coordinate the available resources with the goal to be achieved. He defines data-driven decision-making as the prior preparation and analysis of data for timely decision-making. Hence, this necessitates building up an analysis-based corporate culture. To build up a data-driven decision-making strategy within the military, he recommends the collection of data in all the available sources, the Internet of Things included, after which the data is evaluated, grouped and presented. This comes with

a number of advantages. For instance, with real-time data obtained from various sources, it is easy to get precise information regarding situations that can also be adjusted to meet specific undertakings. This also eliminates human biases and limitations, allowing military leaders to come up with accurate and timely decisions (Haraburda 2019). However, imaginative skills are needed to enhance the quality of decisions to be made. This strategy can be valuable in areas such as military logistics, location assessment, and deployment possibilities in addition to the replenishment of supplies and other needs on the battlefield (Treiblmaier 2022).

Similarly, to enhance military strategy, Rettore *et al.* (2023) propose the concept of Military Data Space (MDS), which integrates civilian and military data. Typically, the MDS consists of two divergent data sources: Inter- Military Data (IMD) and Extra-Military Data (EMD). While IMD encompasses data-sets provided by the military, EDM includes data-sets collected from physical or virtual sources like social media, in addition to government reports. This set of data could allow a comprehensive understanding of local behavior explaining the environment around the military operation. For efficiency, the study introduces the concept of data fusion as the authors consider that, in military applications, having varied sets of data has the potential to boost information dominance and awareness in multifaceted warfare scenarios. They add that data fusion could alleviate information overload and, therefore, enhance accuracy, coming up with sufficient knowledge to support strategic operations and situation assessment.

The study, however, notes that data harvested from external military sources do come with cyber security risks, making the military systems prone to cyber-attacks. This is well articulated by the recent rise in cyber-attacks, with reports indicating that data breaches cost businesses approximately $4.35 million in 2022, up from $4.24 million in 2021 (Griffiths 2024). It is also observed that once data is manipulated, the consequences could be severe to the populace as well as the process of military decision-making, hence undermining the integrity of the stipulated data sources. This is clearly illustrated by the current spread of misinformation and disinformation on social networking sites mostly used for political gain (Rettore et al. 2023).

Data in Tactical Intelligence and Surveillance

The Cold War, in addition to globalization, massively transformed the strategic security framework during the mid and late 1990s. However, the onset of the new millennium saw the proliferation of technologies that have not only altered every aspect of human lives but also contributed to the production of huge amounts of data globally. At present, almost 402.74 million terabytes of data are produced daily (Duarte 2024), with the figure expected to rise exponentially. Just as business entities, this massive production of real-time data has proved valuable for tactical commanders to engage successfully high-priority targets (Romine 1994). Hence, through technological inventions, the battlefield has been broadened at unimaginable levels, bringing forth the need to reevaluate the existing doctrines governing wars and conflicts.

With diverse data sources, intelligence entities have been presented with extraordinary capabilities to collect and process useful and relevant information to national interest promptly (Katz 2020). Technical intelligence, for instance, can aid the forces in uncovering signals used by the opponents and help detect abnormal behaviors within the battlefield, thus enabling them to forecast any forthcoming dangers (Katz 2020). In the Navy, data on intelligence, surveillance, and reconnaissance from devices such as drones can be useful in situational awareness or assist in safely navigating the vessels in addition to target identification (Porche et al. 2014). By the same token, through the massive data available, the armed forces have been presented with nouvelle opportunities in intelligence gathering as well as targeting domains, opening up the possibilities of swiftly unravelling a target, leading to successful litigations (King 2024). Through intrusive surveillance and targeting, a suspect's activity online, location and movement can be unraveled (Hammond-Errey 2022). This can be achieved by making use of spyware. Although Allen (2020) predicted a data-swept battlefield in 2035, where data will be supreme in all aspects, this happened sooner than expected. In 2021, the Israel Defense Forces utilized AI and data for precision to mount a series of strikes against Hamas in Gaza. Accordingly, this effective use of data prompted the attack to be labelled as the first-ever digital war (King 2024) to be successfully executed.

Currently, tactical intelligence that involves the analysis and transmission of data by specialized units and is majorly engrossed in holding up operations at the tactical level (Gragido and Pirc 2011) is already cyber-oriented. This transformation is evident in the field of open-source intelligence (OSINT), where information of tactical value is identified, processed and disseminated for tactical applications (Allen 2020). Apart from OSINT, Allen notes that the Internet of Things (IoT), because of its numerous vulnerabilities, presents exciting tactical intelligence opportunities. If intelligence and cyber operations are well harmonized, IoT could be an asset since it is capable of exposing the numerous sensors that could help unmask adversaries.

The value of data in intelligence analysis can further be showcased by its ability to highlight previously unknown relationships, even without the knowledge of the context and causality of these relations (Landon-Murray 2016). Through the analysis of data from signal intelligence sources such as phone communications, human behavior can be predicted, hence to the extreme, allowing stakeholders to devise directives to mitigate any negatives associated with the identified behavior (Reilly 2015). Additionally, considering that social media sites have been identified as the instigators of sentiment analysis, they could be of value to intelligence organizations as well as policymakers in predicting trends and, therefore, adjusting accordingly in terms of strategic change (Landon-Murray 2016). And, while data presents great opportunities for intelligence organizations, there exist possibilities of data corruption that could compromise targeting either by obstruction or leading to false targeting (King 2024). Adversaries may engineer data with the sole intent of

deceiving and confusing intelligence agencies. This manipulation could also lead to massive intelligence failure that could result in loss of lives. The October 7th 2023, attack on Israel by Hamas is a typical example, where the sensors, signals, image and human intelligence networks all failed, leading to massive loss of lives, abductions and loss of property (King 2024).

Case Study:

Russia and Ukraine

The war between Russia and Ukraine escalated on 24th February 2022, after what is described as an unprovoked and unjustified invasion of Ukraine by Russian troops (Shafy Ramadhan 2023). To date, this war has experienced a decentralized military engagement, where violence has not only been spewed over the traditional battlefields of war, that is, land, sea and air, but also through cyberspace. Making use of cutting-edge technologies, both sides have employed contemporary innovations such as armed drones and Artificial intelligence-enabled systems for prompt intelligence gathering (Favaro and Williams 2023). Leveraging the data explosion experienced globally over the past years, military intelligence, targeting and decision-making processes have been made easy and accurate (King 2024). The Russian invasion of Ukraine, therefore, presents a sneak peek of warfare in a data-rich environment, with each side capitalizing on data to foresee the enemy's next move.

Since its invasion, Ukraine, along with its allies, has been able to capitalize on technology for its defense against Russia. By making use of the current explosion of open-source data such as phone and radio messages, actionable intelligence has been realized. Through photos posted online by both civilians and combatants, locations of key Russian targets have also been identified. On December 31st 2022, for instance, exploiting pictures posted on social media by Russian soldiers, Ukraine was successfully able to strike the barracks in Mariivka, where over 600 Russian recruits are believed to have been killed (King 2024). Also, just before the invasion, open-source satellite imagery sourced from private companies, as well as photos and videos posted on social networking sites like TikTok, helped Ukraine uncover Russian forces' activities along its borders. Through social media intelligence and biometric data, it was also possible to identify Russian agents working within Ukrainian borders (Mysyshyn 2024).

Since the onset of the war, Ukraine has also made use of remote sensing for tactical intelligence. Through smart remote sensing devices, data is collected in remote areas analyzed, visualized and then interpreted using specialized software, where patterns, trends and anomalies are identified (Mysyshyn 2024). This technique has been valuable in documenting war crimes executed by the Russian troops as well as providing situational awareness on occurring events besides areas currently experiencing active war or environmental hazards. To illustrate this, although Russia

denied any dealings to do with images that occurred of dead civilians along the streets of Bucha, analysis of satellite images and videos provided placed Russian troops at the location where the bodies of the civilians were. Additionally, making use of satellite images, the cause of death of Ukrainian prisoners of war held in Olenivka in July 2022 was easily pinpointed to the Russian troops that had occupied the village (Mysyshyn 2024).

The current digital atmosphere has provided an ideal breeding ground for propaganda and disinformation, evoking the concept of weaponizing information to point out its damaging nature to the targeted group of people (Mandić and Klarić 2023). In Russia, information warfare has been used consistently as part of its strategic thinking to achieve its objectives and has continuously propagated falsified information to justify its "special military operation" in Ukraine (Fortuin 2022). Making use of social media sites, Russia has intentionally spread propaganda to garner support in addition to spreading hate against Ukraine and its Western supporting counterparts. To substantiate this, Geissler *et al.* (2023), in their study on the use of propaganda on social media during Russia's invasion of Ukraine, deduced that online propaganda has become a powerful tool in modern warfare. Making use of social media, fabricated information is easily available and can be spread swiftly. The study records that the bulk of pro-Russian messages have been disseminated through X, formerly Twitter, by bots. To note is that on the day of the UN vote on Resolution ES-11/1, Russian propaganda was directed towards the countries that abstained from voting, suggesting a deliberate and strategic manipulation of public opinion on X (Geissler et al. 2023).

Discussion and Findings:

The Russian invasion of Ukraine was majorly provoked by Ukraine's reassertion of their intentions of getting enlisted in NATO (Khoirunnisa and Sugiati 2024). Expressing its dissatisfaction, Russia deployed strategies, both military and non-military, against Ukraine with the sole intention of toppling what is seen as a Western-aligned government of Volodymyr Zelenskyy. After successfully invading and seizing Crimea in 2014, along with its strategic and economic might (Kramer 2015), Russia's expectation indicated that Ukraine would be easily subdued. However, three years on, this is not the case. Ukraine's synergy when it comes to modern technologies, along with skilled combatants, has proved valuable in the current war environment (Śliwa 2022). Following the attack, Ukraine has harnessed technology for its defense (Mysyshyn 2024), accentuating its tactical advantage and, at the same time, the numerous ethical dilemmas that come along with it. Together with private entities, Ukraine has been able to make use of data via technologies such as remote sensing, AI and facial recognition to boost its capabilities. This visible presence of non-state actors opens up new debates on the role of tech companies, mostly privately owned, manufacturing and holding patents to the numerous advanced military technologies currently being used on the battlefield.

Further, the war has transformed Ukraine into a research lab, with private companies testing and deploying their innovations on the battlefield (Sharma 2023). Tech companies such as Palantir, an American company specializing in software platforms for big data analytics, have been incorporated into the Ukrainian war routine with numerous government agencies the defense included utilizing the company's products (Bergengruen 2024). This collaboration calls to attention the extreme incorporation of technology into the various defense processes. Additionally, international companies are scrambling for data captured from the Ukrainian battlefield to help improve AI and machine learning (Sharma 2023). Consequently, a symbiotic relationship between tech companies and the state of Ukraine, both benefiting from the ongoing war, has been created and enhanced. To note further is that the relationship between the West and Ukraine has been enhanced, and this is evidenced by the bilateral agreement between the two states put forward in June 2024 (The White House 2024).

Data is the basis of innovativeness (McCormick and Slaughter 2021). Through data, the world has been able to experience new innovations such as AI and Machine Learning that have been used to alter the battlefield. Currently, the Ukrainian battlefield has encountered innovations that are likely to interfere with human judgment. Making use of the available data along with the technologies mentioned above, in the near future, key decisions on the battlefield are likely to be determined by algorithms, disregarding the human judgment, which is vital in the preservation of human rights. What this means is that there is a likelihood of massive infringement of human rights with the wide spread of the use of non-human elements within the battlefield. Additionally, as most of these technologies are owned by tech companies, the possibilities of them posing as independent actors within the battlefield are massive (Bergengruen 2024).

Nouvelle innovations have not only transformed the Ukrainian battlefield but have also presented overwhelming challenges to democracy and privacy rights (Mysyshyn 2024). Technologies in use for surveillance and face recognition, for instance, have proved to be detrimental to individuals' privacy as the majority of the time, data extracted or accessed is done without the user's consent. The use of Clearview AI, for instance, is facial recognition software identifying people by images previously sourced from social networking sites and other search engines, such as Google (Mysyshyn 2024). Although this technology is aimed at identifying Russian adversaries, the photos uploaded therein were uploaded without the consent of the users. The fact that Clearview AI's database has been sold to different authorities indicates the intentional violation of personal data for the force's gain, violating the International Humanitarian Law.

Conventional wars are regulated by the International Humanitarian Law. However, a transformed battlefield, as showcased in the Russian- Ukraine war, has uncovered loopholes in war management. The war has demonstrated that the current international institutions are not sufficient to deal with the proliferation of

data; neither are they prepared to deal with the developing flaws (McCormick and Slaughter 2021). Even with the explosion of cross-border data flows, global data management remains unregulated. This intensifies the concerns on the state of global security, bearing in mind the stipulated capabilities of data in as far as AI and machine learning are concerned. Also, as highlighted by Mone *et al.* (2024a), data inequality between the Global North and South has allowed the Global North to weaponize data to enhance their economic and technological influence. Maintaining control over data, companies in the North have continuously disregarded the opinions of those in the South on data mining and the supposed use of the data mined.

Recommendations:

The presence of data and its availability has transformed modern warfare. This is evidenced by the ongoing Russia-Ukraine war, where data has been used in war decision-making and strategies, military tactics and intelligence collection. Making use of AI and Machine learning, precision in targeting has been enhanced. And, as data is incorporated into key military strategies, concerns are raised considering that in the near future, key decisions on the battlefield are likely to be determined by algorithms, disregarding human judgment. Thus, the likelihood of contravening the International Humanitarian Law is eminent. Therefore, while technology and its accessories are deployed on the battlefield, caution needs to be exercised to ensure the preservation of human rights as per the IHL.

Additionally, the Russian- Ukraine war has demonstrated massive public – private partnership with the private sector putting forward technologies to enhance military strategies. While this is desirable, it is important to note that having these forms of technologies in the hands of private entities presents a huge challenge to global security as they can be misused if they land in the wrong hands. Also, the fact that private entities have been actively involved on the battlefield automatically grants them the chance of being players in the conflict, complicating the war situation. With this, regulations need to be put in place to manage the extent to which third parties, in this case, private entities, need to be involved in the battlefield. This will bring forth clarity on who the actual enemy is, avoiding cases of victimization, especially in as far as private entities are concerned.

Lastly, as demonstrated in this paper, the capabilities of data in war situations are massive. Basically, it has been transformed to be the "heart of the global body", as its importance cannot be overemphasized. However, despite its position, there is no international regulation managing its application and use. Consequently, chances of data misuse not only in the battlefield but also commercially do exist. Thus, just as the IHL oversees international conflicts, it is important to put in place agreeable legislation to oversee the global use of data, especially in the war front. This will ensure that ethics as well as privacy are adhered to.

Conclusion

Technology has no doubt been encompassed in every aspect of human life, and the more we use it, the more data is produced, intensifying its importance. With this, a paradigm shift has emerged across all sectors, the military included, where data has become valuable in not only intelligence gathering but also in predictive maintenance and strategic decision-making. Through massive amounts of data, military operations have been remolded to strengthen their effectiveness, thus enhancing their capabilities. Nonetheless, data has proved to be a double-edged sword; apart from generating ethical debates in matters of privacy and security, misuse of data by collecting agencies has been widely reported. With the current emerging trend of incorporating data in military operations, questions have emerged in terms of ethics, management and misuse of data within the battlefield. Based on this, therefore, this study calls for caution in the deployment of technology and its accessories on the battlefield to ensure the preservation of human rights as per the IHL. Additionally, with third parties in the form of technology companies being actively involved in the battlefield, the importance of regulations to manage their role cannot be emphasized enough, as this will eliminate instances of victimization, especially concerning these private entities. Lastly, with the rapid evolution of technology, its management, especially on the battlefield, is key. In reference to this, therefore, agreeable legislation to oversee their deployment, especially in the war front, will be valuable in ensuring ethics as far as the deployment of technology is concerned.

References

Allen, Capt T S. 2020. "Finding the Enemy on the Data-Swept Battlefield of 2035." *Military Review* 28: 28–37.

Apostolicas, Paul. 2019. "Silicon states." *Harvard International Review* 40 (4): 18–21. https://www.jstor.org/stable/26917261.

Army Technology. 2023. "How Data Became the New Frontier in Modern Warfare." https://www.army-technology.com/sponsored/how-data-became-the-new-frontier-in-modern-warfare/.

Bergengruen, Vera. 2024. "Tech Companies Turned Ukraine Into an AI War Lab." *Time.* https://time.com/6691662/ai-ukraine-war-palantir/.

Davenport, Thomas, and Laurence Prusak. 1998. *Working Knowledge: How Organizations Manage What They Know*. *Ubiquity*. Vol. 1. https://doi.org/10.1145/348772.348775.

Dawson, Jessica, and Katie E Matthew. 2024. "Data as Ammunition–A New Framework for Information Warfare." *The Cyber Defense Review* 9 (2): 93–108.

Duarte, Fabio. 2024. "Amount of Data Created Daily (2024)." *Exploding Topics*. https://explodingtopics.com/blog/data-generated-per-day.

Farivar, Masood. 2023. "FBI Warns About China Theft of US AI Technology." *Voice of America (VOA)*. https://www.voanews.com/a/fbi-warns-about-china-theft-of-us-ai-technology/7202760.html.

Farnell, Richard, and Coffey Kira. 2024. "AI's New Frontier in War Planning: How AI Agents Can Revolutionize Military Decision-Making ." *The Belfer Center for Science and International Affairs*. https://www.belfercenter.org/research-analysis/ais-new-frontier-war-planning-how-ai-agents-can-revolutionize-military-decision.

Favaro, Marina, and Heather Williams. 2023. "False Sense of Supremacy: Emerging Technologies, the War in Ukraine, and the Risk of Nuclear Escalation." *Journal for Peace and Nuclear Disarmament* 6 (1): 28–46. https://doi.org/10.1080/25751654.2023.2219437.

Fortuin, Egbert. 2022. "'Ukraine Commits Genocide on Russians': The Term 'Genocide' in Russian Propaganda." *Russian Linguistics* 46 (3): 313–47. https://doi.org/10.1007/s11185-022-09258-5.

Geissler, Dominique, Dominik Bär, Nicolas Pröllochs, and Stefan Feuerriegel. 2023. "Russian Propaganda on Social Media during the 2022 Invasion of Ukraine." *EPJ Data Sci.* 12 (1). https://doi.org/10.1140/epjds/s13688-023-00414-5.

Gragido, Will, and John Pirc. 2011. "6 - State-Sponsored Intelligence." In *Cybercrime and Espionage*, edited by Will Gragido and John Pirc, 81–114. Boston: Syngress. https://doi.org/https://doi.org/10.1016/B978-1-59749-613-1.00006-6.

Griffiths, Charles. 2024. "The Latest Cyber Crime Statistics (Updated July 2024) ." *AAG IT Support*. https://aag-it.com/the-latest-cyber-crime-statistics/.

Gu, Hongfei. 2023. "Data, Big Tech, and the New Concept of Sovereignty." *Journal of Chinese Political Science*. https://doi.org/10.1007/s11366-023-09855-1.

Hammond-Errey, Miah. 2022. "Big Data and National Security: A Guide for Australian Policymakers." Sydney: Lowly Institute. https://www.lowyinstitute.org/publications/big-data-national-security-guide-australian-policymakers.

Haraburda, Scott S. 2019. "Benefits and Pitfalls of Data-Based Military Decisionmaking." *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/benefits-and-pitfalls-data-based-military-decisionmaking.

Herian, Robert. 2021. *Data: New Trajectories in Law*. 1st edition. Routledge. https://doi.org/10.4324/9781003162001.

Hotho, Andreas, Rasmus Ulslev Pedersen, and Michael Wurst. 2010. "Ubiquitous Data" In "Ubiquitous Knowledge Discovery: Challenges, Techniques, Applications." edited by Michael May and Lorenza Saitta, 61–74. Berlin: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-16392-0_4.

Human Rights Watch. 2019. "China's Algorithms of Repression." https://www.hrw.org/sites/default/files/report_pdf/china0519_web.pdf.

Jang, Simon. 2023. "The Role of Data Collection and Big Data in Military War Planning. "| *CISS AL Big Data | Medium*. https://medium.com/ciss-al-big-data/data-is-constantly-generated-a-collected-in-the-modern-era-by-everything-3738f0d8ac10.

Katz, Brian. 2020. "The Collection Edge." *Center for Strategic and International Studies (CSIS)*. http://www.jstor.org/stable/resrep25236.

Khoirunnisa, Khoirunnisa, and Cristy Sugiati. 2024. "Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare." *Journal Public Policy* 10 (2): 138–45.

King, Anthony. 2024. "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence." *Journal of Global Security Studies* 9 (2): ogae009. https://doi.org/10.1093/jogss/ogae009.

Kofman, Michael, Anya Fink, Dmitry Gorenburg, Mary Chesnut, Jeffrey Edmonds, Julian Waller, Kasey Stricklin, and Samuel Bendett. 2021. "Russian Military Strategy: Core Tenets and Operational Concepts."

Kramer, David J. 2015. "The Ukraine invasion: One Year Later." *World Affairs* 177 (6): 9–16. http://www.jstor.org/stable/43555264.

Landon-Murray, Michael. 2016. "Big Data and Intelligence." *Journal of Strategic Security* 9 (2): 92–121. http://www.jstor.org/stable/26466778.

Mandić, Josip, and Darijo Klarić. 2023. "Case Study of the Russian Disinformation Campaign during the War in Ukraine – Propaganda Narratives, Goals, and Impacts." *National Security and the Future* 24 (2): 97–140. https://doi.org/10.37458/NSTF.24.2.5.

Manning, Robert A. 2020. "Emerging Technologies: New Challenges to Global Stability ." https://www.internetworldstats.com/stats.htm.

Marr, Bernard. 2016. *Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results*. John Wiley & Sons.

McCormick, H. David, and J. Matthew Slaughter. 2021. "Data Is Power." *Foreign Affairs.* https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age.

Mcwilliams, Timothy S, and Nicholas J Schlosser. 2004. "U.S. Marines in Battle: Fallujah." Marine Corps University.

Michael, David. 2017. "What and Where Is My 'Data'?" *GPSolo* 34 (2): 46–49. http://www.jstor.org/stable/26425848.

Mone, Varda, Sadikov Maksudboy Abdulajonovich, Ammar Younas, and Sailaja Petikam. 2024a. "Data Warfare and Creating a Global Legal and Regulatory Landscape: Challenges and Solutions." *International Journal of Legal Information*, 1–11.

___. 2024b. "Global Legal and Regulatory Landscape: Challenges and Solutions." *International Journal of Legal Information*, 1–11. https://doi.org/DOI: 10.1017/jli.2024.22.

Motupalli, Venkat. 2017. "How big data is changing democracy." *Journal of International Affairs* 71 (1): 71–80. https://www.jstor.org/stable/26494364.

Mysyshyn, Anna. 2024. "Advanced Technologies in the War in Ukraine: Risks for Democracy and Human Rights." *The German Marshall Fund*.

Nwanga, Mathew E., Elizabeth N. Onwuka, A.M. Albinu, and O.C. Ubadike. 2014. "Leveraging Big Data in Enhancing National Security in Nigeria." *International Journal of Knowledge, Innovation and Entrepreneurship* 2 (2): 66–80.

Nye, Joseph S. 1990. "Soft Power." *Foreign Policy*, no. 80 (March): 153–71. https://doi.org/10.2307/1148580.

___. 2023. "Soft Power" In "Soft Power and Great-Power Competition: Shifting Sands in the Balance of Power Between the United States and China.", edited by Joseph S Nye, 3–15. Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-0714-4_1.

Offiong, E, Eke Nta, and Inyang Etim Bassey. 2021. "The Role of Information Technology in Enhancing National Security in Nigeria (2001-2020)." *Pinisi Journal of Art, Humanity and Social Studies* 1 (1): 44–53.

Poland, Corrie. 2018. "NATO Focuses on Big Data and Artificial Intelligence ." Energy, Installations, and Environment. https://www.safie.hq.af.mil/News/Article-Display/Article/1548241/nato-focuses-on-big-data-and-artificial-intelligence/.

Porche, Isaac R, Bradley Wilson, Erin-Elizabeth Johnson, Shane Tierney, and Evan Saltzman. 2014. "Big Data:" In *Data Flood*, 1–6. Helping the Navy Address the Rising Tide of Sensor Information. RAND Corporation. http://www.jstor.org/stable/10.7249/j.ctt6wq8rr.9.

RadioFreeEurope/RadioLiberty [RFE/RL]. 2020. "Putin Bans Armed Forces Members From Carrying Electronic Devices, Gadgets." https://www.rferl.org/a/putin-bans-armed-forces-members-from-carrying-electronic-devices-gadgets/30598888.html.

Räsänen, Minna, and James M Nyce. 2013. "The Raw Is Cooked: Data in Intelligence Practice." *Science, Technology, & Human Values* 38 (5): 655–77. http://www.jstor.org/stable/23474819.

Reilly, Brant C. 2015. "Doing More with More." *American Intelligence Journal* 32 (1): 18–24. http://www.jstor.org/stable/26202099.

Rettore, Paulo H L, Philipp Zißner, Mohammed Alkhowaiter, Cliff Zou, and Peter Sevenich. 2023. "Military Data Space: Challenges, Opportunities, and Use Cases." *IEEE Communications Magazine-Series Military Communications and Networks.* https://tinyurl.com/semdam.

Reuters. 2023. "Chinese Hackers Attacked Kenya State Agencies." *The EastAfrican*. https://www.theeastafrican.co.ke/tea/news/east-africa/chinese-hackers-attack-kenya-government-4245006.

Romine, B Harl. 1994. "Intelligence data for tactical commanders." *American Intelligence Journal* 15 (1): 30–38. http://www.jstor.org/stable/44326486.

Sacks, Samm, and Justin Sherman. 2019. "Defining Data Governance." *Global Data Governance*. Concepts, Obstacles, and Prospects. New America. http://www.jstor.org/stable/resrep19968.4.

Shafy Ramadhan, Muhammad Damar. 2023. "The decision to invade: an internal perspective to the russian invasion of Ukraine." *Global: Jurnal Politik Internasional* 25 (2): 29–53. https://doi.org/10.7454/global.v25i2.1283.

Sharma, Ritu. 2023. "Ukraine-Russia War 'Attracts' Tech Firms Keen To Gather 'Invaluable' Battlefield Data & Build Future Warfare Tech." *Eurasian Times.* https://www.eurasiantimes.com/new-invaluable-data-tech-firms-want-a-piece-of-ukraines/.

Shewale, Rohit. 2024. "Google Search Statistics 2024 (Most Searches & Trends)." *Demandsage*. https://www.demandsage.com/google-search-statistics/.

Śliwa, Zdzisław. 2022. "The Synergy between Technology and Soldiers in Warfare: The Russian Armed Forces Image during the War in Ukraine." *Wiedza Obronna*.

The White House. 2024. "Bilateral Security Agreement Between the United States of America and Ukraine." 2024. https://www.whitehouse.gov/briefing-room/statements-releases/2024/06/13/bilateral-security-agreement-between-the-united-states-of-america-and-ukraine/.

Treiblmaier, Alexander. 2022. "Improving Efficiency Through Data-Driven Decision-Making In A Military Environment - ." *TDHJ*. https://tdhj.org/blog/post/data-driven-decision-making-military/.

Tucker, Patrick. 2020. "Russian Arms Production Slowed by Coronavirus, Analysts Find." *Defense One*. https://www.defenseone.com/technology/2020/05/russian-arms-production-slowed-coronavirus-analysts-find/165071/.

Ülgen, Sinan. 2016. "Data flows." *Governing cyberspace*. A Road Map for Transatlantic Leadership. Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep26924.8.

Wang, Huiyao, and Joseph S Nye. 2022. "Power Shifts in the Twenty-First Century" In "Understanding Globalization, Global Gaps, and Power Shifts in the 21st Century: CCG Global Dialogues." edited by Huiyao Wang and Lu Miao, 131–45. Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-3846-7_8.

Wilbik, Anna. 2024. "The Real Value of Data: A Matter of Fusion and Diffusion."

Zabala-López, Alexandra, Mario Linares-Vásquez, Sonia Haiduc, and Yezid Donoso. 2024. "A Survey of Data-Centric Technologies Supporting Decision-Making before Deploying Military Assets." *Defence Technology*. https://doi.org/10.1016/j.dt.2024.07.012.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Artificial intelligence in multidomain operations: a SWOT analysis

Captain (N) (r) Sorin TOPOR, Ph.D.*
Adrian Victor VEVERA, PhD. Eng.**
Alexandru Georgescu, Ph.D.***
Ella Magdalena Ciupercă, Ph.D.****

*National Institute for Research and Development in Informatics ¨– ICI Bucharest/
Associate member of the Romanian Academy of Scientists
e-mail: sorin.topor@ici.ro
**National Institute for Research and Development in Informatics – ICI Bucharest
e-mail: victor.vevera@ici.ro
***National Institute for Research and Development in Informatics – ICI Bucharest
e-mail: alexandru.georgescu@ici.ro
****National Institute for Research and Development in Informatics – ICI Bucharest
e-mail: ella.ciuperca@ici.ro

Abstract

Multidomain operations are a strategic concept that integrates multiple domains of operation (land, sea, air, space and cyber) to achieve common objectives in a complex and dynamic environment. In the context of rapidly evolving technology, Artificial Intelligence (AI) has become an essential tool for optimizing and streamlining multi-domain operations, providing innovative solutions for sectors such as mobility and maneuver of forces and weapons, logistics, decision-making and other military technologies. In this paper, we will highlight the applications, benefits and challenges associated with the implementation of AI in multi-domain operations through a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis and propose some future development directions.

Keywords:
Artificial Intelligence; multidomain operations; SWOT analysis.

Article info
Received: 15 February 2025; Revised: 3 March 2025; Accepted:14 March 2025; Available online: 2 April 2025

Citation: Topor, S., A.V. Vevera, A. Georgescu și E.M. Ciupercă. 2025. "Artificial intelligence in multidomain operations: a SWOT analysis". *Bulletin of "Carol I" National Defence University*, 14(1): 108-121. https://doi.org/10.53477/2284-9378-25-07

The implementation of Artificial Intelligence (AI) in multi-domain operations is considered a turning point that will provide innovative solutions, based on the valorization of all previous experiences and knowledge of the military domain and incorporating not only new capabilities in data processing and decision-making systems, but also other emerging technologies such as augmented reality, quantum cryptography and new cybersecurity models.

However, the success of its implementation depends on the correct approach to weaknesses and threats, as well as capitalizing on strengths and opportunities. In our paper, through SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis we will demonstrate that an army that invests in AI, in a balanced perspective, combining technological innovation with ethical and strategic responsibility, will not only have an essential decision-making support tool but also has a real capability to connect to an increasingly intelligent future.

State of the art - the specificity of using AI in multidomain operations

Initially, multidomain operations were considered a set of operational functions. Today, they represent a central doctrinal element through which modern armies are shaped and soldiers are transformed into fighters capable of facing future military operations. Multidomain operations integrate the use of space and cyber capabilities in land, air and naval operations (FM3-0 2022). This historical stage represents a revolution in the conduct of military operations in that, for the first time, technologies specific to these capabilities were used by adversary forces to challenge decisions and execute offensive measures against their own combined forces.

The operational environment understanding model represents the absolute novelty of this new doctrine. Knowledge of the operational environment is the precursor to any effective activity. It is made up of five domains (land, maritime, air, outer space and cyberspace) and three dimensions (physical, informational and human). For its knowledge and understanding, disruptive technology, especially AI, represents a real support for the collection, analysis and processing of information, support in the development of decisions and in the dissemination of information to autonomous combat platforms or which integrate command-control (C2) systems of different capabilities and specific to each domain.

Cyberspace, one of the five domains of the operational environment, integrates digital networks and information technology infrastructures, resident information, telecommunications networks, computer systems, embedded processors and controllers, relevant frequency bands in the electromagnetic spectrum, etc., into global networks that allow fast connections, anywhere and anytime, as well as the geostrategic context in which they operate (Vevera and Ciupercă 2019). The systems that operate within these networks are of one's own forces, friendly or allied, of

enemies, of host nations or supporters of a cause, communication and mobile telephony systems, social and media networks, and other technical infrastructures such as weapons, autonomous platforms, computers, controllers, etc.

AI has the potential to be the most important technological development of the historical period we are going through, attracting the attention of many specialists in the field of security and defense sciences. In fact, the final report of the US AI Security Commission (Final Report 2025) mentions that this technology is so versatile that a historical parallel can be drawn with the transformative effect of electricity in all fields of human activity, an effect that the American inventor Thomas Edison described as "a field of fields... it holds the secrets which will reorganize the life of the world" (Schmidt 2021).

The current stage of development and implementation of AI is at a level where we can encounter new threats and vulnerabilities, as well as disruptive events, as a result of the large-scale implementation of the technology (Georgescu 2022). This trend shapes international relations and global cooperation frameworks in this area (Ciupercă et al. 2022), stimulating the ambitions of confirming the normative power position in the field of the EU and the USA on the one hand and of China and Russia on the other. These powers seek to implement AI in a sustainable and safe way to maximize the positive impact on their own military, economic and strategic capabilities, but at the same time to ensure that their own and other actors do not generate unacceptable risks to critical infrastructures and digital systems which the functioning of the globalized world depends on. The new operational environment forces military leaders to understand the information relations specific to war through three dimensions, namely: the physical, the informational and the human. In this view, any military activity involves the organization of echelons and the coordinated conduct of their activities in the three directions determined by terms of time, space, and purpose. Thus, the combat power of a dominant operational component is applied to the other components of the combined force, coordination being achieved through unique requirements regarding the organization and conduct of combat.

The major challenge lies in the reality that anyone can use these technologies, adapting them quickly to be used safely and to counteract the effectiveness of previous versions. In this context, understanding the adversary's relative advantage requires understanding the capabilities of all actors involved, the adversary's purpose and objectives, the particularities of the operational environment for the geographical area where the conflict is taking place and, more than that, the influences and interdependent relationships of each domain and dimension. The large number of activities specific to armed conflict, from logistical support to direct combat, leads us to focus on the analysis of a set of challenges and circumstances essential for maintaining the security of forces in the context of increasing the lethality of weapons and combat systems. Of particular interest are the operational-

tactical decisions in direct confrontations, decisions developed with the support of disruptive technologies (AI). These are embodied in battle orders, in the design of courses of action and the choice of the optimal course, in the selection of offensive reaction measures in response to threats from the operational environment and the enemy, and in measures to coordinate efforts and achieve effective cooperation, with potentially lethal consequences.

In some armies, norms and recommendations are developed regarding the use of autonomous systems in combat. For example, regulations regarding the use of precision-guided munitions (fire-and-forget missiles) are designed with systems for monitoring target identification by a human operator, without the possibility of his intervention (DoD Directive 3000.09 2012).

The regulation of the development and use of AI by the armed forces is a complex matter, governed not only at the national level but also at the European level, at the alliance level or at the corporate level. In addition to the emerging national framework, the most important framework is the European one, which seeks to encourage ethical and trustworthy AI through specific legislation (European Commission 2021a), action plan (European Commission 2021b) and voluntary standards generated by High-Level Expert Groups (European Commission 2019) that broadly define no-risk applications, minimal-risk applications, high-risk applications and unacceptable-risk applications, each with different levels of regulation and different emphasis on self-regulation.

The two most important frameworks for a perspective on AI regulation for the armed forces are those created by the US Department of Defense (DoD 2019) and NATO (Stanley-Lockman and Christe 2021), which have a strong compatibility of vision, both being focused on several force principles: accountability, legality, fairness, explicability and traceability, governability, reliability. Here, we should also add voluntary frameworks created by companies in the AI industry or industries implementing AI. These frameworks can be more cost-effective by being specialized on the specific challenges of the respective industry. An example of this is the automotive industry, through the BMW AI governance framework (BMW Group 2020). However, we could also see voluntary frameworks in the arms industry because these companies will want to prevent the risk of overregulation by the state by demonstrating their own responsibility.

The lessons learned from contemporary warfare fully demonstrate that current military technology offers multiple opportunities, with advances in all fields of science establishing fewer and fewer barriers to limiting threats and violence against global peace. Revisionist and revanchist tendencies of some actors will inevitably trigger tensions that will be based on the performance of military technologies and the race to achieve relative balance in military efficiency. AI technology will probably

be the most important for delegating authority to combat systems/platforms, as well as for establishing the level of human control. Choosing the wrong direction in cyber diplomacy, even if it is represented by a set of promises and declarations of intent, will not be able to be blurred, with attenuated effects, without careful prior thinking, without identifying the optimal course from a multitude of scenarios.

In this sense, the analysis of AI technology in the context of multi-domain operations, followed by the identification of possible solutions to solve future challenges and the use of opportunities for beneficial purposes for human safety can bring added value to research and development in the field of military sciences.

Method – SWOT analysis

Based on the existing literature analysis, specific to the field of military sciences, we used the SWOT (Strengths, Weaknesses, Opportunities and Threats) method to better reflect the characteristics of AI in multi-domain operations. The purpose of this analysis is to identify the advantages of developing military applications based on AI, to distill the opportunities for implementing scientific advances in future military operations, as well as the current challenges for the target areas of the ratio of requirements for strengthening human security vs. economic and technological development. We believe that the results of this analysis will provide some guidelines to guarantee a positive change in the development and use of AI technology in support of the decision-making component for organizing and planning multi-domain operations.

As a result of the analyzed literature, we identify the following strengths, weaknesses, opportunities and threats that AI can bring to each area and direction established for multi-domain operations, presented in table no. 1.

Strengths

S.1 – *Automate decisions regarding speed and efficiency*: AI can quickly analyze information from a variety of sources such as: satellites, drones, individual sensors or implemented in combat equipment, etc., can search online scientific publications and propose solutions in the development of strategies or for the efficient coordination of operations that are carried out simultaneously in multiple domains. Autonomous systems, such as drones or land and naval robots, can be supported or even coordinated by AI to perform complex missions without direct human intervention. Sufficiently advanced AI systems can even systematize in real time information from human agents who verbally report changes on the battlefield.

S.2 – *Advanced data analysis capabilities*: AI algorithms can reduce human errors, provide solutions that are more accurate by analyzing large volumes of data and information, execute complex operations and learn to adapt to new situations. They

TABLE NO. 1

Implementing AI in Multidomain Military Operations: A SWOT Analysis

	FAVORABLE FACTORS FOR AI IMPLEMENTATION IN MULTIDOMAIN OPERATIONS	UNFAVORABLE FACTORS TO AI IMPLEMENTATION IN MULTI-DOMAIN OPERATIONS
INTERNAL SOURCE (ARMY)	*Strengths* *S1: Automate decisions for speed and efficiency* *S2: Advanced data analytics capabilities* *S3: Optimized resource consumption and logistics* *S4: Increased interoperability* *S5: Reduced risks to the human component* *S6: Increased precision and lethality to the adversary*	*Weaknesses* *W1: Technology dependency* *W2: High implementation and maintenance costs* *W3: Complexity of integration into current organic structures* *W4: Capital intensity* *W5: Errors in the decision-making process (programming, data interpretation, etc.) with serious consequences* *W6: Cascading compromise of military information systems* *W7: Cyber vulnerabilities*
EXTERNAL SOURCE	*Opportunities* *O1: Development and implementation of technologies* *O2: Integration of knowledge from several scientific fields* *O3: Inter-institutional and international collaboration and cooperation* *O4: Spin-offs and spin-ins as a way to compensate for increased costs*	*Threats* *T1: Use of AI for aggressive purposes* *T2: Ethical and legal challenges* *T3: The problem of human resources in the competition for high-performance AI* *T4: Amplification of the technological gap between national components of the joint forces* *T5: Dependence on the civilian economic environment for specific resources*

can also be used to create predictive models and simulations of operational scenarios, providing essential support for anticipating results and optimizing strategies.

S.3 – *Optimization of resource consumption and logistics*: AI can automate repetitive and complex processes, reducing execution time and the value of the effects of human errors. By analyzing operational requirements and their predictability, it can optimize field distribution, minimizing delays and risks associated with supply. In addition, AI facilitates communication and coordination between operational components involved in a multi-domain operation in real time, protecting critical infrastructure and sensitive information. The application of predictive AI models together with blockchain technologies allows for the secure and efficient management of intelligent, informational and energy networks, allowing for high precision and efficient exploitation of human resources, weapons and combat systems. Especially in multi-domain operations, this aspect represents the rapid and efficient management of resources within the framework of logistical support.

S.4 – *Increased interoperability*: AI technologies can contribute to increased interoperability between different multinational armed forces and host nation or international organizations. AI algorithms can optimize communication between units, even in conditions of great diversity and technological complexity.

S.5 – *Reduced risks to the human component*: Autonomous or semi-autonomous systems can take over risky tasks, increasing the overall security of the mission and the safety of human life. In addition, it can provide personalized experiences, increasing the level of training and training of the military while substantially reducing the physical risks of equipment destruction and injury to the military.

S.6 – *Precision and increased lethality among adversaries*: AI can contribute to increased precision of attacks, identifying targets with precision. Increased lethality can occur through the analysis and prediction of enemy behavior, by increasing autonomy and combat effectiveness, and by developing autonomous weapon systems. Of course, a number of ethical issues arise here that require clarification.

Weaknesses

W.1 – *Technology Dependence*: One of the main risks is related to the excessive dependence on AI that can lead to the loss of essential human critical thinking skills and new types of vulnerabilities, in case of technological and system failures. If an AI-based system were to be affected by a cyber-attack, the entire operational ecosystem could be compromised. On the other hand, resistance to change from decision-makers or operators who fear replacement or loss of their position in the function can represent a threat within the team intended to solve a mission.

W.2 – *High implementation and maintenance costs*: The development and implementation of advanced AI solutions requires considerable resources, both financial and human specialists. These costs include research, algorithm development, specialized infrastructure, specific acquisitions and specialized personnel training programs. In addition, the continuous maintenance and updating of systems to keep them at the highest performance standards is another critical economic factor.

W.3 – *Complexity of integration into current organizational structures*: Integrating AI technology into existing military echelon technologies can be a major challenge. This involves staff training and cognitive changes for operators to quickly adapt to new technologies and abandon traditional technologies and processes.

W.4 – *Capital intensity*: The increased technological capital needs of the defense industry necessary for multi-domain operations can represent a major vulnerability by limiting investments in military equipment as well as in communication systems, cyber warfare, AI, drones, satellites, etc., but also in training personnel to operate effectively in specific military domains. Thus, high operational costs and the risk of economic overload will aggravate economic instability and the capacity to conduct multi-domain operations. Another aspect concerns the lack of long-term sustainability. With the investment sector no longer being managed correctly, the maintenance of equipment and infrastructures will exceed maintenance plans, the collapse of financial and technological support capacities being a clear possibility.

W.5 – *Decision-making errors (programming, data interpretation, etc.) with serious consequences*: Although AI can improve the decision-making process, programming or data interpretation errors can lead to serious consequences. In multi-domain operations, where wrong decisions can lead to high loss of human lives or the escalation of conflicts, excessive dependence on AI without critical human supervision can represent a serious threat. A key issue in this context is the

phenomenon known as the "black box" of artificial intelligence, which refers to the difficulty humans face in understanding and auditing AI decision-making processes. This lack of transparency reduces accountability and limits the ability to optimize algorithms by correcting errors. The consequences of this situation are twofold: AI systems may be unjustifiably accepted, leading to unforeseen and potentially devastating effects, or they may be rejected, hindering competitiveness and widening technological gaps relative to adversaries.

W.6 – *Cascading compromise of military information systems* to affect not only the targeted system but also other components in the network (weapon systems, communications, weapon networks, etc.), with chain effects that endanger the entire operational capacity. Thus, if a domain control system is compromised, for example, a land forces cyber system, the capabilities of the air and naval components will also be affected, disrupting the synchronization and coordination of operations carried out in several directions.

W.7 -–*Cyber vulnerabilities*: AI technology is closely linked to the digital infrastructure and can become the target of cyber-attacks. In addition, the exploitation of programming errors or the admission of information controlled by the adversary during the machine learning process can lead to wrong decisions or mission failure and loss of trust in the technology. Vulnerabilities to cyber-attacks can be amplified by the complexity of communication networks and the large number of connection points of electronic devices in the networks used. Also, the architecture of AI systems can be opaque to military technical support personnel, meaning that the remediation of problems caused by an adversary or errors could only be done by the provider, introducing an additional element of complexity in the planning and conduct of operations.

Opportunities

O.1 – *Development and implementation of technologies*: Disruptive technologies and especially AI can be used to create innovative solutions in areas such as disaster management, crisis management and other multi-domain operations, where rapid coordination between entities of the various components of the combined forces is essential. Innovations in the field of natural language machine learning or digitalized visual observation can be new capabilities that improve operational efficiency.

O.2 – *Integrating knowledge from multiple scientific fields*: The use of AI algorithms allows the integration of knowledge from multiple fields, improving the process of knowledge discovery and decision-making. This approach leverages the strengths of AI technology specific to military applications to provide much more comprehensive information.

O.3 – *Inter-institutional and international collaboration and cooperation*: The use of AI can stimulate collaboration between various government entities and international

organizations, combining expertise from various professional and scientific fields, facilitating the exchange of information and the coordination of resources to resolve transnational events such as terrorism or cyber conflicts. In addition, AI can contribute to identifying solutions to complex global problems such as adapting to climate change or strengthening cyber defense.

O.4 – *Spin-offs and spin-ins as a way to offset increased costs*: The interaction between the civilian and military sectors facilitates the transfer of technology and resources to develop multi-domain operations and to support innovation in both domains. For example, the Internet, GPS and drones are military systems that have been transferred to the civilian sector and have a huge impact on the global economy. Specifically, spin-ins, AI and ML (machine learning), battery and energy storage technologies, autonomous vehicle technology, etc., are being adapted and integrated into the military sector to improve the performance and efficiency of military operations.

Threats

T.1 – *Use of AI for aggressive purposes*: In addition to using AI for defensive purposes, an adversary can also exploit it to increase the aggressiveness of attacks. For example, autonomous drones and cyber-attacks can be used to develop lethal weapons and undermine the defense and security of both operational and national security components. The paradigm of hybrid threats is also undergoing transformations because AI-based systems can implement cyber, physical or electronic attacks on critical infrastructures, as well as disinformation, manipulation and propaganda campaigns, with much lower costs and risks for the actor implementing them.

T.2 – *Ethical and legal challenges*: Responsibility in the use of autonomous weapons as well as the use of AI in autonomous decision-making applications, raises numerous ethical and legal issues. For example, there is no global regulation for establishing responsibility in the event of an error in an autonomous system. We consider the scenario in which an American drone, operated by AI, decided to attack anyone who tries to prevent it from carrying out its orders, including its own operator (Nețoiu 2023). In addition, the use of autonomous weapons may amplify concerns about possible human rights violations.

T.3 – *The problem of human resources in the competition for high-performance AI*: In the context of multi-domain operations, where technology plays an essential role in the success of missions, human resources become a critical factor in both the development and implementation of intelligent solutions and in increasing the shortage of professionals. These will generate significant delays in the development and implementation of innovative solutions, high costs of recruitment, training and retention of personnel, and difficulties in developing an organizational culture for public and military entities. Thus, the costs and resources necessary to ensure continuous professional training of civilian and military personnel will be much higher and will put additional pressure on the already affected budgets of the

institutions. These issues affect all armed forces around the world, regardless of resource abundance, as the relative gap between the private and military sectors remains significant in all countries.

T.4 – *Widening technology gaps between national components of joint forces*: The rapid pace of AI technology development in line with national economic opportunities can lead to technology gaps, which, at the level of national armed forces, establish different levels of readiness to face emerging challenges and threats. Thus, some nations may be vulnerable if they do not invest sufficiently in technological research and development to keep up with the rapid pace of development of disruptive and emerging technologies. A sharp technology gap limits the ability to cooperate with allies, including political and strategic consequences (Stanley-Lockman and Christe 2021).

T.5 – *Dependence on the civilian economy*: AI implementation is subject to increasingly stringent regulations, which can limit flexibility and increase compliance costs, which can erode the interest in their development by a private partner. Developers of AI solutions with military potential may be targeted by an adversary for sabotage, data theft or infiltration into systems to distort the functioning of AI systems or provide access to other military systems. Last but not least, the global economic model that emphasizes the mobility of capital has resulted in numerous instances in which critical entities in the development of technologies with dual potential have been taken over partially or entirely by an entity from a rival/adversary state, possibly also in coordination with the armed forces or intelligence services of that state (such as China's digital and electronic technology companies). Also, the dependence of military entities on critical civilian communications or energy networks can affect the conduct of a multi-domain operation by importing vulnerabilities specific to civilian infrastructures to physical and cyber-attacks by the enemy. In addition, if civilian economies are not sufficiently robust or resources are limited, they can generate difficulties in providing materials and logistical services, aspects that can lead to conflicts of priorities between civilian and military infrastructures. In the case of AI, military actors in countries with limited resources can end up depending on civilian suppliers not only for the development of specific AI solutions but also for computing capacity, data sets or other services under the Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS) paradigm. Last but not least, a global or regional economic crisis can affect both the civilian and military sectors, generated, in particular, by economic sanctions and trade blockades that will limit access to external resources.

Discussions on the interaction of the analyzed elements

Capitalizing on strengths and opportunities can counterbalance weaknesses and threats and create advantages for the development of divergent and disruptive technologies, through AI. Information created based on AI can quickly reform

multi-domain operations strategies as well as contribute to identifying opportune operational requirements for the development of combat means and platforms. The identified opportunities can eliminate threats (except T2).

The ethical and legal aspects that are included in T2 cannot be eliminated through AI development opportunities, which are related to the human factor. Thus, concurrently with these developments, a reconversion of the military career and professional specialties is necessary; therefore, university training programs must be adapted to the particularities of hybrid warfare, with an emphasis on innovative ways to identify solutions to deal with the listed threats, independently, at the level of each decision-making echelon.

In addition, based on the strengths, plans can be developed to develop new opportunities in industry and military education, with military bases becoming centers for the development of the regional economy (Topor 2024). To do this, mindsets must be changed, and initiatives regarding equipment, acquisitions and education must be prioritized based on impact studies according to the ultimate objective, namely maintaining national security and defending the population, resources and critical infrastructures.

Anyone using an internet search engine will be able to observe a paradox, namely that simultaneously with the evolution of revolutionary technologies such as AI and quantum computing, more and more malicious cyber actors are attacking critical infrastructures such as: communication and energy networks, banks and financial services, other critical infrastructures and even the citizens of a country. The purpose of these actions is to degrade the economic capacity of a state, to degrade the defense capacity, to limit or sabotage the production of critical goods and services including for the armed forces, but also to demoralize the population, to prove the attacker's power for psychological coercive purposes and to undermine the trust in authorities of citizens but also of partners, allies and investors. Moreover, it is recognized that a contemporary conflict is staged and takes place predominantly in the digital domain.

Under this approach, we appreciate that strategies based on the SWOT combination can transform and strengthen the security of multi-domain operations based on AI, maximizing their growth and stability by:

- Government support for investments in the development of companies that produce electronic chips and conductors, as well as for those that develop critical AI infrastructure. They can be achieved through strategic approaches to trade and import/export policies that help Romanian companies develop and create data centers and digital platforms whose services could be exported worldwide;
- Government support for the effective governance of the development of ethical and trustworthy AI systems by ensuring reliability, transparency, accountability and other attributes of safe AI systems enshrined in the European and NATO frameworks. An important role is played by the state's

involvement in ensuring secure sources of relevant data for training AI models. Poisoning of datasets for AI models is one of the most insidious new cyber threats, and safe and trustworthy datasets have become a critical national resource to identify, protect and capitalize on (Sambucci and Paraschiv 2024);
- Development of competent leadership, especially in the procurement and technology implementation sectors. AI generates effective solutions, but without the critical thinking of human leadership, gains in efficiency, costs, and security will not be maximum. All national communities, including the military and intelligence, must streamline their procurement services, modernizing based on AI, cloud and revolutionary technologies, whose exploitation period is relatively very short, due to their constant renewal. Hence the need to outsource such services, which through blockchain technology can ensure a high level of information security;
- Development and multiplication of public-private collaborations in the field of cyber defense. The expansion of identified threats to other areas, not only that of military operations, will affect governmental and economic relations of the spin-ins type, with rapid effects on the combat power of all military components involved. In this regard, strengthening the existing effort to institutionalize operational collaboration will allow private sector agencies and companies to act more quickly to respond to incidents and to support national institutions in blocking cyberattacks. In addition, international institutional collaboration relationships in the field of cyber defense can be formed and strengthened. This way, good practices can be exchanged and popularized, collaborative procedures can be established to discover vulnerabilities in software, and safe and secure models can be built that are constantly adapted to new AI security challenges.

Even though AI is and will remain a subject and goal of interstate competition for a long time to come, it must be accepted that it also represents a huge potential in the field of economic and military development. This strategy can materialize in operational plans that transform inter-institutional cooperation into directions for the development of AI technologies in order to establish safe and sustainable adoption models. Thus, the transatlantic dialogue and cooperation between the US and the EU is to occupy one of the most important roles in the face of China's tendencies, and implicitly other countries, to gain hegemonic positions in the AI competition to determine future superpowers.

Conclusions

Artificial intelligence is an emerging digital technology with systemic impact, which can also have a transformative effect on multidomain operations. Within these operations, AI-based systems can perform data collection and analysis roles, support decision-making, facilitate communication and interoperability between actors

and systems, and occupy concrete functions in the order of battle, such as logistics and maintenance optimization roles, cyber attacker and defender roles, but also autonomous systems operation roles. In a military context, all these functions bring significant benefits. In the context of multi-domain operations, in the five domains identified by NATO (air, water, land, space and cyber), the role of AI will be vital to ensure the congruence, coordination, effectiveness and flexibility of the forces engaged in such operations. In this article, a SWOT analysis was conducted on the field of AI in the military context, which resulted in a series of recommendations for the Romanian authorities. The existing framework for cross-border cooperation in the military field on the regulation of the ethical and responsible use of AI was also analyzed based on the risks of corruption by adversaries or the malfunction of these complex and difficult-to-repair systems. We believe that further research can lead us to concrete standards for the implementation of AI in military systems, including weapons systems, that are compatible with the NATO and European frameworks, and that ensure not only the necessary capabilities for the armed forces in multi-domain operations, but also a leveling factor against a potential adversary with more numerous military resources.

References

BMW Group. 2020. *BMW Group Code of Ethics on AI.* https://www.bmwgroup.com/content/dam/grpw/websites/bmwgroup_com/downloads/ENG_PR_CodeOfEthicsForAI_Short.pdf.

Ciupercă, E.M., C.E. Cîrnu, A. Stanciu, and I. Cristescu. 2022. "Leveraging socio-cultural dimension in cyber security training." *EDULEARN22 Proceedings.* ISBN: 978-84-09-42484-9, ISSN: 2340-1117. pp. 5242-5248. doi:10.21125/edulearn.2022.1239.

DoD. 2019. "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence." Defense Innovation Board, USA. https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.

DoD Directive 3000.09. 2012. "Autonomy in Weapon Systems." U.S. Department of Defence. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

European Commission. 2021a. "COM (2021) 206 final Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

European Commission. 2021b. "Coordinated Plan on Artificial Intelligence 2021 Review." ANNEXES to COM(2021) 205 – Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A205%3AFIN.

—. 2019. *Ethics guidelines for trustworthy AI. High-Level Expert Group on AI.* https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Final Report. 2025. National Security Commission on Artificial Intelligence, p. 20. https://assets.foleon.com/eu-central-1/de-uploads-7e3kk3/48187/nscai_full_report_digital.04d6b124173c.pdf.

FM3-0. 2022. "Operations." Headquarters, Department of the Army. https://irp.fas.org/doddir/army/fm3-0.pdf.

Georgescu, A. 2022. "Cyber Diplomacy in the Governance of Emerging AI Technologies – A Transatlantic example." *International Journal of Cyber Diplomacy,* (ISSN 2668-8662) vol. 3: pp. 13-22. https://doi.org/10.54852/ijcd.v3y202202.

Nețoiu, R. 2023. "Noile drone controlate de inteligența artificială îi omoară chiar și pe operatorii lor. Scenariul Terminator de care se teme armata SUA." *Digi24.ro.* https://www.digi24.ro/stiri/externe/noile-drone-controlate-de-inteligenta-artificiala-ii-omoara-chiar-si-pe-operatorii-lor-scenariul-terminator-de-care-se-teme-armata-sua-2372223.

Sambucci, L., and E.A. Paraschiv. 2024. "The accelerated integration of artificial intelligence systems and its potential to expand the vulnerability of the critical infrastructure." *Romanian Journal of Information Technology and Automatic Control* (ISSN 1220-1758) 34 (3): 131-148. https://doi.org/10.33436/v34i3y202410.

Schmidt, E. (coord.). 2021. "Final Report - National Security Commission on Artificial Intelligence." NSCAI, Washington DC, US. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

Stanley-Lockman, Z., and E.H. Christe. 2021. "Summary of the NATO Artificial Intelligence Strategy." *NATO Review.* https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html.

Topor, S. 2024. "The Contribution of Military Research and Development (R&D) to the Developent of the Regional Economy." *Romanian Cyber Security Journal* (ISSN 2668-6430) 6 (2): 85-93. https://doi.org/10.54851/v6i2y202408.

Vevera, A.V., and E.M. Ciupercă. 2019. "The dimensions of CYBER WARFARE in the sino-russian space." *Romanian Cyber Security Journal* 1 (2): 31-36. https://rocys.ici.ro/documents/57/2019_fall_article_3.pdf.

Xinhua. 2024. "China accelerates AI development to build AI innovation center." *English.gov.cn., The State Council, The People's Republic of China.* https://english.www.gov.cn/news/202404/06/content_WS6610834dc6d0868f4e8e5c57.html.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Challenges of equipping with 155 mm self-propelled howitzer systems from a DOTMLPF-I perspective

LTC Adrian MIREA*

*"Carol I" National Defence University, Bucharest
e-mail: mirea.adrian@yahoo.com

Abstract

Fire support systems represent a combat power multiplier for force structures, making a significant contribution in all types of operations, as they directly facilitate the force's ability to accomplish its mission. Considering national programs for equipping with modern military systems, this article has addressed the potential challenges of transitioning land force structures from being equipped with 152 mm towed artillery systems to NATO standard 155 mm self-propelled artillery systems. The challenges have been considered through the lens of the NATO capability foundation model, described by the acronym DOTMLPF-I (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability). This paper aims to underline some aspects that may influence the integration and exploitation of fire support capabilities, provided by equipping national land forces structures with this type of 155 mm self-propelled howitzer system. I have structured the article into two sections, aiming in the first part to briefly present the relevant basic ideas of the NATO capability foundation model, and in the second part to argue the challenges of equipping with 155 mm self-propelled howitzer systems and to include some actions, which I consider necessary, on the eight directions described by the acronym DOTMLPF-I. The perspective presented aims to highlight useful ways to enhance the national-level fire support capability provided by the new NATO-standard 155 mm self-propelled howitzer systems.

Keywords:
equipping; fire support; self-propelled howitzer; NATO model; DOTMLPF-I.

Article info
Received: 12 February 2025; Revised: 3 March 2025; Accepted: 7 March 2025; Available online: 2 April 2025

Citation: Mirea, A. 2025. "Challenges of equipping with 155 mm self-propelled howitzer systems from a DOTMLPF-I perspective". *Bulletin of "Carol I" National Defence University*, 14(1): 122-135. https://doi.org/10.53477/2284-9378-25-08

Equipping national land forces structures with 155 mm self-propelled howitzer systems implies, first and foremost, a revision of the doctrines and combat manuals in force concerning the use of these systems in operations. National armed forces structures will be able to exploit the new fire support capabilities acquired both in combat operations, in stability and support operations and for peace support operations. Thus, existing doctrines, combat manuals or various operating procedures will have to be adjusted or updated in some way to allow the potential of these capabilities to be exploited in the actions and activities carried out by force structures in all types of operations.
Updating the current doctrinal framework is not the only measure needed to integrate and exploit the full potential of the new fire support capabilities that will be introduced in land force structures. In order to have a more comprehensive perspective on all the implications of this new equipment, I have used the NATO capability foundation model (NATO 2021, 7) with the eight action lines described by the acronym DOTMLPF-I (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability).

In writing this article I applied the method of documentary analysis as a research method for the systematic review and evaluation of physical and electronic documents (Bowen 2009, 27) in the field of study. Being a method specific to qualitative research, the documentary analysis in this case involved the examination and interpretation of data on the equipping with 155 mm self-propelled howitzer systems, in order to be able to understand the implications of the substantiation of the new capabilities obtained by the national armed forces structures. *"What are the implications of equipping with 155 mm self-propelled howitzer systems from the perspective of the NATO capability foundation model?"* is the research question that I set out to answer in this paper. To this end, I explored open sources of information - mainly websites, NATO-level publications and authored papers, detailing the conceptual way of capability foundation as well as relevant aspects of military equipping and exploitation in operation, so that I can argue for actions needed at national level on the eight directions described by the NATO model.

According to the Army Media Agency's website we have, as a strategic objective, the modernization of the Romanian Army through the development of capabilities according to the Romanian Army 2040 program and the Multiannual Plan for Equipping the Romanian Army, which includes a program for the equipping with Battalion level 155 mm self-propelled howitzer system (Bâtcă 2024). The systems agreed upon at the national level are the 155 mm self-propelled howitzers - K9 Thunder (Curtifan 2024) and the contract with the Korean manufacturer Hanwha Aerospace, foresees the acquisition of 54 K9 self-propelled howitzer systems and 36 K10 refuelling vehicles.

The equipping of land forces structures with such systems will lead to doctrinal and organizational changes, in terms of how to use self-propelled howitzers in operations,

in order to exploit the full potential of these modern fire support platforms. In addition, the novelty and specific nature of self-propelled howitzer systems will also create a need for tailored training of military personnel, both for their operation and maintenance and for their timely exploitation in accordance with the operational needs of the force structures they will be part of. From another perspective, the commissioning of the new systems will only take place once the organizational status of the designated structures has been updated and the territorial infrastructure and the quantities of materials of all classes of supply will ensure the minimum necessary for the proper operation and maintenance of the howitzers. In my view, these aspects presented argue the need to identify the measures required at the national level, along the eight lines of the NATO capability foundation model.

Figure 1 NATO capability foundation model
Source: Adaptation in accordance with MD Harris Institute 2013

How can we use the NATO capability foundation model?

The NATO capability foundation model, described by the acronym DOTMLPF-I, is a comprehensive standardized methodology (Willi 2016) in my view, that can be used to assess the impact of equipping national land force structures with 155 mm self-propelled howitzer systems. The NATO model is also a useful tool for the identification of potential needs for preliminary enhancement of the forward-looking capability in the eight action lines under the acronym DOTMLPF-I. The exploitation of the fire support potential that self-propelled howitzer systems can have in an operation, depends on a multitude of factors that can be addressed within the aforementioned action lines. This comprehensive perspective will ensure, in my view, the maximum level of effectiveness of 155 mm self-propelled howitzer systems in national armed forces structures operations.

The actions identified in the *doctrine* direction aim primarily at standardization, so that specific activities and actions are carried out according to the same "best practice guide" implemented uniformly across force structures. The common doctrinal framework ensures clarity and efficiency in the exploitation of the capability and is the basis for training personnel in the accomplishment of their missions so that the capability can be effectively exploited according to operational needs.

Concerning the *organization's* direction, the actions aim at achieving the optimum operational effectiveness of force structures. Efficient organization involves clearly establishing the command authority and the role of personnel within the structure so that the objectives set can be effectively achieved. The level of coordination of component elements and structural functionality determines the maximum available capability potential.

The *training* actions aim to ensure and maintain the optimal level of training for the force structure personnel in order to be able to perform their specific tasks effectively in all types of situations or scenarios. The purpose is to build and maintain a competent and flexible force structure capable of accomplishing its mission in a dynamic operational environment. Force education and training are indispensable to performance and ensure the ability to meet all operational challenges. The way in which training is carried out is clearly established by the normative framework in force, which includes doctrines, field manuals and regulations with specific tactics, techniques and procedures.

The actions identified in the field of *materiel* are aimed at the efficient management of military equipment and materiel so that the capability in question is permanently operational. This line of action covers all military equipment throughout its life cycle, including all aspects of the logistic support required by force structures.

As far as *leadership* is concerned, the actions in this direction focus on the training of military leaders with emphasis on the development of their specific skills and competencies – high level of professional knowledge, integrity, responsibility, adaptability, etc. The exploitation of a capability directly depends on the level of professional competence of military leaders, as they train the force structure personnel and influence their operational effectiveness. Moreover, military leaders are also those responsible for initiating the process of adaptation of the military organization at the tactical and institutional levels (Nistorescu 2024, 205).

The identification of actions in the *personnel* direction is aimed at staffing force structures with highly qualified personnel, able to exploit the full potential of the capability pursued. The available human resources influence the capability's level of operability, the effective management of individuals in positions/functions suited to their skills and competencies ensuring a force structure truly capable of accomplishing the entrusted mission. Actions in the area of *personnel* also aim at maintaining the health and morale of individuals with a direct impact on the performance and operability of the pursued capability.

Actions in the *facilities* direction are mainly aimed at providing the required infrastructure in order to properly operate and maintain the operational status of the targeted capability. This also includes those actions resulting from assessing conformity or operational status of existing national facilities, including those in

barracks or road communications to be operated by the new capabilities. Military personnel and equipment must be provided with all those elements of infrastructure – spaces, buildings, utilities, etc., on which the operational status of any capability is directly dependent.

The *interoperability* action line can be explored through its three domains – technical, human and procedural interoperability. Actions in this direction aim at both the component elements' interoperability of a capability and its interoperability as a whole with other elements, systems or capabilities already existent or deployed. As this article explores the way to apply a NATO capability foundation model, interoperability is an integrating element of all the action lines addressed.

What are the implications of equipping with 155 mm self-propelled howitzer systems?

The utility of the NATO model detailed above is reflected in ensuring the operational effectiveness of the new capabilities by focusing the effort on each direction of the DOTMLPF-I acronym. Some requirements can thus be identified for updating, adjusting or harmonizing the existing doctrinal normative framework, the current logistic support and the way in which the beneficiary force structures must reorganize or train so that the new capabilities acquired can be exploited and leveraged according to the purpose for which they were developed and acquired.

The perspective presented below comes as a response to the research question *"What are the implications of equipping with 155 mm self-propelled howitzer systems from the perspective of the NATO capability foundation model?"*, arguing potential actions along the eight strands of the DOTMLPF-I acronym, thus applying a method of analysis used at the alliance level (NATO 2018).

***Doctrine* direction**

The current doctrinal normative framework does not detail how self-propelled artillery systems are to be employed in operations. Although the artillery missions and the specific lethal/nonlethal tasks they accomplish in an operation are basically the same for all fire support systems, the employment of the new 155 mm self-propelled howitzer systems has some particularities. A first doctrinal action would be to detail and integrate the particularities of the use of self-propelled howitzers in the current doctrinal normative framework, so that their superior characteristics – mobility, firepower, maximum striking range, automated fire control system, etc., can be used in the actions of land force structures.

Considering as starting points the specific documentation provided by the manufacturer, alongside the training and expertise gained by the military personnel involved in the takeover from the Korean partner, we will have to develop (update)

our own doctrines, field manuals and specific regulations to clarify how to use in combat the new 155 mm self-propelled howitzer systems. In my view, the relevant publications available from the alliance or NATO member militaries operating such tracked self-propelled howitzers will prove useful in this regard. Exploiting the potential of 155 mm self-propelled howitzer systems can also be the subject of joint operations, but in my view, this should be done based on a joint fire support doctrine, a national-level necessity that I have argued in another paper: "Implementing a joint fire support doctrine - a requirement of joint operations". (Mirea and Stanciu 2024)

Another action that I consider necessary in the *doctrine* direction is implementing in current national doctrines, field manuals and regulations, those lessons learned in recent conflicts within which tracked self-propelled artillery systems (M109, PZH2000, AS-90 and Krab), similar to those that will be used in our national land forces structures, have proven their relevance and operational effectiveness. In addition, the increased interest of Western armies (Vlad 2024) in the development of the conflict in Ukraine is recognized, as they have the opportunity to test in combat both military equipment and doctrines in force. The need to implement the lessons learned in recent conflicts is all the more obvious if we consider that, at the national level, the last self-propelled tracked artillery systems (the Romanian self-propelled howitzer cal. 122 mm, md. 1989 - **2S1**) were removed from our land force structures in 2005 (Stroea and Băjenaru 2010).

***Organization* direction**

The new 155 mm self-propelled howitzer systems are operated by a small number of crew members compared to the towed artillery systems they will replace, and this will also be reflected in the organization of beneficiary artillery structures. If the 152 mm towed artillery usually had a total of 8 crew members (Military-history Fandom 2025), the new 155 mm self-propelled artillery systems, have 5 crew members (Global Defense News 2024). In addition to the implicit issues of reorganizing personnel currently assigned to the new structure, certain challenges arising from the reduction in the number of servicemen operating self-propelled systems must also be considered, such as the challenges of providing the physical protection needs of force structures, like: guard duties (in peacetime) or the close defence of firing positions (in wartime). Another challenge caused by the reduction in the number of servicemen is the operation of self-propelled howitzer systems for long periods of time, specific to a high-intensity conflict, where the physical and mental attrition of the personnel involved (24 hours a day) is an important element that can influence the very combat power of the artillery structure as a whole.

Following the analysis of the above-mentioned implications, actions in the *organization's* direction will also include, in my view, an appropriate resizing of personnel structure (including, for example, one or more guard/military police/ infantry sub-units), as well as a review of specific tactics, techniques and procedures, thus reducing the risks associated with the downsizing of the new self-propelled

tracked artillery units/sub-units. The artillery structure must have the appropriate regulatory framework and the resources of all types in order to be able to accomplish its mission both in peacetime and in war.

***Training* direction**

Given that, as mentioned, the last self-propelled tracked artillery systems were removed from our land force structures in 2005 (Stroea and Băjenaru 2010) both the training of personnel, directly involved in the operation of the new self-propelled howitzers and of those involved in their operational exploitation, have a lot of catching up to do. Until the doctrinal normative framework is established (updated) we will use for training purposes the specific documentation provided by the manufacturer with the expertise gained by military personnel involved in equipment takeover from the Korean partner and the publications in the field available at the alliance level or at NATO member armies equipped with tracked self-propelled howitzers. Moreover, lessons learned from recent conflicts such as the one in Ukraine, where, as mentioned above, tracked self-propelled artillery systems (M109, PZH2000, AS-90 and Krab), similar to those that will be used in our national land force structures, have proved their operational effectiveness.

Another *training* action aims at specific training of force structure staff through command post exercises, field applications, joint exercises, etc., in order to integrate the potential of self-propelled howitzers into all operational processes. The advantages and disadvantages of exploiting the new capabilities in operations must be understood by all the personnel of the beneficiary force structures, especially those responsible for planning and providing fire support using such systems.

Given the fact that Romania is a member of the ASCA community (Artillery System Cooperation Activities) (Orjanu 2023), and that 155 mm self-propelled howitzers have modern fire control systems interoperable at the NATO level, it offers the possibility of implementing specific actions in the *training* direction, through the integration and participation of national land force structures equipped with such systems in training activities conducted in a multinational context. In addition to joint training with members of allied and partner armies (Statul Major al Apărării 2021), the benefits of involvement in such training activities include the validation of the doctrinal normative framework on the use of new capabilities in operations and the possibility of implementing lessons identified (including from recent conflicts), aspects which provide an up-to-date perspective on the potential of self-propelled howitzers.

***Materiel* direction**

The availability of modern equipment in accordance with the equipping programs (Ministerul Apărării Naționale 2025) generates, as mentioned above, multiple challenges for the force structures (updating the doctrinal normative framework, the need for reorganization, training, etc.) so that the newly acquired capabilities can be exploited according to the purpose for which they were purchased. Some of the

challenges of equipping with modern systems stem from the need for harmonization, at least in the first phase, regarding the use of new capabilities together with old or existing ones at the force structure level. Thus, until we replace all 152 mm artillery systems, there will probably be a transitional period during which the two types of artillery systems – 152 mm towed and 155 mm self-propelled, will be operated simultaneously. A first action in the field of *materiel* would be, in my view, to review logistic support at the force structure level to ensure the operability of new and old capabilities alike, at least during the transition period. Resourcing new and old capabilities alike will entail a considerably greater effort for logistic structures given the different needs for fuels, lubricants and maintenance products, 152 mm and 155 mm NATO standard munitions or 12.7 x 99 mm NATO standard munitions).

Another action on *materiel* is to review the current national equipping rules. The revision of the organization of the land force structures directly benefiting from new equipment must be accompanied by a revision of the rules of equipping with all types of resources so that the specific needs of the new capabilities are covered from all points of view. In my opinion, all materiel quantities available to force structures equipped with modern systems should be reviewed in order to identify possible shortfalls in the efficiency of the units in their core mission. The main argument is that the changes brought about by equipping with 155 mm self-propelled howitzer systems, will have an impact on all the elements that define the structure of the operation (displacement of forces, available fire system or engineer support). The quantities of military equipment and materials of all types available to the force structures must ensure operational effectiveness in all respects.

***Leadership* direction**

Training military leaders represents an outcome of the entire educational process and the development of their skills and competencies is based on the training, and adequate professional and personal development of individuals. Equipping with modern self-propelled artillery systems will determine, as a first step in the *leadership* direction, the identification, promotion and filling of command positions, starting from the lowest hierarchical level, with the most suitable available personnel with the appropriate level of training, skills and qualities of military leadership. The operational effectiveness of the newly acquired capabilities will depend on these personnel. From a different perspective, the attractiveness of positions will be higher in these structures targeted for equipping with modern artillery systems, and will probably generate competition, including for leadership positions in such structures, a positive aspect that will result in a larger selection base and in identifying the most suitable personnel for the available positions.

Another action in the *leadership* direction is, in my view, to update the curriculum of career courses for field artillery officers, in order to include in the professional training of current and future military leaders the study of new self-propelled artillery systems with their specific technical and operational features. In my view,

the same *leadership* direction actions also include the appropriate professional training of command post staff members responsible for planning and integrating fire support into operations. The fire support coordinator (at the brigade level he is also the commander of the organic artillery battalion) together with his staff are the 'first' specialists in the operational exploitation of self-propelled howitzer systems and are also responsible for training subordinate personnel to exploit the full potential of the new fire support capabilities in operations.

***Personnel* direction**

The novelty of modern capabilities, which are or will be part of our national armed forces structures, makes them more attractive and is thus an argument in favour of increasing the professional quality of the military personnel directly involved in their exploitation. As stated in the leadership direction, the attractiveness of available positions in the structures targeted for equipping with modern artillery systems is likely to generate greater competition for their recruitment – with a larger selection base, the professional quality of the personnel recruited will also be higher. A major challenge, in my opinion, will be the staffing of functions that are novel for the current artillery structures, such as the driver functions for each tracked vehicle in the perspective organization. There is thus a need for action on the *personnel* side in terms of retraining existing personnel (to receive a certificate of professional competence as drivers), specific training of new soldiers in training centres (Agenția Media a Armatei 2017) or identification of those already certified. This is a requirement to transition from towed artillery structures – with truck drivers – to self-propelled artillery structures - with specialized drivers, and certified personnel who will be on every K9 self-propelled howitzer, every K10 supply vehicle, every K11 fire control vehicle, and also on other armoured vehicles that the acquisition contract include.

Once the positions are filled with the most suitable individuals, another *personnel* action will be the development (consolidation) of professional knowledge and skills of all personnel involved in the operation and exploitation of the new capabilities. By the time the new self-propelled howitzers arrive in the country, at least some of the personnel of the structures concerned will be involved in training activities adapted to the requirements of the new systems. This training may take several forms, including participation in specialization courses organized by the manufacturer of the systems, by prior training of a small number of soldiers on the *train the trainer* basis, or it may be carried out gradually directly in the units which will be equipped with the new systems during their arrival in barracks. In either case, there will probably be a transition period necessary for the personnel involved in operating the new systems to be trained in order to switch to the new organization of artillery structures and achieve full operational capability.

Another *personnel* action that I consider necessary is the training of responsible staff members on how to capitalize on the new capabilities in operations. In addition to

the aforementioned action to train military leaders, the training of all personnel involved in the planning and integration of fire support into the operation, as well as in the target management process, should be considered. Command post exercises are a good opportunity, in my view, for members of the various cells or working groups with responsibilities in the field of fire support and target management, to visualize and practice ways to exploit the full potential of the new capabilities available.

***Facilities* direction**

A first action in the *facilities* direction would be to assess the infrastructure of the territorial units (if it has not been done so far), where the new self-propelled howitzers will be exploited and maintained in operational condition. The aim is to identify possible shortcomings in ensuring the minimum required conditions for the physical protection, safe operation and proper maintenance of all components and materials intended for the new systems. I appreciate that such modern equipment has a higher sensitivity in terms of requirements for preservation, operation and specific maintenance compared to the towed artillery systems they will replace. A further argument for the need to assess the available infrastructure may be the different requirements for palletization, transportation and storage of 155 mm munitions. Such an assessment may highlight some related needs for the beneficiary territorial units, such as the need for forklift trucks, the need for reworking of the earth cover and protection for storage or the need to keep storage spaces within certain temperature and humidity limits. Enforcing new, NATO level, regulations may be required in order to properly secure storage conditions for the new 155 mm munition type (e.g. *AASTP-1 Manual of NATO safety principles for the storage of military ammunition and explosives*).

I will mention among the ongoing actions at the national level in the direction of facilities, the commitment of our defence industry in the opening of assembly lines and production of the K9 self-propelled howitzer starting in 2026 (Defense Romania 2024), and with the entry into the country of the first systems, will begin the production of 155 mm NATO standard munitions (Grădinaru 2024). Once materialized in the form of production units, these actions at the national level will ensure the operability of 155 mm self-propelled howitzer systems without the land force structures being dependent on any external manufacturer or supplier of components and materials.

Another action in the *facility's* direction is to analyze the opportunity of setting up or delimiting a training range within national territory that would allow firing at long distances to test, for example, the accuracy of 155 mm rounds fired at maximum range. We should consider that the transition from 152 mm calibre ammunition to the standard NATO 155 mm calibre ammunition will make it possible to engage targets at long distances, with higher lethality and accuracy than with 152 mm rounds. The munition used by the K9 self-propelled howitzer systems can hit

targets at ranges of 30 km (with standard explosive projectiles) and 40-50 km using rocket-assisted projectiles - RAP (Global Defense News 2024; European Security & Defence 2022). The existing nationally approved training areas ensure the firing of artillery munitions within certain limits. In my opinion, the possibility of firing 155 mm self-propelled howitzers at maximum range on national territory (perhaps offshore?) should be considered or, failing that, a solution should be identified in a suitable range of an allied or partner state, so that this new capability-specific target engagement solution can be periodically tested and validated. The utility of using such a range can also be extended to other systems in the current or prospective equipping of national armed forces structures, for example, to M142 HIMARS (High Mobility Artillery Rocket System) or Bayraktar drones.

***Interoperability* direction**

The capability foundation model described by the acronym DOTMLPF-I is a NATO model, and at the alliance level, interoperability itself is a force (NATO 2023). The interoperability requirements for elements of the new capabilities, provided by equipping with 155 mm self-propelled howitzer systems, should be analyzed from the perspective of its three domains - technical, human and procedural interoperability.

From the perspective of technical interoperability K9 155 mm self-propelled howitzers come with automated fire control systems that will most likely be integrated into the IFATDS (International Field Artillery Tactical Data System) already operated by national structures equipped with HIMARS. As this is an international command and control system, it can be estimated that K9 155 mm self-propelled howitzers ensure a high degree of technical interoperability. The above-mentioned actions on *facilities*, concerning the local production of 155 mm ammunition, sub-assemblies and K9 systems also used by other allied armies, reinforce the high degree of technical interoperability of the new capabilities.

A necessary action in the technical interoperability direction is, in my view, to ensure the compatibility of 155 mm self-propelled howitzer systems with current and future systems intended for command and control of force structures and for ISR (Intelligence, Surveillance and Reconnaissance). The superior characteristics of the new self-propelled howitzer systems and their full operational potential can only be exploited in operations if they are combined with equally high-performance command and control and ISR systems.

Human and procedural interoperability will be ensured in particular through the above-mentioned actions in the *doctrinal*, *leadership* and *personnel* directions. Intending to update the doctrinal framework and implement tactics, techniques and procedures specific to operating 155 mm self-propelled howitzers, in a form similar to those in force in allied armies, I believe that they will constitute a common basis for the professional training of personnel and for the participation of force structures, equipped with self-propelled howitzers, in military exercises in an allied or multinational context.

Conclusions

Equipping land force structures with modern military equipment, according to our developing national programs, comes with some challenges in terms of ensuring all the necessary conditions to exploit the full potential of the new capabilities thus acquired. Updating the doctrinal framework in force, reorganizing the force structures directly involved in operating the new systems or ensuring the infrastructure and facilities corresponding to the new requirements, are just some of these challenges. In addition to the operational impact of the new capabilities, a comprehensive perspective on equipping with modern systems can, in my view, be achieved by addressing all areas influenced by the implementation of current or prospective acquisition programs.

I believe that the NATO capability foundation model, described by the acronym DOTMLPF-I, is a useful tool for analyzing the implications of equipping with 155 mm self-propelled howitzer systems and, through this paper, I was able to argue its relevance. Focusing on each of the DOTMLPF-I model's eight directions for action, I have highlighted potential shortfalls in exploiting and harnessing the new capabilities and presented some actions to eliminate or mitigate the influence of these shortfalls. I have thus come up with a reasoned answer to the question *"What are the implications of equipping with 155 mm self-propelled howitzer systems from the perspective of the NATO capability foundation model?"*.

Assumed capabilities, for strengthening the national defence capacity and as a contribution to NATO collective defence, must be analyzed from both an operational perspective and through DOTMLPF-I type instruments, as some related procurement requirements, harmonization or optimization needs for the current context of deployment can be identified. On meeting these needs may depend the actual ways of exploiting the new capabilities in operations.

References

Agenția Media a Armatei. 2017. „Curs de brevetare mecanici conductori." https://presamil.ro/curs-de-brevetare-mecanici-conductori/.

Bâtcă, Marius. 2024. „Programele de înzestrare, adaptate la riscurile și provocările actuale." *Agenția Media a Armatei.* https://presamil.ro/programele-de-inzestrare-adaptate-la-riscurile-si-provocarile-actuale/.

Bowen, Glenn. 2009. "Document Analysis as a Qualitative Research Method." *Qualitative Research Journal* 27-40. https://doi.org/10.3316/QRJ0902027.

Curtifan, Tudor. 2024. „Offsetul pentru obuziere: K9 Tunetul va fi produs în colaborare cu industria din România. Dar într-o fabrică ridicată de la zero." *Defence Romania.* https://www.defenseromania.ro/offsetul-pentru-obuziere-k9-tunetul-va-fi-produs-in-colaborare-cu-industria-din-romania-dar-intr-o-fabrica-ridicata-de-la-zero_629372.html.

Defense Romania. 2024. „Când am putea avea obuziere K9 „made in Romania", parte dintr-un plan mult mai ambițios. Și de ce Coreea e dispusă să realizeze linii de producție la noi." https://www.defenseromania.ro/cand-am-putea-avea-obuziere-k9-made-in-romania-parte-dintr-un-plan-mult-mai-ambitios-si-de-ce-coreea-e-dispusa-sa-realizeze-linii-de-productie-la-noi_630696.html.

European Security & Defence. 2022. "Hanwha Defense & UK Team Thunder – The Future of Mobile Fires." https://euro-sd.com/2022/09/sponsored-content/27272/hanwha-defense-uk-team-thunder-the-future-of-mobile-fires/.

Global Defense News. 2024. "K9 Thunder." https://armyrecognition.com/military-products/army/artillery-vehicles-and-weapons/self-propelled-howitzers/k9-thunder-south-korea-uk#google_vignette.

Grădinaru, Anca. 2024. „Ministrul Economiei, întrebat de ce fabricile românești nu produc muniție NATO de calibru 155: Să ne dea Armata specificațiile, mai întâi!" *Europa Liberă.* https://romania.europalibera.org/a/ministru-economiei-intrebat-de-ce-fabricile-sale-nu-produc-munitie-de-calibru-nato-155-pentru-armata-sa-ne-spuna-intai-ce-echipamente-are/32860331.html.

Ministerul Apărării Naționale. 2025. „Programe de înzestrare." *Direcția generală pentru armamente.* https://www.dpa.ro/programe-de-inzestrare/.

MD Harris Institute. 2013. "DOTMLPF-P Analysis for War and Peace." https://mdharrismd.com/2013/11/09/dotmlpf-p-analysis-and-military-medicine/.

Military-history Fandom. 2025. "152 mm towed gun-howitzer M1955 (D-20)." https://military-history.fandom.com/wiki/152_mm_towed_gun-howitzer_M1955_(D-20)?utm_source=chatgpt.com.

Mirea, Adrian, and Cristian-Octavian Stanciu. 2024. "Implementarea unei doctrine a sprijinului prin foc de nivel întrunit – cerință a operației întrunite." *Colocviu Strategic Nr. 1* 1-6.

NATO. 2018. "NATO's Joint Air Power Strategy." https://www.nato.int/cps/en/natohq/official_texts_156374.htm?selectedLocale=en.

___. 2021. "NATO CD-E Handbook, A concept developer`s toolbox." Norfolk: Allied Command Transformation. https://www.act.nato.int/wp-content/uploads/2023/05/NATO-ACT-CDE-Handbook_A_Concept_Developers_Toolbox.pdf.

___. 2023. "Interoperability: connecting forces." https://www.nato.int/cps/en/natohq/topics_84112.htm.

Nistorescu, Claudiu Valer. 2024. „Adaptarea organizației militare - o condiție esențială pentru obținerea succesului pe câmpul de luptă -." *Gândirea Militară Românească*, Iulie 1: 194-209.

Orjanu, Gheorghiță. 2023. „HIMARS deschide uși. Artileria Armatei României a intrat în „clubul select" ASCA. SUA – rol cheie în primirea României în ASCA." *Defense Romania.* https://www.defenseromania.ro/himars-deschide-usi-artileria-armatei-romaniei-a-intrat-in-clubul-select-asca-sua-rol-cheie-in-primirea-romaniei-in-asca_622036.html.

Statul Major al Apărării. 2021. „Start DACIA 21 LIVEX." https://www.defense.ro/start-dacia-21-livex.

Stroea, Adrian, and Gheorghe Băjenaru. 2010. *Artileria română în date și imagini.* București: Centrul Tehnic-Editorial al Armatei.

Vlad, Farcas. 2024. „Artileria autopropulsată pe roți – o variantă mai potrivită pentru războiul modern?" *Karadeniz-press.* https://karadeniz-press.ro/artileria-autopropulsata-pe-roti-o-varianta-mai-potrivita-pentru-razboiul-modern/.

Willi, Bernie. 2016. "Assessing Nations for NATO Partnerships." *Transforming Joint Air Power The journal of the JAPCC* 51-54.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Lessons learned on cybersecurity project proposals for successful EU grant applications

Christine DEMETER, Ph.D.*
Dănuț MAFTEI, Ph.D.**

*National Cyber Security Directorate, Bucharest
e-mail: demeter.chris@gmail.com
**National Cyber Security Directorate, Bucharest
e-mail: dn.maftei@gmail.com

Abstract

This paper analyses the key aspects of successfully preparing cybersecurity project proposals to secure EU funding. It is structured around three major topics: (1) Global cybersecurity challenges, highlighting advanced cyber threats; (2) EU policies and funding mechanisms, analysing key regulations such as NIS2 Directive, the Cyber Resilience Act, and funding programs like Horizon Europe, Digital Europe, and CEF Digital, which support research, innovation, and digital security infrastructure; (3) Best practices for developing successful EU-funded projects, focusing on aligning proposals with EU priorities, building strong consortia, demonstrating impact, and avoiding common mistakes.

By integrating strategic alignment, policy frameworks, and effective project planning, this study provides actionable recommendations for governments, organizations, and cybersecurity professionals aiming to enhance digital resilience through EU-funded initiatives. The findings contribute to a better understanding of the complexities related to securing EU grants and developing sustainable cybersecurity solutions across Europe.

Keywords:

project proposal; strategies, regulations, policies, and legal framework on cyber issues; resilience; challenges; cyber security; risks; innovation; financing.

Article info
Received: 14 February 2025; Revised: 26 February 2025; Accepted: 12 March 2025; Available online: 2 April 2025

Citation: Demeter, C. și D. Maftei. 2025. "Lessons learned on cybersecurity project proposals for successful EU grant applications". *Bulletin of "Carol I" National Defence University*, 14(1): 136-153. https://doi.org/10.53477/2284-9378-25-09

As digital technologies become more and more deeply integrated into every segment of our society, cyber security is an increasingly critical concern worldwide, playing a central role in the smooth functioning of modern society.
In recent years, the European Union's (EU) increasing dependence on digital technologies has led to growing concerns about cyber security risks. Given the cyber challenges facing states, organizations, and citizens today, cyber security is no longer a matter of choice but a fundamental necessity to ensure the protection and resilience of EU societies and economies.

As a component of national security, the importance of cybersecurity cannot be underestimated (Romanian Government 2021). With the rapidly evolving digital landscape, a large number of states have become increasingly exposed to a wide range of cyber challenges targeting critical information infrastructures, disrupting key services and sectors such as finance, healthcare, transportation, energy, communication networks, and supply chains, all of which pose significant risks to national and international security, but also to economic, political, social stability, democracy and society at large. Such malicious activities can be used by state or non-state threat actors to conduct or support hybrid campaigns or activities specific to Foreign Intelligence Manipulation and Interference (FIMI).

Cyber resilience has become a cornerstone of the *EU Cyber Security Strategy for the Digital Decade* (European Commission 2020b). These are the EU's overarching cybersecurity objectives for critical information infrastructure and a secure digital future, with the European Union focusing on building a robust framework that can withstand and recover quickly from cyber incidents. Cyber resilience goes beyond simply preventing cyber attacks, as it involves preparing for potential disruptions, minimizing their impact, and restoring normal operations as quickly as possible.

Cyber issues and digital resilience are also key topics for the *EU's Union Security Strategy* (European Commission 2020a). The EU has prioritized the protection of its digital infrastructure (a critical area where cybersecurity plays a vital role), including energy networks, communications, supply chains, and financial systems, which are increasingly dependent on interconnected technologies.

Cyber security is essential for maintaining public trust in digital services and preventing unauthorized access to sensitive information. Privacy is another significant concern in the EU's cybersecurity framework. The European Union is a world leader in privacy protection, with a specific legal framework – the General Data Protection Regulation (GDPR) of 2016 (EUR-Lex 2016), which sets high standards for data security. The GDPR imposes strict rules for handling personal data, requiring organizations to implement robust cybersecurity measures to protect citizens' privacy. Breaching this law can lead to heavy fines and reputational damage. As more and more personal data is generated and stored digitally, ensuring the security of this data has become more important than ever.

It can be seen that the EU has put in place several strategies, regulations, policies, and legal frameworks to strengthen its cyber security. These focus on setting objectives to protect critical information infrastructures, create a secure digital space, strengthen cooperation between Member States, adopt stringent cybersecurity management standards in key sectors, or establish a framework for European cybersecurity certification schemes for ICT products, processes, and services. These efforts reflect the EU's commitment to building a united and secure digital ecosystem and further demonstrate the EU's proactive approach to cyber security.

In order to lay the foundations for a secure and prosperous digital future, in addition to existing cyber strategies, regulations, policies, and legal frameworks, submitting project proposals for EU grants can benefit **research, innovation, digital infrastructure development, capacity building in the cyber security sector, security of networks and information systems, international cooperation, exchange of information and experience, etc**.

Thus, the European Union has established several funding programs that align with its cybersecurity strategies, policies, and regulations to ensure a coordinated and strategic approach to cyber resilience, thus reinforcing the objectives outlined in the *EU Cybersecurity Strategy for the Digital Decade* and the *EU Strategy on the Security of the Union*.

Key funding instruments include the **Horizon Europe Programme** (European Commission 2021c), which prioritizes cybersecurity research and innovation, supporting projects that develop cutting-edge security technologies, and encouraging collaboration between academia, industry, and government agencies. Another important program, the **Digital Europe Programme** (European Commission 2021d), focuses on building digital capabilities, including cybersecurity resilience, through large-scale deployment projects and promoting digital skills training. In addition, the **Connecting Europe Facility - CEF Digital** (European Commission 2021a) is a key EU funding instrument to promote competitiveness, growth, and jobs through targeted infrastructure investments across the Union. It aims to stimulate public and private investment in digital connectivity infrastructures of common interest to the EU. In addition, the **EU Funding & Tenders Portal** (European Commission 2021b) is a key tool providing centralized and up-to-date information on available grants, eligibility requirements, and application procedures.

Developing and submitting a proposal for a cyber security grant project is a complex exercise that requires the strategic integration of European, national, and organizational priorities. Such alignment not only demonstrates the relevance of the project but also ensures that it responds to the real needs identified at all levels.
The current work will analyze the importance of cybersecurity proposals for ensuring the protection and resilience of EU societies and economies, as well as the key aspects of successfully developing cybersecurity project proposals for EU funding.

This research is relevant for national governments, the cybersecurity industry, academia, civil society, the legislature, as well as the EU institutions, as it identifies the specific challenges, lessons learned, best practices, success factors, and complexities involved in the successful development of EU cybersecurity project proposals.

The methodology used and research hypotheses

The study adopts an **analytical and exploratory** methodology, based on the following components: (1) **Desk review**: examining relevant EU directives and regulations, such as the NIS2 Directive, the Cyber Resilience Act, Horizon Europe, Digital Europe, and CEF Digital, which set the cybersecurity framework and requirements for obtaining EU funding; (2) **Benchmarking**: comparing EU strategies and policies with the requirements and challenges of funding applicants, to identify discrepancies and key success factors; (3) **Best practice review**: Identifying factors that have contributed to the success of previous project proposals in the field of cybersecurity and extracting lessons learned to optimize the application process; (4) **Actionable recommendations**: formulating concrete suggestions for effectively aligning projects with EU requirements, thus maximizing the chances of obtaining funding and successfully implementing cybersecurity projects.

The presented methodology provides a **practical and grounded insight** into the complexities of the funding application process, supporting stakeholders in improving their chances of success and contributing to the development of a robust framework for cybersecurity projects in Europe.

This article explores how cybersecurity projects can be optimized to obtain funding and contribute to the EU's digital resilience. The research aims to highlight the critical factors influencing the success of these initiatives, with a focus on compliance with European strategies and regulations, as well as the effectiveness of consortia and implementation mechanisms.

The study is based on the following research hypotheses:

1. Alignment with EU, national and organizational strategies, compliance with the legal framework, and prioritization of EU funding issues are key factors of the success of cybersecurity projects in obtaining funding and their contribution to strengthening digital resilience and critical information infrastructure protection;

2. A strategic and well-informed approach to cyber issues and project development ensures long-term sustainability and relevance;

3. Building strong consortia and demonstrating the impact of projects are key factors for the successful acceptance and implementation of cybersecurity project proposals.

Challenges related to cyber security, hybrid warfare, and FIMI around the world

According to the present research, the major challenges existing in the cyber security domain across the globe are currently related to:

- **The expanding range of IT devices, and the increasing sophistication of cyber attacks** (Spencer 2024), including state-sponsored, ransomware, phishing, advanced persistent threats, data breaches, terrorism, and cyber espionage attacks. They are harder to detect, harder to counter, increasing in frequency and sophistication. Such malicious activities can also be used by state or non-state threat actors to conduct or facilitate hybrid campaigns (European Union 2023) and specific FIMI activities.
- **FIMI**: One of its most damaging effects is the erosion of public trust in democracy and democratic institutions. At the same time, misinformation, fake news, and hate speech, including against ethnic, religious, and sexual minorities, widen social divisions in democratic states, lead to increased discrimination and violence, and fuel political and cultural polarization. Trust in institutions and traditional media is also being eroded, leading to increased scepticism and difficulties in distinguishing between real and false information (Maftei and Bogdan-Duica 2024).
- Malicious actors (especially non-state actors) **conduct hybrid warfare-specific operations**, including by exploiting vulnerabilities of social media platforms or using cyber-attacks, thus affecting children, girls, women, citizens, societies, economies, critical services, democracy, and national security (Maftei and Bogdan-Duica 2024). Researchers have observed the steady evolution of Russian information warfare doctrine, which has deep roots in Soviet practice (Giles 2016; Snegovaya 2015). Recent Russian military thinking emphasizes hybrid warfare as a new persistent reality, with the ”information sphere” and ”information warfare” as a critical battlespace.
- **Cybersecurity governance and coordination, appropriate strategies, policies, and legal frameworks on cyber issues are lacking or underdeveloped**. Several countries are faced with fragmented cybersecurity systems, where national efforts are not coordinated, and policies can differ widely. This can lead to ineffective responses against national and cross-border cyber threats, which requires better international cooperation and standardized approaches to cybersecurity.
- **Lack of implementation of national strategies, policies, and legal framework on cyber issues**. Although existing strategies, policies, and legal frameworks are well drafted, in some countries they are not properly implemented. The reasons could range from political interests to financial or human resources issues.
- **A low level of cybersecurity and cyberspace hygiene**.
- **Low level of cybersecurity education and culture and lack of adequate training** of network and information systems operators (Maftei 2024). Lack of

digital literacy and education on cyber issues leads to human errors that make IT systems and networks vulnerable (European Commission 2023).

- **Lack of qualified cybersecurity professionals**. The demand for qualified cyber experts outstrips the supply, making it difficult for organizations to effectively defend against attacks. This shortage of experts hinders the coagulation of a sufficiently qualified cyber security workforce (Maftei 2024). However, the EU is working hard to raise public and business awareness of cybersecurity risks and best practices. Educational programs and certifications are also being developed to close the cybersecurity skills gap in both EU institutions and private organizations.

- **Retention of human resources**. Governments, critical and important entities, or operators of critical information infrastructures face difficulties in retaining cybersecurity experts, who often leave the organization for better salaries. However, several states have identified ways to address such challenges. For example, in Romania, the National Cyber Security Directorate - DNSC - a specialized body of the central public administration, under the authority of the Government, responsible for ensuring the cyber security of national civilian cyberspace (DNSC 2022), has managed to multiply four (4) times the favourable conditions necessary for retaining cyber professionals within the organization: 1) by hiring the experts as contracted staff; 2) due to this type of contract, by allowing part-time work for other organizations (of course, the conflict of interest must be absent); 3) also, by allowing part-time work in externally funded cyber security projects; 4) by amending the legal framework necessary to increase the salaries of staff employed as cyber security experts.

- **Cyber resilience is often weak**, with some countries lacking the necessary cyber resilience capabilities. Cyber resilience refers to the ability to anticipate, respond and recover from cyber attacks. The ability to quickly restore operations after a cyber incident is critical to mitigating long-term damage and many states around the world have underdeveloped recovery plans or vulnerable cybersecurity infrastructures (CISCO 2025).

- **Privacy concerns** are a challenge as more and more personal and sensitive data is stored and shared digitally. Balancing the need for security with protecting citizens' privacy remains a delicate task, especially as laws and regulations such as the GDPR put pressure on organizations to comply with strict privacy standards.

- **National, regional, and international cooperation is not sufficiently developed**. Old mindsets and silo thinking (Gleeson 2013) still exist within some organizations. This has a particularly high negative impact on increasing trust between partners, the level of cooperation, information sharing and countering cyber incidents or other security challenges.

- **Public/private partnerships should be developed**. Only a few countries in the world could be presented as examples of this type of partnership. For example, in Romania, one of the five main objectives of the Cyber Security

Strategy for the period 2022-2027 is the *Pragmatic Public Private Partnership*. "A pragmatic public-private partnership between public authorities, private entities, academia, research and citizens is a necessity, given that cyber-attacks target a large number and broad spectrum of networks and information systems" (Romanian Government 2022). This demonstrates the government's focus on public/private partnerships.

- **Cyber incidents are underreported** by citizens, private businesses, critical information infrastructure operators, supply chain members or even state institutions, and the reasons can be different: lack of awareness or understanding; lack of clear regulations for incident reporting; fear of reputational damage; legal and financial consequences; fear of escalation of attacker threats; disruption of operations; government and regulatory pressure; internal divergences; cost and resource constraints, etc. (Maftei 2025). Improved cyber incident reporting enables governments to take informed, initiative-taking actions that protect national security, support economic stability, strengthen economic resilience, and contribute to the development of policies and regulations needed to improve cybersecurity in general.
- **Emerging trends in cybersecurity**. Today, there is an increasing use of artificial intelligence and machine learning both by cyber professionals seeking to identify and mitigate cyber threats faster and more effectively, and by malicious actors using increasingly complex techniques to carry out attacks. Such emerging technologies, including quantum computing, could rapidly change the cybersecurity landscape, and the EU must be ready for such advances (Apriorit 2025).

***

The aforementioned challenges highlight the need to adopt and implement comprehensive cybersecurity strategies, policies, legal frameworks, education, cooperation, and investments in both technology and human resources to address the growing cyber challenges. Given these challenges, cyber security is no longer an option but a fundamental necessity to ensure the protection and resilience of EU societies and economies.

Essential components of a cybersecurity project proposal for successful EU grants

Developing and submitting a proposal for a cyber security grant project is a complex exercise that requires the strategic integration of European, national, and organizational priorities. Such alignment not only demonstrates the relevance of the project, but also ensures that it responds to the real needs identified at all levels.

How can European, national, and organizational strategies be aligned?
One of the most important challenges is to demonstrate the alignment of the project proposal with the priorities set at European, national, and organizational levels. This requires a well-defined process based on thorough analysis, integration, and justification. Understanding the strategic context, making direct links between the project objectives and the proposed solutions, and justifying the intended impact are essential steps. These are only the first steps.

EU legal framework on cyber issues to consider...
The European Union has put in place several strategies, regulations, policies, and a legal framework to strengthen its cybersecurity. Thus, according to key documents such as the *EU Cybersecurity Strategy for the Digital Decade*, the EU considers cybersecurity as a major strategic priority. This document demonstrates the EU's proactive approach to cybersecurity and sets clear objectives for protecting critical information infrastructures, creating a secure digital space, and strengthening cooperation between Member States. These objectives are essential for any project that aims to contribute to strengthening the EU cyber security framework.

Another key document is the *NIS2 Directive (Network and Information Systems Directive*) (EUR-Lex 2022a), which sets stringent standards for cybersecurity management in key sectors such as health, transport and energy. Compliance with the requirements of the Directive is essential to demonstrate that the project aligns with European priorities. The NIS2 Directive is linked to the *Critical Entity Resilience Directive* (EUR-Lex 2022b).

Regulation 881/2019, known as *the EU Cybersecurity Act* (EUR-Lex 2019), strengthens the role of the European Union Agency for Cyber Security (ENISA 2025) and establishes a Cybersecurity Certification Framework for ICT products, services and processes. The Regulation also aims to ensure the smooth functioning of the internal market and to achieve a high level of cybersecurity, resilience, and trust within the EU. On the other hand, ENISA produces a large number of reports on EU projects and comprehensive analyses of the EU cybersecurity landscape.

The Regulation on Cyber Resilience - Regulation (EU) 2024/2847[1] (EUR-Lex 2024) provides EU-wide minimum cybersecurity standards for digital products and software connected to the internet, setting a high level of technological excellence. This regulation will improve the overall security of society, with increasingly secure electronic devices available on the market as designs with ICT components must clearly demonstrate how they meet or exceed the set standards.

[1] The Regulation is also known as the *Cyber Resilience Act*.

https://doi.org/10.53477/2284-9378-25-09

There are, of course, other sectoral directives and regulations that form part of the legal framework on cyber issues. All these, together with the new European Cyber Security Competence Center (ECCC 2025), the EU's innovation hub for advancing cybersecurity technologies, reflect the commitment of the EU and its Member States to build a united and secure digital ecosystem.

Alignment with national strategies...

At the national level, each EU Member State has its own cybersecurity strategy, adapting European priorities into measures specific to the national context. These strategies often emphasize CERT[2] capacity building and securing critical information infrastructures. At the same time, national recovery and resilience plans include strategic investments in digital transformation, creating opportunities for projects focused on building digital resilience.

A well-founded project should clearly demonstrate how it addresses the priorities outlined in these national strategies. For example, a project focused on securing the digital infrastructure of hospitals should align with national digital health strategies and specific measures specified in the implementing legislation of the NIS2 Directive and also with additional sector-specific measures.

[2] Computer Emergency Response Team.

Integrating organizational strategy...

In addition to being aligned with European and national priorities, the project proposal should also reflect the mission, vision and strategy of the organization developing it. This integration demonstrates that the project is not just a response to a funding application, but is part of a broader, well-articulated plan that reflects the values and strategic direction of the organization.

For example, if an organization's mission is *to increase the digital resilience of the public sector*, the proposal should outline how the proposed solutions contribute to this mission. Similarly, the organization's long-term vision, such as *becoming a regional leader in cybersecurity solutions*, should be supported by the project's ambitious goals.

A project aligned with the organization's strategy is more likely to benefit from its resources and expertise. For example, if the organization's strategy includes securing critical information infrastructures, the proposal should highlight its continuity with previous initiatives and demonstrate how it adds value. Such alignment can be argued through concrete examples of the organization's experience, such as the successful implementation of similar projects. This demonstrates a deep understanding of the domain and the ability to deliver tangible results.

... And the objectives of open calls – "call-fiche"

Another key aspect of developing a proposal is to explicitly align it with the objectives of the open calls for proposals. These calls set out specific priorities,

expected results and eligibility criteria that the proposal must address.
For example, if a funding request focuses on *increasing the digital resilience of critical information infrastructures*, the proposal must articulate how the proposed solution directly addresses this objective. This may include presenting a detailed technical solution that addresses the problems outlined in the request, demonstrating its alignment with strategic priorities such as interoperability, innovation, or sustainability, and defining clear performance indicators such as, for example, reducing response time to cyber incidents or improving data protection.
Open calls may also specify additional requirements, such as *cross-border collaboration or private-sector involvement*. The proposal should address these requirements explicitly, detailing how the project contributes to the objectives pursued.

Justifying the impact and establishing a solid implementation plan...
A well-structured proposal includes a clear section justifying the impact of the project, supported by measurable objectives and performance indicators. For example, a monitoring system that reduces the response time to cyber-attacks from 24 hours to 2 hours should be explicitly presented in the proposal. Such results can be backed up with relevant statistics and reports, such as those from ENISA.
The proposal should also contain a detailed implementation plan, including the resources available, the team involved and the project milestones. These elements create an overall picture that gives confidence to the evaluators.

Who said it was easy?
Developing a proposal for a cybersecurity project is an achievable process when it is approached systematically, following steps of thorough documentation, strategic alignment, and detailed justification. By integrating EU, national and organizational strategies, as well as the objectives of open calls for funding, the proposal proves its relevance, feasibility, and value. In this way, the proposed project becomes more than just an idea; it emerges as a solid solution that contributes to increasing cybersecurity resilience at all levels.

Challenges, lessons learned, good practices, and success factors for successful application to EU-funded cybersecurity programs

Applying for EU-funded cybersecurity programs can be a complex but rewarding process. Such activity presents several challenges, which can be both complex and time-consuming. Based on experiences from previous applications, some key challenges, lessons learned, and good practices related to funded programs dealing with cybersecurity have been revealed, such as:

Understanding program objectives, priorities, and requirements. Not all EU programs are similar. Each program has its own specific goals, objectives, and

priorities. Many applicants fail to align their project proposals with the main objectives of the program, leading to rejection. Please carefully read the call for proposals, work programs and any related documentation. The project must align perfectly with the objectives presented. Priority needs to be given to addressing EU-wide challenges such as critical infrastructure protection, cross-border cyber threats, or resilience to cyber attacks. It is particularly important that the technical, legal, and financial aspects required in proposals for EU-funded projects should be well understood and respected.

Focus on innovation and impact. EU funding tends to favour innovative, scalable, and impactful cybersecurity projects. Proposals with vague objectives or low impact often fail to stand out, with limited chances of winning. The project must provide a clear innovative solution to urgent cyber security challenges. Measurable results such as strengthening cyber security capabilities, improving threat detection, or developing cross-border collaboration need to be demonstrated.

Strict compliance with EU policies and the legal framework to be followed (regulations, financial management directives, eligibility criteria, funding limits, evaluation criteria, reporting, data protection, state aid law, sustainability objectives and any other sector specific legal requirements). Applicants must ensure compliance with these rules and failure to do so may lead to disqualification of the project or rejection of funding. This can be particularly difficult for organizations that are unfamiliar with specific EU rules or that operate in multiple jurisdictions.
Applicants should invest time and effort to understand the policies and legal framework relevant to the projects. In parallel, it is essential to involve legal or financial experts who are familiar with EU compliance and funding requirements.

Highly competitive environment. Many EU funding programs, particularly in the area of cybersecurity, are highly competitive because of the fairly large number of applicants and the low proportion of proposals that could receive funding. A strong record in cybersecurity or EU-funded projects, development of a highly innovative and impactful project that directly addresses EU cybersecurity priorities, strong partnerships and clear alignment with EU objectives can significantly increase the chances of success.

Complex application processes and procedures. The application process for EU-funded programs is often complex and requires extensive documentation. It involves several steps (proposal writing, budgeting, partner agreements, compliance checks, etc.). The complexity of the application may be a barrier for smaller organizations or those with limited experience in EU funding. Incomplete or inaccurate proposals may result in disqualification. This is why applicants should devote sufficient time and resources to understand the requirements of the application and to ensure that all conditions are correctly fulfilled. Career guidance or consultants can also be helpful.

Difficulty in creating the right consortium. Collaboration is often key to the success of proposals. Many EU-funded cybersecurity programs require the involvement of multiple partners, including government bodies, research entities, academia, private companies, and NGOs. Weak or insufficient partnerships can lead to the failure of a funding application. Identifying suitable, reliable partners to commit to the project can be a challenge and an incomplete or weak consortium can undermine the quality and chances of the proposal, making it difficult to meet the program requirements. In addition, inter-partner dynamics, different organizational cultures and unclear roles can affect project implementation. Experts with complementary skills should be recruited and all partners must be fully engaged and contribute equally to the project. Establishing a strong consortium requires careful planning, and clear and transparent communication from the outset about roles and responsibilities is essential. On the other hand, applicants should partner with trusted organizations that bring complementary skills and resources. It is clear that the EU's international initiatives in the field of cybersecurity should be further explored, including cooperation with NATO, the UN, and non-EU states in addressing global cyber threats.

Budgeting and financial planning. Poorly prepared financial plans, unrealistic budgets or administrative errors are often found in submitted proposals. Insufficient clarity or transparency can also lead to doubts about project feasibility. Projects have to adhere to specific rules on eligible costs, co-financing and reporting requirements, and there is often a detailed breakdown of how the funds will be allocated. A lack of clarity or inaccurate financial planning may lead to the rejection of the proposal. In addition, financial complexity may discourage small businesses or research institutions without in-house financial expertise. Applicants should carefully follow the program's financial guidelines. A detailed and realistic budget and transparency in the allocation of funds are essential. Consultation with financial experts can ensure compliance with EU rules. Applicants must be clear about how the funds will be allocated and ensure compliance with EU financial rules. It is also necessary that the programme guidelines are followed and that the administrative documents are complete and accurate.

Risk of blocking activities and limited reporting. After receiving funding, beneficiaries must report regularly on progress, results, and financial management. This can be time-consuming and failure to comply with reporting requirements can lead to sanctions or loss of funds. Applicants may underestimate the effort required for post-grant activities (e.g. progress monitoring and reporting), which may result in delays, mismanagement or even project failure.
In order to avoid such problems and to ensure good project management, applicants should prepare a robust monitoring and evaluation framework to track project milestones, outputs and expenditure incurred, as well as allocate the necessary resources for regular reporting and internal audits.

Risk management. Cybersecurity projects face numerous risks, including delays, technical challenges, and potential collaborative failures. Underestimating risks or providing weak mitigation strategies can lead to poor evaluation scores. A comprehensive risk management plan outlining potential risks (technical, financial, operational) and mitigation strategies should be developed. Being proactive in addressing risks increases confidence in project execution.

Holding discussions with EU officials and other entities involved. Many applicants fail to make timely contact with EU officials or other involved entities with an important role in cybersecurity. This may limit the understanding of the program priorities, leading to poorly aligned proposals. Active participation in information days, networking events and webinars organized by the EU or funding bodies could be a huge asset. In the meantime, engagement with relevant stakeholders and officials early in the process to clarify any questions and refine the project, as well as getting feedback from EU bodies, is important.

Sustainability. To be successful, projects need to consider long-term sustainability, as EU funds are interested in supporting projects that have a lasting impact beyond the funding period. Applicants need to clearly articulate how the project will be sustained beyond the end of funding, conditions which would require establishing self-financing models, partnerships with industry actors or ensuring that the results will be adopted by end-users, including government bodies, businesses, and the public sector.

Communication and reporting. To avoid creating confusion and undermining confidence in the project, a transparent, clear, and concise communication plan should be developed, including measurable results, timelines, and regular reporting. All stakeholders should be kept regularly informed of project developments.

Long and uncertain deadlines. Applications for EU funding usually involve long preparation times and a delayed funding approval process. The assessment, selection and funding agreement phases can take months or even longer. Prolonged timelines can create uncertainty for organizations, especially if they need immediate funding to start cybersecurity projects. Delays in receiving funding can also affect the project implementation timetable. Applicants should plan ahead and be prepared for possible delays. It is useful to have alternative funding sources or backup measures in place to fill gaps during waiting periods.

Managing cross-border collaboration. Many EU cybersecurity programs involve international collaboration, which means different partners in different EU Member States need to work together. Cultural differences, different regulatory environments and different legal systems can complicate the coordination process. Managing a multinational project requires effective communication, understanding of different laws and a harmonized approach to project objectives. These challenges can lead to misunderstandings, delays, or inefficiencies.

Clear governance structures, well-defined roles and regular communication are essential for successful international collaborations. It is important that all partners understand the project objectives and are committed to the common vision.

Limited knowledge of cybersecurity needs. Applicants may have difficulties in fully understanding or addressing the specific cybersecurity challenges highlighted by the EU. As the cybersecurity landscape is constantly evolving, it is essential to be well versed in new types of threats, trends and emerging technologies through briefings and consultation of EU publications, research papers, as well as participation in relevant EU events addressing cybersecurity issues. The project proposal should also be aligned with the latest EU cyber security strategies.
Proposals that do not adequately address current or future threats to cybersecurity are unlikely to be accepted. In addition, misalignment of the project with EU priorities or failure to demonstrate the relevance of the project to the European cybersecurity agenda may affect the application.

Lack of post-project sustainability. EU funding often requires projects to demonstrate how the results will be sustained and scaled up after the end of the funding period. Many applicants strive to provide a clear roadmap for the long-term sustainability of their projects, as those who fail to demonstrate clear sustainability after the EU funding period risk being rejected. Funders want to ensure that projects create a lasting impact and do not rely solely on continued EU funding. A sustainability plan should be developed outlining how the project will continue to operate, whether through commercialization, government support, industry partnerships or other means.

Intellectual property and data sharing. In EU-funded collaborative projects, intellectual property and data-sharing issues can be controversial. Some rights disputes may also arise, especially when partners have different national or institutional policies. To avoid friction between partners, delayed projects, legal problems or funding sanctions, attention should be paid to the mismanagement of intellectual property and non-compliance with data protection legislation. Intellectual property, data-sharing agreements and confidentiality clauses should be defined in advance. All partners need to be aligned on these issues and comply with EU data protection and intellectual property legislation.
Preparing applications in advance. As the proposal development process often requires significant time and effort, work should start early, allowing time for drafting, review, refinement, and revisions.

***

By applying these best practices and learning from previous experiences, organizations can increase their chances of success when applying for EU-funded cybersecurity programmes.

Conclusion

Looking ahead, it can be concluded that the continued evolution of cyber threats and the increasing dependence on digital technologies require sustained investment, innovation, research, and development of digital infrastructure while increasing the level of security of networks and information systems, capacity building in the cyber security sector, exchange of information and experience, and better collaboration in the field of cyber security. Strengthening international cooperation, fostering public-private partnerships and improving cyber security education will also be essential to ensure a secure digital future in the EU and the world, to ensure the protection of privacy, the resilience of EU societies and economies, stability, national and international security, the security of critical information infrastructure assets, as well as democracy and the functioning of democratic institutions.
This paper has analysed the importance of cyber security project proposals for ensuring the protection and resilience of EU societies and economies.

The scientific research, based on an analytical and exploratory methodology, validates the research hypotheses and confirms that the success of cybersecurity project proposals is conditioned by their alignment with EU strategies, compliance with the legal framework and effective integration of European funding requirements. The literature review of relevant directives and regulations, such as the NIS2 Directive, the Cyber Resilience Act and the Horizon Europe, Digital Europe and CEF Digital funding programs, highlights the importance of projects' compliance with the objectives set by the European Union for cybersecurity and digital resilience.

Comparing EU strategies and policies with the needs and challenges of applicants reveals that differences between European requirements and the ability of organizations to meet them can influence the chances of success of proposals. Thus, strategic and documented alignment of projects not only demonstrates their relevance but also ensures better integration into the European digital security ecosystem. The research also confirms that a systematic approach to project development, including a clear justification of their impact and long-term sustainability, is essential for the success of applicants.

Analysis of good practice from previous successful proposals shows that a key determinant is the formation of strong, interdisciplinary, and international consortia, where partnerships between government institutions, private companies and academic entities contribute to increasing innovation capacity and demonstrating project impact. In this context, impact assessment and the definition of measurable objectives are critical to validate the relevance of proposals.

Research also underlines the importance of effective risk management and compliance with EU requirements. The implementation of a detailed risk management plan, including clear mitigation strategies and robust monitoring

mechanisms, contributes to optimizing the implementation process and avoiding administrative obstacles. Therefore, projects that demonstrate rigorous planning, clear integration into EU strategies and a sustainable approach are the most likely to get funding and contribute to strengthening the EU's digital resilience.
By recognizing and proactively addressing the challenges identified, while applying the good practices presented and learning from past experiences, applicants/ stakeholders can increase their chances of success in securing EU funding when applying for cyber security programmes.

Identifying the strategies and key components of successful proposals, examining best practices, relevant case studies and lessons learned from previous EU cybersecurity proposals could be vital factors for writing effective applications.

The current scientific research contributes to a better understanding of the specific complexities of obtaining EU grants and developing sustainable cybersecurity solutions in the EU and EU Member States and could have a direct impact on EU policies on cybersecurity project proposals or the effectiveness of specific funding programs.
The study is of importance for national governments, the cyber security industry, academia, civil society, legislators, and the EU institutions as it identifies the specific challenges, lessons learned, best practices, success factors and difficulties in preparing successful cyber security project proposals within the European Union.

At the same time, this work may be of relevance to cybersecurity professionals, organizations, and policymakers in the EU. The material also provides concrete recommendations for organizations wishing to submit successful cybersecurity project proposals in the EU context.

References

Apriorit. 2025. "CyberSecurity Trends in Information Technology and Emerging Future Threats." doi:10.6084/m9.figshare.16937014.

CISCO. 2025. "What Is Cyber Resilience?" https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html.

DNSC. 2022. „Lege nr. 366 din 19 decembrie 2022." https://legislatie.just.ro/Public/DetaliiDocumentAfis/262941.

ECCC. 2025. "European Cybersecurity Competence Network and Centre." https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre.

EEAS. 2024. "Tackling Disinformation, Foreign Information Manipulation & Interference." https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

ENISA. 2025. "ENISA." https://www.enisa.europa.eu/.

EUR-Lex. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data." https://eur-lex.europa.eu/eli/reg/2016/679/oj.

—. 2019. "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA." https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

—. 2022a. "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

—. 2022b. "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC." https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

—. 2024. "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements." https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

European Commission. 2020a. "COM(2020) 605 final." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020DC0605.

—. 2020b. "The Cybersecurity Strategy." https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

—. 2021a. "Connecting Europe Facility." https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/connecting-europe-facility_en.

—. 2021b. "EU Funding & Tenders Portal." Editor European Commission. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home.

—. 2021c. "Horizon Europe." https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.

—. 2021d. "The Digital Europe Programme." https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

—. 2023. "Cyber Skills Academy." https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy.

European Union, General Secretariat of the Council. 2023. "Revised Implementing Guidelines of the Cyber Diplomacy Toolbox no. 10289/23." https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf.

Giles, Keir. 2016. "Handbook of Russian Information Warfare." https://www.ndc.nato.int/news/news.php?icode=995.

Gleeson, Brent. 2013. "The Silo Mentality: How To Break Down The Barriers." https://www.forbes.com/sites/brentgleeson/2013/10/02/the-silo-mentality-how-to-break-down-the-barriers/.

Maftei, Dănuț. 2024. "The Cyber Competences Act – a Vital EU Regulation Concerning Mandatory Certification of Critical Network and Information Systems' Operators across the European Union." *Informatica Economică* 45-60. doi:10.24818/issn14531305/28.2.2024.04.

—. 2025. "LinkedIn post." https://www.linkedin.com/posts/danut-maftei-phd-39418a68_cyberincidents-criticalinformationinfrastructure-activity-7291046307190759424-LL9w?utm_source=share&utm_medium=member_desktop.

Maftei, Dănuț și Lorin Nicolae Bogdan-Duica. 2024. "Risks, threats, and vulnerabilities related to social media platforms and search engines. Regulations and national legal frameworks." *Bulletin of "Carol I" National Defence University* ("Carol I" National Defence University Publishing House) 13 (4): 249–265. doi:https://doi.org/10.53477/2284-9378-24-62.

Romanian Government. 2021. „Ordonanță de urgență nr. 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică." https://legislatie.just.ro/Public/DetaliiDocumentAfis/246652.

—. 2022. „Strategia de Securitate Cibernetică a României, pentru perioada 2022-2027." https://securitatea-cibernetica.ro/documente/Strategia-de-securitate-cibernetica-a-Romaniei.pdf.

Snegovaya, Maria. 2015. "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare, Institute for the Study of War." https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

Spencer, Patrick. 2024. "2024 Cybersecurity and Compliance Landscape: 50 Critical Statistics Shaping Our Digital Future." https://www.kiteworks.com/cybersecurity-risk-management/2024-cybersecurity-landscape-50-critical-statistics/.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Human security in the context of unconventional security threats. A theoretical approach

Vasile PAȘCA, Master Student*

*Babeș-Bolyai University, Cluj-Napoca
e-mail: pascavasile279@gmail.com

Abstract

This article explores the concept of human security in the context of the emergence of a suite of unconventional threats that undermine traditional state-centered security paradigms. Drawing on document analysis, the article redefines security as individual-oriented, emphasising the interdependence between fundamental rights, human development, and global stability. It addresses the complex dimensions of human security – economic, food, health, environmental, ecological, personal, community and political – and the principles that underpin it, including the legitimacy of authorities, multilateralism and a focus on prevention and early intervention. This article highlights the shift from exclusively military to multidimensional security, in which the state shares responsibility with international organizations, NGOs and civil society. The importance of the theme lies in its ability to respond to global challenges such as climate change, migration and pandemics, reaffirming the imperative of transnational cooperation to protect the dignity and well-being of individuals.

Keywords:
security; human security; individual; threats; responsibility to protect (R2P); international community.

Article info
Received: 27 January 2025; Revised: 26 February 2025; Accepted: 4 March 2025; Available online: 2 April 2025

Citation: Pașca, V. 2025. "Human security in the context of unconventional security threats. A theoretical approachh". *Bulletin of "Carol I" National Defence University*, 14(1): 154-168. https://doi.org/10.53477/2284-9378-25-10

"Systems are only as strong as their weakest link, creating a zommon and mutual vulnerability between all actors" - Jorge Nef

In one of his seminal writings on the theory of international society, "The Anarchical Society", published in 1977, the renowned Australian professor Hedley Bull suggested that the world order is "*fundamental and primordial [...] because the ultimate elements of the great society of mankind are not states [....] but individuals*" and *"the question of a world order arises irrespective of the political or social structure of the globe*" because *"if international order really has value, it is only because it is useful for achieving order in human society as a whole*" (Griffiths 2003, 241), thus intuiting the broad process of fundamentally reconceptualizing the meaning of the concept of security and the elements to which security should be provided.

The redefinition of security has two main sources. First of all, we are talking about a new field of international relations, which gained ground during the 1980s, namely international political economy (IPE), whose literature attempted to provide logical explanations for the turbulence generated by the globalization process. Secondly, there was a growing involvement of the social sciences in the field of security studies, attempting to provide explanations for hitherto quite irrelevant issues such as identity, ethnicity, religion, poverty, terrorism, organized crime, environmental issues, etc. The predominantly military content of security studies during the Cold War period established a clear distinction between external and internal security, which were always analyzed as distinct areas of national security. The end of the Cold War, the new literature bringing to the fore the process of globalization, plus the new information technology, which has reduced the limitations imposed by space and time on the movement of capital, services, ideas, and labour, have given rise to a transnational process that is radically changing the environment and the traditional agenda of security studies. Thus, the military aspects have been relatively blurred by political, economic, societal, and environmental aspects, while the international dimension of crises has become regionalised. Moreover, security has ceased to be the exclusive prerogative of the state, although it remains its main task. In this sense, the culture of security has become increasingly assimilated by civil society, with the security agenda being written, in practice, in the public arena. Thus, during the 1990s, security had become a "*public emergency register of the most pressing political, military, economic, societal, environmental issues*" (Sava 2005, 13-14; 16).

In this "*register*" the questions, and especially the answers, were not those dealt with by security in its traditional version because it (A/N security) was seen as the main "*Westphalian prerogative of the nation*" contracted in sovereign states that, internally, had concluded "*a Hobbesian bargain with subjects, who would have ceded certain rights in exchange for the protection of Leviathan against war*", a vision that no longer fully reflected the tangible realities of the international

community. Moreover, what this "*bargain*" failed to foresee was the situation in which the state[1] is *unable* or *unwilling* to protect its citizens in the face of unconventional threats consisting of serious human rights violations practiced by the state itself, or underdevelopment, which the state does nothing to alleviate/remove, or any other unconventional threats where the state "*no longer claims that its use of force is legitimate*" (Tadjbakhsh 2005, 4). Against this backdrop of the conceptual inconsistencies of traditional security in the context of the occurrence of a series of unconventional threats to it (A/N security), which have revealed the weaknesses and limitations of traditionalist paradigms, objectified by the inability of the state to cope with these threats, have disrupted the stability of global security and have highlighted the need to rethink the concept of security.

[1] As the supreme, sovereign and legislative power in a given territory, depositary of the monopoly on legitimate violence.

The main *purpose* of the article is to theoretically assess the concept of human security, with the specific aim of understanding the mechanisms and valences that define human security, as well as to identify and explain the fundamental principles underlying it.

In order to achieve this aim, the article has the following *objectives*: (1) to define and conceptualize human security, with a focus on clarifying the different interpretations of the concept and identifying its constituent elements; (2) to define the key principles underlying human security; and (3) to identify the differences and particularities between traditional, state-centric and human security, as well as to identify the main approaches and debates on the latter. At the same time, in order to achieve the proposed goal, we aim to answer the following *research questions*: Whose security and by whom? Security from which threats?
From the *methodological* point of view, the present article is a mark of qualitative studies, the main method of documentation and substantiation of the research being based on document analysis.

From traditional security to human security

The discussion in this chapter starts from the rather controversial idea that security is a *fundamentally contested concept*. A proponent of critical security studies, W.B. Gallie[2] was the first to describe security as a "fundamentally contested concept" in a 1956 paper. What the author meant to express was that security, as a fundamentally contested concept, "*differs [...] so widely on a value scale that they could never agree on what it means*" (Robinson 2010, 46-47). Therefore, in the spirit instilled by the Scottish political scientist, sociologist and philosopher, W.B. Gallie, this chapter attempts to capture an important element, often omitted by researchers in the field, namely that "*the issue of security is, first and foremost, a matter of perception*" (Miroiu 2006, 182).

[2] Walter Bryce Gallie was a Scottish sociologist, political scientist and philosopher. His 1956 paper in which the "fundamentally contested concept" formula appears is entitled "Essentially Contested Concepts", Proceedings of the Aristotelian Society, vol. 56, 1956, pp.167-198.

In this sense, we can analyse the transition from traditionalism to human security by using two concepts that have come into use fairly recently, namely *negative security*, which is mainly valid for the traditionalist symbolism of security, and *positive security*, which is in favour of security as an intersubjective process. Thus, the symbolism of security understood through the prism of negative security aims at the fact that the most important and, in fact, the only actor of security is the state, which "*counteracts security threats by external means, namely organized violence, with recourse to armed force as its most eloquent expression*". In this key, state security becomes a security of survival (Dumitrescu 2020, 14-15).

The need to transition towards human security can be understood through the prism of positive security, a concept that suggests that security practices must generate trust and build capabilities, which is why the characteristic emotions of this type of security are safety and stability, with practices being mainly nonviolent. Positive security emphasizes the concept of *'everyday security'*, understood as the institutional capacity of the state to generate predictability for the ordinary citizen on a routine basis. Routinely conveyed, security is thought to become the hallmark of the "multiple actor", in the sense that security, as a process, is sustained not only by the state and its formal institutions, but also by the informal institutions of the state, namely family networks, kinship networks, professional networks and so on. Thus, like Arnold Wolfers, the positive security view argues that security, as an intersubjective process, "*represents a permanent negotiation between the state and the individual, especially with regard to the meanings attributed to security threats*" (Dumitrescu 2020, 14-15).

Against this backdrop, the emergence of human security was conditioned on the one hand by the need to redefine it (A/N security) as a "*subjective experience at the micro level*", and on the other hand, by the new post-Cold War realities, which problematized the relationship between nations and state, which had been considered until then an irreducible element of global politics.
The need to redefine security as a subjective experience at the micro level was simplistic, but well characterized by the Iranian-American researcher Shahrbanou Tadjbakhsh who stated that:

> "*'Security' for a farmer growing poppies in Badakhshan or Helmand was the livelihood he gained from selling his crops to a middleman, but this form of security was very different from the 'security' interests of recipient states concerned about their drug addicts and about the terror-crime-drug-mafia networks. For a school teacher in Jalalabad, security was the fact that he could properly clothe and educate his children and invest in the construction of his house, confident that the little he had today would not be taken away from him tomorrow. His security was quite a different matter from that of the coalition troops in Paktika, fearful of a suicide attack or a renewal of insurgency by the Taliban or Al Qaeda*" (Tadjbakhsh 2005, 4).

As for the problematization of the nation-state relationship, this has been accentuated by the new post-Cold War realities. Thus, during the 1990s and early 2000s, 57 major armed conflicts took place in 45 states, of which only 4 conflicts[3] could be categorized as conventional inter-state conflicts. Thus, the exponential increase in the number of civil wars and intra-state conflicts, resulting in significant loss of life (e.g. through ethnic cleansing) and massive displacement of people putting pressure on various states, demonstrated that "*traditional security approaches could not respond to these problems, as they were not sufficiently sensitive to a range of factors such as cultural, ethnic or religious differences*". Moreover, unconventional threats began to be predominantly directed against society, thus undermining the state's ability to govern and manage threats as a unit (Leucea 2012, 99-100).

[3] The invasion of Kuwait by Iraq and the subsequent international intervention (August 2, 1990); the war between Ethiopia and Eritrea (1998-2000); the conflict between India and Pakistan (1999) and the US-led intervention in Iraq (2003-2011).

Human security: emergence and conceptualization

The idea of a security that considers the *individual* as the object of reference of security studies (*whose security?*) stems from the 1994 Human Development Report of the United Nations Development Program.
The concept of human security *challenges the state-centric security narrative by cultivating an emphasis on the individual as the referent object of security* (Leucea 2012, 105). In this sense, human security is primarily concerned with the "*security of individuals and communities rather than the security of states and combines human rights and human development*" (Kaldor 2010, 214).

The 1994 Human Development Report of the United Nations Development Program is considered to be the first official document to introduce the term human security as a universal, people-centred framework of analysis with *seven (7) interrelated components*, which together lay the conceptual foundation for human security:

- economic security – ensuring a secure basic income;
- food security – physical and economic access to food;
- health security – ensuring a minimum level of protection against disease and infection;
- environmental security – ensuring access to safe drinking water, clean air, and an undamaged land system;
- personal security – protection against physical violence and threats;
- community security – ensuring the security of cultural identity; and
- political security – ensuring protection of fundamental human rights and freedoms (WHO 2002, 2).

Furthermore, the baseline report states *four (4) essential characteristics of human security*: (1) it is a universal concern; (2) its components are

interdependent/interconnected; (3) human security is better ensured through early prevention than late intervention; and (4) it is people-centred (Caballero-Anthony 2002, 23).

As *guiding principles*, human security involves:

- *supremacy of human rights* – as the main difference between human security and traditional, state-centred approaches. In this sense, human security states that fundamental rights, such as the right to life, to a home or the right to freedom of expression must be respected and protected even during conflicts.
- *legitimate political authority* – as the main condition for achieving human security. Thus, human security depends on the existence of institutions/authorities vested with legitimacy and public trust, as well as with a certain capacity to assert themselves. Legitimate institutions/authorities here do not necessarily refer to the state but may include local or regional public authorities or international political arrangements such as protectorates or transitional administrations.
- *multilateralism* – as a principle intricately linked to *legitimacy*, an aspect that distinguishes the human security approach from that of neo-colonialism. Seen from a human security perspective, *multilateralism implies*: (1) a commitment to act together with international institutions and through the procedures of multinational institutions; (2) a commitment to creating common rules and norms, solving problems through regulation and cooperation, and ensuring that rules are enforced; and (3) the inclusion of coordination rather than duplication and rivalry, as an effective approach to human security requires coordination between intelligence, foreign policy, economic exchange policy, development policy and security policy initiatives.
- *the 'bottom-up' approach* – as a guiding principle for decision-making on the type of security and development policies to be adopted. Thus, these policies should be made with an exclusive focus on the most basic needs identified by people affected by violence and insecurity, in which communication, consultation and dialogue are indispensable tools for security and development;
- *regional focus* – as opposed to national focus, given that non-conventional threats are often transnational, materializing through refugees and displaced persons, minorities living in different states, criminal and extremist networks, or other phenomena that transcend the capacity of a single state to manage them (Kaldor 2010, 217-223).

Since the 1994 Human Development Report of the United Nations Development Program, the concept of human security seems to have developed in *two main directions*.

The first was the approach used by the Canadian government, the direction of which was reflected in the Human Security Report published in 2005, which emerged amid

the failure of the international community to combat war crimes, genocide and purge, in which sense the concept of the "*responsibility to protect*" (R2P) was brought into the discussion, which focuses on three main responsibilities: (1) to prevent; (2) to react; and (3) to rebuild (Dungaciu 2019, 529-531). The R2P principle is that, *a state's sovereignty is no longer absolute, but is directly conditioned by the fact that if the state is unable or unwilling to provide its population with basic rights, the international community finds itself obliged to override the sovereignty of the state in question in order to ensure the security of its citizens* (Fukuda-Parr and Messineo 2012, 10). The report also makes a number of important points:

- it redefines the meaning of sovereignty to include a dual responsibility of the state: (1) in external affairs, where the state is responsible to respect the sovereignty of other states, and (2) in internal affairs, where the state is responsible to respect the dignity and fundamental rights of all its citizens;
- it redefines interventions as "*actions taken against a state or a leader, with or without its consent, for purposes defined as humanitarian or protective*". These would include both military intervention and a range of *soft power* alternatives, such as economic sanctions and criminal prosecutions, used mainly as measures to prevent the need for military action. However, the Report stated *six (6) criteria that had to be met for military intervention to be justified*: (1) obtaining authority from the UN Security Council to intervene; (2) the existence of a situation that could lead to significant loss of life or large-scale ethnic cleansing; (3) the existence of the need to stop or avoid massive human suffering; (4) the use of military force as a last resort; (5) the use of appropriate methods/proportionate to the threat; (6) the existence of reasonable prospects for success of the intervention;
- it includes clarifications on the post-intervention policy, which should ensure a return to peace and order, (re-)establishment of justice, reconciliation, and local development. At the same time, the report stipulates the need to set a time limit within which post-intervention policies should be stopped in order to limit the duration of the international community's intervention in the internal affairs of other states (Tadjbakhsh 2005, 14-15).

The second direction was evidenced by the emergence of two documents that attempted to clarify the threats to human security and the measures that the international community should take in this regard. The two documents were: (1) the UN High-Level Panel Report on Threats, Challenges and Change, entitled "*A more secure world: Our shared responsibility*" (2004) and (2) the reform agenda proposed by Kofi Annan, then UN Secretary-General, in "*In Larger Freedom: Towards Development, Security and Human Rights for All*" (2005).

Thus, the Report "*A More Secure World: Our Shared Responsibility*" advanced the cause of human security by establishing a general framework for collective programs to address unconventional threats, which the group shared into six (6) main categories: (1) economic and social threats, such as poverty and deadly infectious

diseases; (2) inter-state conflicts and rivalries; (3) internal violence, including civil war, state collapse and genocide; (4) nuclear, chemical and biological weapons; (5) terrorism; and (6) transnational organized crime. Beyond recognizing these threats, the report also clarified the interlinkages between them, arguing that large-scale development is indispensable for the establishment of the new collective security, which would require a higher degree of intergovernmental cooperation, for which national, regional actors and civil society are a defining element.

The UN High-Level Panel also presented a package of reforms that Kofi Annan proposed in his report "*In Larger Freedom: Towards Development, Security and Human Rights for All*", aimed at restoring the UN's credibility and relevance on collective security issues. Although Kofi Annan's report did not specifically use the term human security, it clearly emphasized "the *links between human rights, development and security as three mutually reinforcing imperatives*". Alluding to the widespread concern about the conditions created when states fail to provide for the basic needs of their citizens, the report noted that these threats "*could undermine not only human survival but also the state as the basic unit of the international system*" (Tadjbakhsh 2005, 12-13).

Whose security and by whom? Security from what threats?

As for the referent of the concept of human security (Whose security?), this is clear from the issues outlined above. *Whose security? The security of the individual* as a basic unit that cannot be broken down is the ultimate reality of social life.

Security by whom? We believe that the responsibility for providing human security lies primarily with the *states*. When states are unable or unwilling to take "responsibility" for their own sovereignty, other actors have, if not an obligation, then at least a "moral responsibility" to act. Thus, in addition to state actors, actors that can play an important role in ensuring human security are: (1) *non-governmental organizations (NGOs)*, whose activities extend beyond the borders of a single state, they can be both service providers, providing humanitarian assistance, monitoring human rights and offering conflict mediation services and can also exert pressure on governments and international organizations; (2) *social movements*, representing groups that are often involved in various forms of protest, they tend to be local in character, although they can also establish cross-border coalitions; (3) *networks*, which represent "loosely articulated coalitions between NGOs and social movements, often using the opportunities offered by the internet to directly publicize the groups' arguments"; (4) *think tanks and commissions*, which are often situated close to elites and primarily use the power of words, shaping specific proposals and policies; and (5) *international mass-media* (radio, television, print and web), which often plays an important role in drawing attention to crises in distant places, being "a tool, an expression of public debate rather than an independent actor" (Kaldor 2010, 34-51).

Moreover, by emphasizing the interconnectedness of unconventional security threats and giving moral priority to the security of individuals, the human security paradigm lays the foundation for a *culture of responsibility* in the sense that, in order to ensure the survival, livelihood and dignity of the population, those in a position of power must submit to new responsibilities:

- first, that of the state, for if sovereignty once meant the monopoly over the legitimate use of violence and the defence of national territory from external threats, *now the state must integrate and submit to the idea of the responsibility to protect its citizens*.
- secondly, the concept of human security requires an increasing recognition of the *role of the people in ensuring their own security*, given that it is the complementary duty and response of the people that will enable the state to assume its true role and gain the legitimacy it needs to achieve that goal. Moreover, as I stated at the beginning of the article, "*security is a public good that involves subjective feelings* and requires people to make demands and requests and to be prepared to make effective use of what they are given", and they in turn have a responsibility to act for the common good at the expense of self-interest.
- third, the concept of human security also holds the international community responsible for fulfilling its responsibility to protect in the event that the state actor is unable or unwilling to fulfil this responsibility. However, what the concept of human security entirely fails to do is to hold the international community accountable in terms of taking the blame (along with the independent state actor) for the mass underdevelopment of certain areas, the existence of famine, disease and continued environmental degradation (Tadjbakhsh 2005, 23-26).

Security from what threats? Threats to security are represented, in the traditionalist view, as external to the state, being a precondition of human nature characterized by a deep sense of insecurity, which instils in the human being distrust and suspicion of other people, peculiarities that spread automatically to all forms of institutionalized forms of human beings, thus creating an anarchy at the systemic level, characterized by the absence of a central, moral authority to direct and resolve in complete impartiality the dissensions between certain individuals or states (Miroiu 2006, 95).

However, new concrete realities in the sphere of international relations have destabilized the conceptual and philosophical foundation of traditional assumptions about the nature and causes of security threats, in which context some scholars have noted the limitations of this perspective and argued for the need to broaden the analytical framework.

Thus, more recent studies under the direction of the Norwegian sociologist Johan Galtung have brought to light a new perspective on human security threats. Galtung defines peace as the opposite of violence, but, for him, violence is not simply the

regulation or controlled use of force by humans but involves "*anything that impedes human self-realization and can be avoided*" (Griffiths 2003, 217). Thus, the novelty brought by Galtung consists in the concept of "*structural violence*", a form of violence that represents "*everything that prevents the self-realization of the human being in terms of the satisfaction of fundamental human needs, which can be physiological, ecological, economic or spiritual*" (Leucea 2012, 125). In this key, he distinguishes four types of violence in world politics: (1) classical violence - which refers to the infliction of suffering through torture or war; (2) poverty - as the lack of minimum living conditions such as food, water, clothing or shelter; (3) repression - as the loss of freedom of individuals to choose and express their own desires; and (4) alienation - as a form of structural violence against our identity and our needs to belong to a community or to establish inter-human relations (Griffiths 2003).

McSweeney also talks about the importance of considering "structural threats", by which he refers to the "*unintended consequences of social action*", i.e. the structure of the global economy, the pattern of power relations and dependencies within it, the profound influence of the food, tobacco and alcohol industries on government policy, gender inequality, relative and absolute poverty levels, income inequality and so on (Stoeva 2020, 5-6).

Also, within peace studies, following the contributions made by the Norwegian sociologist J. Galtung, a distinction can be made between (1) negative peace - as the absence of war, the absence of explicit and overt physical violence and (2) positive peace - as a state of "social justice", characterized by the absence of structural violence, representing, in particular, an idealized form of peace studies (Dungaciu 2019, 478-480).

The problem with concepts that expand the scope of threats to human security is that the "*progressive expansion of the field of security studies jeopardizes the intellectual coherence of security, thereby giving it such a broad meaning that it may become incomprehensible*" (Buzan, Waever and Wilde 2010, 14-15). However, the question remains valid: *security against what threats?*

Among the threats to human security we can consider, without being exhaustive, the following: global infectious diseases (HIV/AIDS, tuberculosis, malaria), respectively pandemics of respiratory infections (SARS-CoV-2, avian flu - H5N1, swine flu - H1N1), but also epidemics of viral hemorrhagic fever (Ebola) (Human Security Course); mental disorders, climate change, biodiversity loss and food insecurity (United Nation Development Programme 2022, Chapter 6); State vulnerability, economic threats (weak economic development limits the resources available to build strong political institutions and the ability of government to meet the needs and demands of the population is limited by a weak economy), transnational crime, environment (biodiversity loss has negative effects on: food security, health, energy security, reduced water availability, degradation of social relations and cultural

identity - given that many cultures value ecosystems or their components, reduced freedom to choose the lifestyle provided by biodiversity, reduction of basic materials), terrorism, violent conflict, lack of law and order, weak state authority coupled with the absence of key public institutions, illegal migration, human smuggling, drug trafficking (Bellamy 2020) and so on.

Although the problem of conceptual ambiguity of human security is one of the frequent criticisms of human security, a simplified table can illustrate, in essence, *the differences between traditional state-centred and human-centred approaches to security*.

TABLE NO. 1

The difference between the traditional state-centred approach and human-centred security

	TRADITIONAL (STATE-CENTERED) SECURITY	HUMAN CENTERED SECURITY
SECURITY REFERENT	In a Hobbesian world, *the state is the main provider of security*: if the state is secure, then those who live in it are secure.	*Individuals are equal to the state* in terms of importance as the referent object of security. State security is a means, not a goal.
PROTECTED VALUES	Sovereignty, power, territorial integrity, national independence.	Personal security, well-being, and individual freedom. Physical security and basic needs. Personal freedom (freedom of association). Human rights, economic and social rights.
SECURITY THREATS	*Direct* organized violence by other states, violence, and coercion by other states.	*Direct* violence (death, drugs, dehumanization, discrimination, international disputes, weapons of mass destruction) and *indirect* violence (deprivation, disease, natural disasters, underdevelopment, displacement, environmental degradation, poverty, inequality), from *identifiable* sources (such as states or non-state actors) or *structural* sources (power relations ranging from the family to the global economy).
PROTECTING BY WHAT MEANS?	Retaliatory force or the threat to use it, balance of power, military means, consolidation of economic power, little attention to law enforcement or institutions.	Promote human development: basic needs plus equality, sustainability and greater democratization and participation at all levels. Promoting political development: global norms and institutions plus collective use of force, as well as sanctions if and when necessary, cooperation between states, trust in international institutions, networks and coalitions and international organizations.

Source: table taken in full of Shahrbanou Tadjbakhsh, *Human Security: Concepts and Implications with an Application to Post-Intervention Challenges in Afghanistan*, Centre for Peace and Conflict Resolution, Sciences Po, 2005, p. 28.

Approaches and debates on human security

As can be seen from the issues outlined above, there is no consensus on threats to human security. Although *proponents* of human security agree that the object of reference of security is the individual and the protection of the individual, there is

debate as to what this entails. The difference of opinion on human security divides proponents of this approach into three schools of thought:

- *the minimalist approach* argues that "the threat posed by political violence by the state or other organized political actor against people must be the primary concern of the concept of human security" which means "protecting people and communities from internal conflict, war or other forms of violence", thus aiming to maintain conceptual clarity and analytical rigour that does not "fall prey" to the over-extension of the security agenda. The minimalist definition of human security is succinctly summarized as *'freedom from fear'*, shaped by works such as Professor Andrew Mack's 'A Signifier of Shared Values', 2004.
- *The maximalist approach* opposes the reductionist view of the minimalists, arguing that human security must encompass more than *'freedom from fear'*. In the maximalist approach, human security must also refer to *'freedom from want'*. For Ramesh Thakur, a maximalist, in his book 'A Political Worldview' (2004), human security means "*protecting people from critical situations, from risks and assaults on human life, whether the threats are related to social activities or natural calamities, whether the source of these threats is within the borders of a state or outside, whether they are direct or structural*".
- *the circular approach to human security*, which seeks to substantiate an analytical framework based on both minimalist and maximalist approaches. Thus, this analytical framework "focuses on human insecurity generated by political violence and the causes of this state. In social science language, human insecurity as political violence (minimalist school) is the dependent variable. Included among the many causes of political violence are the problems of underdevelopment (characteristics of the maximalist approach), and these are independent variables". One of the proponents of this approach is Pauline Kerr, who argues that this framework of analysis has several advantages, namely (1) the connection between the two approaches is quite clear; (2) causal links can be multi-factor and inter-linked; (3) causality can have a circular dynamic; and (4) because it identifies the problem of violence and its causes, the approach can provide decision support in the development of certain policies (Leucea 2012, 114-119).

Criticisms of the concept of human security are mainly based on the *conceptual ambiguity* of the term, which is caused by the fact that "*in trying to be all-encompassing, it has come to mean nothing*". To address this problem, authors Gary King and Christopher J. L. Murray consider that a useful approach would be to include only those domains of well-being that "*have been important enough for human beings to fight for or put their lives or property at risk*" (King and Murray 2001-2002, 593).

At the same time, critics have argued that "*human security lacks sufficient political traction*" because the approach is far too broad "*to serve as a guide for academic research or government policymaking*" (Stoeva 2020, 3), and the crowded list of

threats to human security "*makes it impossible to prioritize political action*", thus leaving the call for quick military solutions as the only option. Thus, advocates of the narrow approach such as S. Neil MacFarlane and Yuen Foong Khong (2006) consider that "*a definition of human security that includes so many components, from the physical to the psychological, without a clearly established hierarchy, presents difficulties for policymakers forced to choose between competing objectives and focus their resources on specific solutions to immediate problems*". On the other hand, proponents of the broad approach to human security, such as Mary Kaldor and Shannon Beebe (2008), Lincoln Chen and Vasant Narasimhan (2003), Shahrbanou Tadjbakhsh and Anuradha Chenoy (2007) or Caroline Thomas (2001), consider, in one form or another, that the approach "*does not seek to elevate every possible problem to the highest political priority, but merely to set thresholds below which people's lives are endangered and their dignity threatened*", and that the prioritization invoked by critics "*may be an exercise in futility, since the concept is based on the assumption that all threats are interdependent*", in the sense that removing a threat will have little effect without "*the implementation of comprehensive security that restores the dignity of individuals*" (Tadjbakhsh 2005, 8).

Last but not least, some of the criticisms of human security are sharpened by a number of state actors, such as the G77 group, which comprises mostly developing countries and for whom the concept of human security "*is still an ethnocentric paradigm emphasizing subjective issues and values*" representing "*yet another attempt by the West to impose its liberal values and political institutions on non-Western societies*", as well as a criterion that challenges "*the sovereign role of the state, threatening the intervention of the international community on behalf of the people*" (Tadjbakhsh 2005, 10).

Conclusions

Paradoxically, the conceptual ambiguity and the breadth of the threat agenda, the main targets of this concept's critics, seem to be the *de facto* main source of its strength and attractiveness.
Beyond considering this concept as a "*mature*" one in terms of conceptual clarity and analytical rigor, the concept of human security has often been attributed to the category of normative concepts, its practical usefulness being that of regulating or prescribing the ideal behaviour, relationships or processes that the panoply of actors on the international relations scene should adopt in order to *free individuals from fear and wants*.

Starting from here, we consider that the usefulness of the concept of human security translates into several strengths, namely: (1) through the magnitude of the threat agenda, the concept creates a sense of urgency and collective responsibility to act, an aspect that gives the concept a mobilizing role; (2) it contributes to guiding positive

analysis by describing facts, processes or relationships without including value judgments, through objective approaches based on observations, data and verifiable facts; (3) it provides a set of terms and definitions that gives a 'common voice' to the international community and can also contribute to policy development; and (4) it provides a scale for assessing progress and identifying conceptual, procedural and action gaps around the issue at hand.

Thus, we believe that the dynamics, flexibility, and adaptability of human security should remain one of its "analytical rigors", as only in this way is the concept able to respond to the complex challenges of global human insecurity. Although it is criticized for its breadth, the essence of human security is simple: prevention of the worst situations that threaten human life and dignity. In this sense, the concept is a call for collective reason and responsibility, emphasizing a deep understanding of the causes of global human insecurity and the development of effective solutions to manage them.

References

Bellamy, Paul. 2020. „Threats to Human Security." *Human Security in World Affairs: Problems and Opportunities (2nd edition).* https://opentextbc.ca/humansecurity/chapter/threats-human-security/.

Buzan, Barry, Ole Waever, and Jaap de Wilde. 2010. *Securitatea. Un nou cadru de analiză.* Translated by George Jiglău. Cluj-Napoca: CA Publishing.

Caballero-Anthony, Mely. 2002. „Overview of Health and Human Security Case." *Health and Human Security: Moving from Concept to Action-Fourth Intellectual Dialogue on Building Asia's Tomorrow*, 21-44. https://jcie.org/researchpdfs/HealthHumSec/health_overview.pdf.

Dumitrescu, Lucian. 2020. *Narațiuni Strategice. Securizare și legitimitate în relațiile internaționale* . București: Editura Institutului de Științe Politice și Relații Internaționale „Ion I.C. Brătianu".

Dungaciu, Dan. 2019. *Enciclopedia de diplomație.* București: Editura RAO.

Fukuda-Parr, Sakiko, and Carol Messineo. 2012. "Human Security: A critical review of the literature." *Centre for Research on Peace and Development (CRPD)*, CRPD Working Paper No. 11 ed. https://sakikofukudaparr.net/wp-content/uploads/2013/01/HumanSecurityCriticalReview2012.pdf.

Griffiths, Martin. 2003. *Relații internaționale: școli, curente, gânditori.* București: Editura ZIUA.

Human Security Course. n.d. "Health as human security." Accessed ianuarie 15, 2025. https://humansecuritycourse.info/module-4-human-security-in-diverse-contexts/issue-4-health/.

Kaldor, Mary. 2010. *Securitatea umană.* Translated by Monica Andriescu, Ana-Maria Butiurcă and Andrei Aroneț. Cluj-Napoca: CA Publishing.

King, Gary, and Christopher J. L. Murray. 2001-2002. "Rethinking Human Security." *Political Science Quarterly*, No. 4 ed.: 585-610. doi:https://doi.org/10.2307/798222.

Leucea, Ioana. 2012. *Constructivism și securitate umană.* Iași: Editura Institutul European.

Miroiu, Andrei. 2006. *Manual de relații internaționale.* Iași: Editura POLIROM.

Robinson, Paul. 2010. *Dicționar de securitate internațională.* Traducere de Monica Neamț. Cluj-Napoca: CA Publishing.

Sava, Ionel Nicu. 2005. *Studii de securitate.* București: Centrul Român de Studii Regionale.

Stoeva, Preslava. 2020. „Dimensions of Health Security—A Conceptual Analysis." *Global Challenges* Volume 4 (Issue 10). doi:https://doi.org/10.1002/gch2.201700003.

Tadjbakhsh, Shahrbanou. 2005. „Human Security: Concepts and Implications with an Application to Post-Intervention Challenges in Afghanistan." *Center for Peace and Conflict Resolution, Sciences Po,.* https://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/etude117_118.pdf.

United Nation Development Programme. 2022. „Chapter 6 - Healthcare systems outmatched by new human security challenges." *NEW THREATS TO HUMAN SECURITY IN THE ANTHROPOCENE*, ed. PART II — TACKLING A NEW GENERATION OF THREATS TO HUMAN SECURITY: 118-137. https://hs.hdr.undp.org/pdf/srhs2022_chapter6.pdf.

World Health Organization [WHO]. 2002. "Health and Human Security." *Regional Committee for the Eastern Mediterranean, Forty-ninth Session, Agenda item 9.* Accessed ianuarie 15, 2025. https://applications.emro.who.int/docs/em_rc49_7_en.pdf.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Impact of equipping with 155 mm self-propelled howitzer systems from the perspective of combat functions

LTC Adrian MIREA*

*"Carol I" National Defence University, Bucharest
e-mail: mirea.adrian@yahoo.com

Abstract

This article brings into focus a useful way of understanding the impact that 155 mm self-propelled howitzer systems in the prospective equipment of national armed forces could have on the conduct of land force operations. The operational framework described by the warfighting functions is a useful tool to understand how the force commander can capitalize on the available capabilities according to operational needs. In writing this paper, I considered the contribution of 155 mm self-propelled howitzer systems to the fulfilment of each warfighting function from the perspective of friendly forces but, within each function, I have also considered the potential for its disruption, from the enemy's perspective. In the first part of the article, I briefly presented basic aspects of the warfighting functions and then detailed a perspective on the impact that equipping with 155 mm self-propelled howitzer systems can have on the conduct of land forces operations. Given that these self-propelled howitzer systems employ 155 mm NATO standard ammunition, I have explored in this article the possibility of using the full range of such ammunition without limiting myself to those mentioned in the purchase contract with the Korean manufacturer. Analyzing in this article the impact of equipping with 155 mm self-propelled howitzer systems emphasizes in my view, the usefulness and applicability of the operational framework described by the warfighting functions including in analyzing the potential of any existing or prospective capabilities, whether belonging to friendly forces, to the enemy or belonging to another actor of interest present in the area of operations.

Keywords:
warfighting functions; self-propelled howitzer; fire support; operational framework; capability.

Article info
Received: 3 February 2025; Revised: 3 March 2025; Accepted: 7 March 2025; Available online: 2 April 2025

Citation: Mirea, A. 2025. "Impact of equipping with 155 mm self-propelled howitzer systems from the perspective of combat functions." *Bulletin of "Carol I" National Defence University*, 14(1): 169-183. https://doi.org/10.53477/2284-9378-25-11

The integration of the new fire support capabilities that will become part of our national land force structures will probably also lead to an in-depth analysis of how these capabilities can be exploited to their full potential in operations – especially combat operations. Warfighting functions are, in my view, a useful tool to understand how the force commander can leverage the available capabilities according to operational needs. As the way in which these warfighting functions are accomplished can also represent a description of the capabilities available at a given moment, this tool can also be exploited to highlight solid arguments to justify the need to provide a certain capability to accomplish the force structure given mission.

By exploring how warfighting functions are performed, one can secure a better understanding of the capabilities` potential available to force structures and, as a logical consequence, can highlight unmet needs that may jeopardize mission success. The usefulness of this tool is also applicable in studying the capabilities of a potential enemy or another actor of interest at a given moment, which will enable commanders and staff members to better understand the confrontation environment and facilitate the determination of centres of gravity for their own forces, for the enemy forces or any other actor of interest in the area of operations.

I have set out, through this article, to bring to attention a novel and useful way of understanding the potential impact on operations of 155 mm self-propelled howitzer systems in the prospective equipping of our national land force structures. For this purpose, I considered the contribution of 155 mm self-propelled howitzer systems, first of all, to the fulfilment of each warfighting function from a friendly forces perspective and, secondly, I took into account the possibility of disrupting the same warfighting functions from an enemy perspective.

For this paper, I have used the method of documentary analysis as I considered it suitable for the systematic selection, review and evaluation of information sources – of an unclassified nature only. In substantiating the article, I explored open sources of information such as websites and authored works, along with specifications of doctrines and field manuals in force at NATO and national levels. Data collection, analysis and interpretation were, as I mentioned, systematically carried out based on documentary analysis (Okoko, Tunison and Walker 2023, 140), a useful research method, but also sufficient in my opinion, for understanding and synthesizing the relevant aspects in the field of study for this paper.

The framework described by warfighting functions in land forces operations

The warfighting functions are a tool that the commander assisted by his staff has at his disposal, to ensure a comprehensive approach to all aspects of land forces operations. The importance of warfighting functions also lies in the fact that, by

synchronizing the effort of available forces in these directions, courses of action and the concept of operation are also developed. Through warfighting functions the commander can visualize the specific activities and actions of his structures within the existing operational framework and, on this basis, he can also describe the actual capabilities of the force. In addition, the warfighting functions assist the commander in determining the force requirements for the conduct of the operation (NATO 2022, 105) and can also argue the modern capability needs of available force structures to perform in the current operational environment.

Warfighting functions in land forces operations are derived from joint functions which, from a NATO (NATO 2022, 105) as well as a national perspective (SMG 2011, 70; SMG 2014, 26), cover *manoeuvre, fires, command and control, intelligence, force protection, information operations, sustainability* and *civil-military cooperation*. The actual characteristics of land operations have led to an adaptation of the joint functions and, at the national level, according to the Land Forces Operations Doctrine F.T.-1 of 2017, which implements the provisions of the Allied Joint Doctrine For Land Operations AJP-3.2 of 2015, these functions are (SMFT 2017, III-13):

- Command and control;
- Intelligence;
- Maneuver;
- Fire support;
- Mobility and protection;
- Information Operations;
- Sustainment.

Given the purpose of this paper, to analyze the impact of a new fire support capability based on these warfighting functions, I will briefly present their fundamental ideas.

Command and control represents the central warfighting function which involves the exercising commander's authority over available force structures to accomplish the established mission. By *command,* we understand the commander's authority and the art of commanding forces in operation, but the command is also the basic element that ensures that the full potential of the available capabilities is explored. *Control* is the process by which the commander, assisted by his staff, organizes, directs and coordinates the activities of force structures. Control is exercised by using standard operating procedures and operating communications equipment within information systems (NATO 2016, 2-16). A key issue, in my view, is the reliance of the command and control architecture on visible capabilities in the electromagnetic spectrum, an increasingly contested and congested environment in today's conflicts.

Intelligence is indispensable to a coherent understanding of the operating environment and supports decision-making. This warfighting function integrates actions and activities conducted at the command level and collection elements to elaborate intelligence products resulting from the information cycle. Thus, the data

collected is processed and analyzed to generate and disseminate information about the enemy, friendly forces, terrain, weather, etc., as directed by the commander's intelligence requirements.

Maneuver as a warfighting function integrates tasks and systems that involve the movement and employment of forces to secure an advantageous position over the enemy (Department of the Army 2022, 2-2). Through manoeuvre, combat power is concentrated where it has a decisive effect on enemy operations by preventing, neutralizing, or disrupting them (NATO 2019, 1-21). An important aspect is the fact that manoeuvre, although manifested in the physical space, can produce psychological effects and influence the enemy's morale by creating situations of uncertainty or confusion.

Fire support as a warfighting function integrates lethal and non-lethal systems fires in coordination with manoeuvre forces both to physically destroy available enemy capabilities and to neutralize or disrupt enemy actions. In fact, *manoeuvre* and *fire support* are essential complementary functions to accomplish mission objectives. Although engagement by fire can be exploited independently, in combination with manoeuvre effects like destroying or neutralizing the enemy's forces and disrupting the enemy's manoeuvre to facilitate the action of friendly forces are achieved. Similar to manoeuvring, engagement with fire can have physical effects such as destruction, but also psychological effects as lowering enemy morale.

Mobility and protection as a warfighting function is about ensuring freedom of movement and force protection by reducing the vulnerability of military personnel and equipment to threats or situations that may jeopardize mission accomplishment. Mobility has two components: on the one hand, it involves ensuring favourable conditions for the movement of friendly forces in the tactical field through specific actions such as ensuring the viability of communication routes, crossing or bypassing obstacles, etc., and, on the other hand, it aims to prohibit or limit the mobility of enemy forces (countermobility) by exploiting friendly fire support assets, by carrying out destruction works, setting up barricades, etc. Force protection is the responsibility of commanders and all personnel to eliminate or reduce the risks and effects of threats that could diminish combat power, operational effectiveness or freedom of action for friendly forces. Specific to force protection are activities such as camouflage and force dispersal, engineer support, air defence, CBRN (Chemical, Biological, Radiological and Nuclear) or electronic protection.

Information Operations integrate actions and activities aimed at modifying information in order to create effects on the enemy's capabilities, will to fight and ability to understand, thus supporting the achievement of friendly forces objectives. I would mention as representative in this field misleading, psychological operations and the physical destruction of information system elements (SMG 2014, 33).

Sustainment is the warfighting function responsible for providing required resources for the execution of the operation throughout its development. The importance of sustainment is obvious in any type of operation since it aims as a warfighting function to provide logistical support (supply, maintenance, transportation, etc.), to maintain or restore the combat power of force structures and has a direct impact on the tempo (rhythm) and intensity of actions.
Any of the available capabilities of the force can be exploited and utilized in one or more warfighting functions. The actual way in which forces and assets are combined and integrated into warfighting functions is usually detailed in the operation order.

The impact of equipping land forces with 155 mm self-propelled howitzer system

According to the national equipment programs, published on the Ministry of National Defense website, we have a program in preparation for equipping with a Battalion level 155 mm howitzer system in order to provide direct fire support to manoeuvre structures (MApN 2024). The nationally agreed version of this capability is the K9 Thunder 155 mm self-propelled howitzer of Korean production (Curtifan 2024a). According to the same source, the contract with Hanwha Aerospace provides for the acquisition of 54 K9 howitzers and 36 K10 refuelling vehicles. A notable aspect, from my point of view, is the production of such systems including at the national level where, according to the same sources, the Korean manufacturer will build a specially designed factory.

In analyzing the impact of equipping with this type of self-propelled howitzers, I also took into account the components of these systems as described in open sources of information. Thus, each of the self-propelled howitzer system has at battalion level, the following components (Soare 2024):

- 155 mm self-propelled howitzer, tracked (K9) - 18;
- 155 mm spare barrel - 9;
- Specialized ammunition carrying and loading machine (K10) - 12;
- Self-propelled artillery observation post - 9;
- Meteorological auto station - 1;
- Technical Evacuation of Damaged Equipment (TEHE-VAC) - 3;
- Acoustic reconnaissance system - 3.

Another important and novel aspect in the realization of this work is the fact that, in the impact analysis, I considered all types of ammunition that such a self-propelled howitzer system can employ. I have thus ignored the current range of ammunition included in the value of the purchase contract which is limited, even elementary in my view, including only 155mm explosive, smoke, illumination and inert rounds for training. Being a system that can use 155 mm NATO standard ammunition, I have

taken into account both the basic explosive ammunition - with a maximum range of 30 km, as well as other types of 155 mm NATO standard such as the M982 Excalibur guided projectiles (Orjanu 2024), those with DPICM (Dual-Purpose Improved Conventional Munition) or RAP (Rocket-Assisted Projectiles) - with a maximum range of 40 km (Global Defense News 2024b). According to other sources (European Security & Defence 2022), some versions of 155 mm RAP-type munitions can have a maximum range of over 50 km.

TABLE NO. 1

SWOT analysis on equipping national land forces with 155 mm self-propelled howitzer system

STRENGTHS	WEAKNESSES
- The most common self-propelled howitzer system worldwide in the last decades; (Namuwiki 2024) - Combat proven system with versions being exploited in the Ukrainian conflict (e.g.: Poland provided Krab); (Ukrinform 2024) - Equipping with such self-propelled howitzer systems contributes to Romania's deterrence strategy of armed aggression; - It contributes to achieving national capability targets assumed within NATO; - As self-propelled systems, they have a high degree of mobility ensuring both increased survivability - in case of counter-battery fire, and increased flexibility in executing fire missions; - They have the required level of technical interoperability with allies from both command and control systems and exploited resources – 155 mm NATO munitions, fuel and lubricants, spare parts, etc.; - It can execute *shoot and scoot*, ensuring an adequate level of survivability in the evermore transparent confrontation environment; - It can engage targets at longer ranges than current towed artillery systems; - They use automated fire control systems that allow a high rate of fire; - Systems include K10 vehicles for resupply with munitions which are automated (robotized) even under enemy fire; (Global Defense News 2024b) - It can use a wide range of 155 mm NATO standard ammunitions with different payloads, including submunitions; - They can execute fire missions in a MRSI (Multiple Rounds Simultaneous Impact) fashion so that one howitzer can strike a target with multiple rounds simultaneously as they travel on different trajectories; - The system integrates acoustic systems for battle space reconnaissance.	- As they represent an important capability for land force structures in all types of operations, 155 mm self-propelled howitzer systems will `become` high-value target/high pay-off target from the enemy perspective that, most likely, will assign additional resources to destroy or diminish their combat power; - The need to assign specialized resources for systems, physical protection and air and missile (drone) defence because, as I mentioned these performant systems will be hunted throughout the entire operation; - The need to provide multispectral protection for such systems – beyond classical camouflage against optical sensors – to protect them against sensors that exploit the infrared, acoustic or electromagnetic spectrum; - Standard operating procedures for using self-propelled howitzers include a higher dispersion in the land forces area of operations, with implicit risk of enemy counter-battery fire upon other friendly structures elements – manoeuvre, command and logistic support, etc.; - Reduced number of crew members can be problematic for exploiting systems over extended periods of time. Towed artillery systems they will be replaced have a higher number of personnel that can also operate in shifts; One other challenge will be organizing the close defence of firing positions with a reduced number of crew members; - National acquisition contract for 155 mm self-propelled howitzer systems does not currently include specially designed antiarmor rounds for both maximum range and in close combat, especially for the close defence of firing positions. Replaced towed 152 mm howitzers and gun-howitzers have the possibility to use armour-piercing rounds and shaped charges for fighting armour.
OPPORTUNITIES	**THREATS**
- Possibility of producing the systems locally with the implicit possibility of operational maintenance through national effort; - Possibility of producing 155 mm NATO standard ammunition locally, as part of partnerships with various dedicated companies in the field; (Curtifan 2024b) - Potential access to future versions of the K9 system, more performant in engaging targets at over 80 km in autonomous conditions (with no crew) (Global Defense News 2024b) - Possibility to participate in multinational exercises capitalizing on Romania's member status in the ASCA (Artillery System Cooperation Activities) community; (Orjanu 2023) - Possible use of entire 155 mm NATO standard ammunition, including those guided type M982 Excalibur; (Orjanu 2024)	- Partial capitalization of systems potential due to current limitations in national ISR (Intelligence, Surveillance and Reconnaissance) capabilities; - Over time reduced effectiveness of self-propelled howitzer systems due to lessons learned by potential hostile actors in recent conflicts such as the Russo-Ukrainian war; (Newsweek 2024) - If nationally provided consumables (including munitions) and component elements are not available, exploiting self-propelled howitzers can become problematic in a crisis and conflict situation, when access to external supply sources would be limited or prioritized; - Some 152 mm munitions, used by current artillery systems, have no equivalent in the 155 mm munitions range that the K9 self-propelled systems use (e.g.: concrete-piercing and armour-piercing rounds, shaped charges or leaflet shells).

Given thus the full scope of fire support capability offered by the 155 mm self-propelled howitzer system I was able to explore how to exploit them according to the operational framework described by the warfighting functions. First of all, I found it useful to provide a perspective on the equipping of national land forces with such systems in the form of a SWOT analysis.

To address the contribution that 155 mm self-propelled howitzer systems can have to the warfighting functions, I have also taken into account the possibility of disrupting the conduct of the same functions from the enemy's perspective, realizing, in my view, a more comprehensive analysis of the potential within studied capabilities in this paper. This approach is based on the elementary role of any fire support system - to engage by fire high-value targets in the enemy's combat formation, with the effect of diminishing his possibilities to fulfil warfighting functions.

Command and control

Equipping land force structures with 155 mm self-propelled howitzers comes with certain advantages in terms of performing the *command and control* warfighting function. The maximum target engagement rate, in conjunction with the performance of the automated fire control systems howitzers have, determines superior efficiency in the execution of counter-battery fire, thus providing superior protection for the command and control systems of friendly forces. This assertion is based mainly on the ability of self-propelled howitzers to effectively combat enemy fire support systems since these assets can endanger both command posts and other components of information systems or communications centers, involved in the command and control of friendly force structures.

Available automated fire control systems alongside the possibility of rapid execution of fire missions using self-propelled howitzers, can be exploited more effectively in comparison with the towed artillery systems they will replace, particularly in engaging targets of opportunity or targets arising in the dynamics of combat actions and against targets classified as TST (Time Sensitive Target).

From a different perspective, the increased range, the automated fire control system and the specific firing rate of self-propelled howitzers allow friendly forces to effectively engage enemy command posts - especially those at the tactical level, as well as elements of information systems or communication centres that these command posts exploit, thus ensuring the disruption of enemy's *command and control* warfighting function.

Intelligence

The equipping and combat employment of 155 mm self-propelled howitzers imply using available automated fire control systems. Thus, the *intelligence* warfighting

function is assisted by the contribution of the fire command and control subsystems to creating the operational picture, exploiting as well the specific data collection capabilities, such as the optical and acoustic battle space reconnaissance kits - integral components of the 155 mm self-propelled howitzer system. Another contribution to the intelligence function is materialized in the form of artillery fire for reconnaissance purposes, where the advantages of increased mobility and rapid execution of fire missions can be exploited for the timely collection of data and information regarding the structure of the enemy's operation in all its aspects – displacement of forces, available fire system or engineer support.

The disruption of the enemy's *intelligence* warfighting function is achieved by degrading its ability to understand the real operational situation by depriving him of information while performing specific lethal tasks with friendly fire support systems. Thus, the destructive potential of self-propelled howitzers can be harnessed against elements of the enemy's reconnaissance systems (radars, radiolocation stations, observation posts, etc.), against elements of high-precision striking systems (e.g., drone launch platforms, laser guidance systems for guided munitions, etc.), as well as against the enemy's electronic warfare assets. Another way to disrupt the enemy's *intelligence* function is to exploit 155mm self-propelled howitzer systems within the framework of deception plans, developed at the task force level, in order to "provide" him with information describing an altered operational picture, favourable to the actions of friendly forces.

Maneuver

One of the essential roles of any fire support system is to support the maneuver of fighting elements, therefore equipping with modern artillery systems will have a major impact on the combat power of these forces. The main characteristics of the 155 mm self-propelled howitzer system, such as maximum target engagement range, firepower or high degree of mobility, determine an increased capability of the systems to provide permanent and timely fire support to manoeuvre forces in all forms of combat they adopt in the operation.

Another aspect that may influence the *manoeuvre* warfighting combat is that the availability of modern artillery systems, such as the 155 mm self-propelled howitzer systems, will also provide, in my opinion, a moral boost for the manoeuvre forces that will benefit from the fire support provided by these systems in achieving their set objectives.

From the enemy's point of view, disrupting the *manoeuvre* warfighting function is achieved by prohibiting the concentration of forces, and therefore their effort, in certain important directions or on the objectives targeted by friendly forces. Manoeuvre disorganization can be facilitated by exploiting the potential of 155 mm self-propelled howitzer systems to mass fire rapidly, at considerable distances and

with high accuracy on various targets in the tactical depth of the enemy combat formation. This highly destructive potential of a 155 mm self-propelled howitzer is mainly due to the technical characteristics of the gun and ammunition used, as well as the availability of automated fire control systems. The use of these self-propelled howitzers will reduce the enemy's combat potential, both in terms of achieving physical effects on military personnel and equipment and achieving psychological effects reflecting on the morale of enemy troops.

Fire support

Self-propelled howitzer systems are primarily intended to provide fire support for the force structures they will be a part of. They will also form the basis of the strike system available to the force, through which it is planned to achieve effects, especially lethal, on enemy personnel and fire systems in accordance with friendly forces' operational requirements. The contribution of 155 mm self-propelled howitzers in the *fire support* warfighting function is closely linked to the *manoeuvre* function as the fire support systems available to the force are a power multiplier of manoeuvre structures in all types of operations. Whether we talk about fire preparation for the attack in an offensive operation, the execution of a defensive fire barrage in front of friendly positions or we consider covering fire for a forward base in a stability operation, the scheme of manoeuvre at the force level has the fire support system as a combat power multiplier, where the superior possibilities of the 155 mm self-propelled howitzer systems can be timely exploited.

In terms of disrupting the enemy's *fire support* warfighting function, the superior characteristics of the 155 mm self-propelled howitzer can be used to neutralize (destroy) the enemy's fire support systems throughout the entire operation. Thus, the increased mobility of self-propelled howitzers (especially in *shoot and scoot*) and the increased firepower accurately applied to targets at considerable distances, in conjunction with automated fire control systems and modern enemy artillery detection capabilities (included in the same equipment program or already existing at the national level), will allow these systems to be used effectively for counterbattery fire. The possibility of executing *shoot-and-scoot* fire missions provides self-propelled artillery systems with a much higher survivability rate compared to towed ones, and this is evident even in Ukraine where self-propelled howitzers of an older generation - such as the M109 Paladin donated by the USA, successfully provided fire support to manoeuvre forces even in close proximity to the frontline (Altman 2023), and were very difficult to counter by enemy artillery.

Denying or making ineffective enemy artillery fire (field artillery or anti-aircraft artillery) is a major objective in all types of operations, and these effects can be achieved by using the full range of 155 mm NATO standard munitions, as counter-battery fire does not only involve reactive fire against enemy assets in firing position but also includes a proactive component aimed at blinding enemy sensors (with

smoke or illumination munitions), hitting command points or disrupting the logistic support of the enemy fire support system (with incendiary and precision rounds or using various submunitions).

Mobility and protection

The contribution of 155 mm self-propelled howitzer systems to the *mobility* of forces consists primarily in diminishing the enemy's potential to create explosive or non-explosive obstacles in the area of operations, by destroying/neutralizing specialized military equipment or enemy elements specially designed for countermobility. Here I have in mind aspects like neutralizing enemy special-purpose detachments - such as those intended for destroying infrastructure components in the area of operations, the destruction of military equipment intended for creating minefields or those generally used to shape the battlespace for countermobility purposes (engineering equipment for example). Compared to the classical artillery they will replace, self-propelled howitzer systems have certain superior technical characteristics which will facilitate the surprise engagement of enemy elements mentioned above, at considerably greater ranges, with high accuracy and lethality. Another contribution in the field of mobility can be the actual destruction by fire of explosive and non-explosive obstacles, where the diversity and destructive potential of 155 mm NATO standard munitions can be exploited.

Regarding the countermobility component of this warfighting function, self-propelled howitzer systems will contribute by destroying at long ranges the enemy's military equipment and other elements involved in securing freedom of movement for his forces. In this regard, I am considering aspects such as the destruction of mobile assault bridges and other specialized enemy capabilities used for gap crossing or the restoration (reinforcement) of communication routes in the area of operations. Destruction of infrastructure elements (e.g. bridges, roads, railroads, etc.) can also assist countermobility, but an important contribution, in my view, of self-propelled howitzer systems to countermobility is the use of 155 mm projectiles with submunitions designed to create minefields as an obstacle, both for the purpose of protecting friendly forces and to deny, channel or delay enemy action on certain directions or in certain areas.

The main contribution of 155 mm self-propelled howitzer systems to force protection is their high capability to combat, effectively and from a distance, elements of the enemy fire support system. As mentioned above, within the fire support warfighting function, disrupting this enemy function constitutes an important contribution to eliminating or reducing the risks and effects of threats that could diminish the combat power, operational effectiveness or freedom of action of friendly forces. Thus, 155 mm self-propelled howitzer systems will be used primarily against the enemy's artillery and ground-based missiles, especially those constituting weapons of mass destruction, as well as against enemy high-precision striking systems, which in my view includes combating drone launch platforms.

From a different perspective, being high-performance systems and, as mentioned in the SWOT analysis, representing an important capability of land force structures in all types of operations, 155 mm self-propelled howitzers will "acquire" the status of high value/high pay-off target and the enemy will seek by multiple means to take them out of the fight. From this point of view, the impact of equipping with such systems on force protection comes in the form of the need to allocate additional resources to providing physical protection of self-propelled howitzers in the modern confrontation environment, especially against drones or loitering munitions. As an argument example, we have the successful use of Lancet drones to hunt down and destroy Krab self-propelled howitzers (Technology.org 2024), similar to those in the national equipping program.

From the enemy's perspective, the disruption of the *mobility and protection* warfighting function involves two aspects. First, the above-mentioned aspects of the mobility and countermobility of friendly forces can be viewed against the respective countermobility and mobility of enemy forces. Second, force protection from the enemy's perspective can be disrupted by the very existence of 155 mm self-propelled howitzer systems. This will impose a considerably greater effort on the enemy to provide force protection over a significant depth within the area of operations where these systems can be employed. From another perspective, the effectiveness of 155 mm self-propelled howitzer systems in counter-battery fire can be an important factor in making enemy manoeuvre forces vulnerable at certain moments of the battle, when they have a greater need for fire support - for advancing towards contact, attacking defended positions, executing a counterattack, etc. Equipping friendly force structures with 155 mm self-propelled howitzer systems will constitute a permanent threat to the enemy's combat power, operational effectiveness or freedom of movement of forces, which will have to be countered or mitigated by active and passive measures throughout the operation.

Information Operations (INFO OPS)

Equipping force structures with 155 mm self-propelled howitzer systems can contribute to the *information operations* warfighting function in various ways. First, the availability of such modern systems can be promoted and exploited to boost the morale and combat readiness of friendly forces, aspects with a direct impact on the combat power of the force as a whole. Secondly, the presence of such systems in the area of operations and their operational effectiveness will be propaganda elements to discourage enemy troops or to influence them psychologically and morally. An example in this respect is the exploitation of the maximum range at which 155 mm self-propelled howitzers can engage targets in the enemy's combat formation to determine deployment of forces or resources concentrations at increased distances from the front line, thus producing effects on the morale of enemy forces in the contact area of operations. Such a role was played by HIMARS systems in the Russian-Ukrainian conflict (Kosoy 2024) and, in my view, access to 155 mm munitions

with a maximum range of 50 km (European Security & Defence 2022) or 80 km (Global Defense News 2024a), will allow even self-propelled howitzers to "push" the concentrations of resources needed by the enemy in the contact area of operations.

From a different perspective, the self-propelled howitzers "status" of high value/high pay-off target for the enemy could be exploited within the information operations function, in order to diminish the enemy's ability to understand the operational environment, stimulating its sensors through specific fire actions and activities, indicating multiple firing positions, false attacks or new directions of effort at the force level. The superior characteristics of self-propelled howitzers can thus be exploited, particularly in the field of mobility and automated fire control. As an example of the exploitation of the high value/high pay-off target status for the enemy, I may mention the role played by HIMARS systems in misleading the Russian forces by concentrating their efforts, initially in the Herson region, followed by a Ukrainian counter-offensive in the Kharkov region (Toroi 2024, 34).

In terms of disrupting the *information operations* warfighting function from the enemy's perspective, self-propelled howitzers can be exploited to combat the enemy's propaganda potential, either by physically destroying components - such as communications systems or by anticipating and countering disinformation in general that involves 155 mm self-propelled howitzers. The essential element, in my view, in disrupting this warfighting function is the awareness of ideas likely to be used in enemy propaganda such as the operational inefficiency of 155 mm self-propelled howitzer systems, their effortless destruction or the wrongful use of such systems by friendly forces in a manner inconsistent with the laws of war, the rules of international humanitarian law or as intended by false flag operations - carried out by the enemy with 155 mm NATO standard munitions. Awareness of these ideas at the force structures level will facilitate their counteraction or even exploitation within the friendly *information operations* warfighting function.

Sustainment

The contribution of 155 mm self-propelled howitzer systems to *sustainment* warfighting function is primarily to protect logistic support forces and resource flows by countering enemy fire support systems. As mentioned above, the increased mobility of self-propelled howitzers (especially in *shoot and scoot*), the high firepower accurately applied to considerable distant targets, the existence of automated fire control systems, as well as modern enemy artillery detection capabilities (included in the same armament program or already existing at the national level), will allow these systems to be used effectively in executing counter-battery fire in order to prohibit striking of friendly logistic system elements or the disruption of all type resource flows.

Sustainability is also ensured by the fact that, as mentioned in the SWOT analysis, the new 155 mm self-propelled howitzer systems will be produced locally, thus

making it possible to maintain their operational status through a purely national effort. This aspect is very important and it could be observed also in the Ukrainian conflict where the possibility of continuous supply of sub-assemblies or various components made the M109 self-propelled howitzers active and exploited in combat while other similar more modern systems (PZH 2000 and Caesar) suffered from certain shortcomings in maintaining their operational status (Hooper 2023).

From another perspective, given that fire support systems are generally very resource-intensive, especially due to heavy and bulky ammunition, the ease in supply (resupply) for these systems is beneficial for the entire logistic system of force structures. Hence a number of contributions of the new 155 mm self-propelled howitzer systems regarding sustainability, consisting of aspects such as:

- automated (robotized) ammunition replenishment thanks to the K10 systems included in the equipping program (Global Defense News 2024a);
- use of 155 mm NATO standard ammunition, including guided or with submunitions, leading to potentially higher target engagement efficiency;
- the ability to execute Multiple Rounds of Simultaneous Impact (MRSI) fire missions, which can improve the operational effectiveness of the systems in certain situations.

These contributions to the use and resupply of 155 mm munitions facilitate the exercise of sustainable warfighting function and, as mentioned above, have the potential to influence the rhythm and intensity of action in both self-propelled howitzer systems and the manoeuvre forces they will provide fire support for.

In terms of disrupting the enemy's *sustainment* warfighting function, the main contribution of 155 mm self-propelled howitzer systems consists of "pushing" sources of supply and concentrations of resources of all types to greater distances from the contact area of operations. Equipping friendly force structures with such systems will determine the enemy to deploy certain elements of logistic support beyond the howitzer's range or, alternatively, to take more risks in securing the continued sustainability of enemy forces in the contact area of operations.

Conclusions

The operational framework described by the warfighting functions is usually used as a tool at the commander's disposal to fully address the characteristic aspects of an operation. Through warfighting functions, it is possible to visualize how the available capabilities of the force structures can be leveraged to meet operational requirements. At the same time, the warfighting functions can be exploited to identify and substantiate new force structure requirements for the accomplishment of the assigned mission under the specific conditions of modern confrontations.

The usefulness of this tool is also underlined by the fact that it is also applicable in analyzing the capabilities available to a potential enemy or the capabilities existent on other actors of interest in the area of operations. This aspect allows commanders

and staff to better understand the confrontation environment and will make it easier to determine the centres of gravity for their own forces, enemy forces or any other actor of interest present in the area of operations.

The ways of performing warfighting functions in an operation describe the capabilities available to the force and, moreover, facilitate an understanding of their full potential that can be leveraged to accomplish the mission. The perspective on the contribution of 155 mm self-propelled howitzer systems presented in this paper comes as an exploration of their potential to assist the warfighting functions of friendly forces while also considering the potential of these systems to disrupt the same functions regarding enemy forces. In the analysis, I considered the 155 mm self-propelled howitzer system as a platform to use the full range of 155 mm NATO standard munitions, without limiting myself to those types of ammunition included in the current contract with the systems manufacturer. I have thus presented some arguments on the usefulness of exploring the full potential of these capabilities when coupled with modern reconnaissance systems to the extent possible and employing high-performance munitions – precision munitions such as the M982Excalibur, long-range RAP or DPICM type with submunitions.

References

Altman, Howard. 2023. "Ukraine Situation Report: M109 Paladins Are Proving Too Wily For Russian Gunners." https://www.twz.com/ukraine-situation-report-m109-paladins-are-proving-too-wily-for-russian-gunners.

Curtifan, Tudor. 2024a. „Offsetul pentru obuziere: K9 Tunetul va fi produs în colaborare cu industria din România. Dar într-o fabrică ridicată de la zero." https://www.defenseromania.ro/offsetul-pentru-obuziere-k9-tunetul-va-fi-produs-in-colaborare-cu-industria-din-romania-dar-intr-o-fabrica-ridicata-de-la-zero_629372.html.

—. 2024b. „România vrea o linie proprie pentru muniția de 120 mm pentru Abrams, dar și 155 mm pentru K9. Doi giganți din industrie vor să se implice." https://www.defenseromania.ro/romania-vrea-o-linie-proprie-pentru-munitia-de-120-mm-pentru-abrams-dar-si-155-mm-pentru-k9-doi-giganti-din-industrie-vor-sa-se-implice_629441.html.

Department of the Army. 2022. *FM 3-0 Operations.* USA: Department of the Army.

European Security & Defence. 2022. "*Hanwha Defense & UK Team Thunder – The Future of Mobile Fires.*" https://euro-sd.com/2022/09/sponsored-content/27272/hanwha-defense-uk-team-thunder-the-future-of-mobile-fires/.

Global Defense News. 2024a. "Former US generals see Hanwha's K9 howitzer and K10 resupply vehicle as key assets for US Army modernization." https://armyrecognition.com/news/army-news/army-news-2024/former-us-generals-see-hanwhas-k9-howitzer-and-k10-resupply-vehicle-as-key-assets-for-us-army-modernization.

—. 2024b. "K9 Thunder." https://armyrecognition.com/military-products/army/artillery-vehicles-and-weapons/self-propelled-howitzers/k9-thunder-south-korea-uk#google_vignette.

Hooper, Craig. 2023. "New Ukraine Howitzers Make Headlines, While The M-109 Gun Toils In Obscurity." https://www.forbes.com/sites/craighooper/2023/01/03/new-ukraine-howitzers-make-headlines-while-the-m-109-gun-toils-in-obscurity/.

Kosoy, Daniel. 2024. "HIMARS, Ukraine's Original Game Changer." https://united24media.com/war-in-ukraine/himars-ukraines-original-game-changer-1613.

Ministerul Apărării Naționale. 2024. „Direcția Generală pentru Armamente." https://www.dpa.ro/programe-de-inzestrare/.

Namuwiki. 2024. "K-9 self-propelled howitzer/operating bureau." https://en.namu.wiki/w/K-9%20%EC%9E%90%EC%A3%BC%EA%B3%A1%EC%82%AC%ED%8F%AC/%EC%9A%B4%EC%9A%A9%EA%B5%AD.

NATO. 2016. *Allied Joint Doctrine for Land Operations AJP-3.2.* NATO Standardization Office.

—. 2019. *Allied Joint Doctrine for the Conduct of Operations AJP-3.* NATO: NATO Standardisation Office.

—. 2022. *Allied Joint Doctrine AJP-01.* NATO: NATO Standardisation Office.

Newsweek. 2024. "Strikes on Ukraine's Most Prized Assets Raise Alarm." https://www.newsweek.com/ukraine-russia-strikes-helicopters-abrams-bradleys-1879148.

Okoko, Janet Mola, Scott Tunison, and Keith D. Walker. 2023. *Varieties of Qualitative Research Methods.* Saskatoon, Saskatoon: Springer Texts in Education.

Orjanu, Gheorghiță. 2023. „HIMARS deschide uși. Artileria Armatei României a intrat în «clubul select» ASCA. SUA – rol cheie în primirea României în ASCA." https://www.defenseromania.ro/himars-deschide-usi-artileria-armatei-romaniei-a-intrat-in-clubul-select-asca-sua-rol-cheie-in-primirea-romaniei-in-asca_622036.html.

—. 2024. „Reușită remarcabilă a obuzierelor K9 care vor intra și în dotarea României: Lovitură chirurgicală cu un proiectil sofisticat american Excalibur (Video)." https://www.defenseromania.ro/reusita-remarcabila-a-obuzierelor-k9-care-vor-ajunge-si-in-dotarea-romaniei-lovitura-chirurgicala-cu-un-proiectil-sofisticat-american-excalibur-video_629615.html.

SMFT. 2017. *Doctrina operațiilor forțelor terestre F.T.-1.* București: SMFT.

SMG. 2011. *Doctrina Armatei României SMG-103.* București: Ministerul Apărării Naționale.

—. 2014. *Doctrina pentru operații întrunite a Armatei României SMG/ PF-3.* București: Ministerul Apărării Naționale.

Soare, Andreea. 2024. „Monitorul Apărării și Securității." https://monitorulapararii.ro/romania-a-semnat-contractul-pentru-obuzierele-autopropulsate-k9-tunet-1-55050.

Technology.org. 2024. "Ukraine is very happy with the Krab howitzer, but it does have a weakness." https://www.technology.org/2024/05/09/ukraine-is-very-happy-with-the-krab-howitzer-but-it-does-have-a-weakness/.

Toroi, George-Ion. 2024. "A theoretical analysis of the art of deception." *Strategic Impact* 25-47.

Ukrinform. 2024. "Poland to sell 60 Krab self-propelled howitzers to Ukraine." https://www.ukrinform.net/rubric-ato/3497984-poland-to-sell-60-krab-selfpropelled-howitzers-to-ukraine.html.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

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
e-mail: faiz@kdu.ac.lk

Abstract

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 prioritising 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.

Keywords:
Food security; national security; Saudi Arabia; Gulf region.

Article info
Received: 12 December 2024; Revised: 10 February 2025; Accepted: 28 February 2025; Available online: 2 April 2025

Citation: Al Harbi, B., and F. MMT Marikar. 2025. "Food security and its impact on Saudi Arabia's national security and gulf security". *Bulletin of "Carol I" National Defence University*, 14(1): 184-198. https://doi.org/10.53477/2284-9378-25-12

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 and Hashim 2017). Food insecurity in the region can profoundly affect national and regional security, leading to economic instability, social discontent, and political turmoil (Haque and 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 destabilise the area. Saudi Arabia, as a member of the GCC, has been actively involved in addressing these concerns (Hameed, Quamar and Kumaraswamy 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 radicalisation, 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.

This research aims 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.

https://doi.org/10.53477/2284-9378-25-12

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.

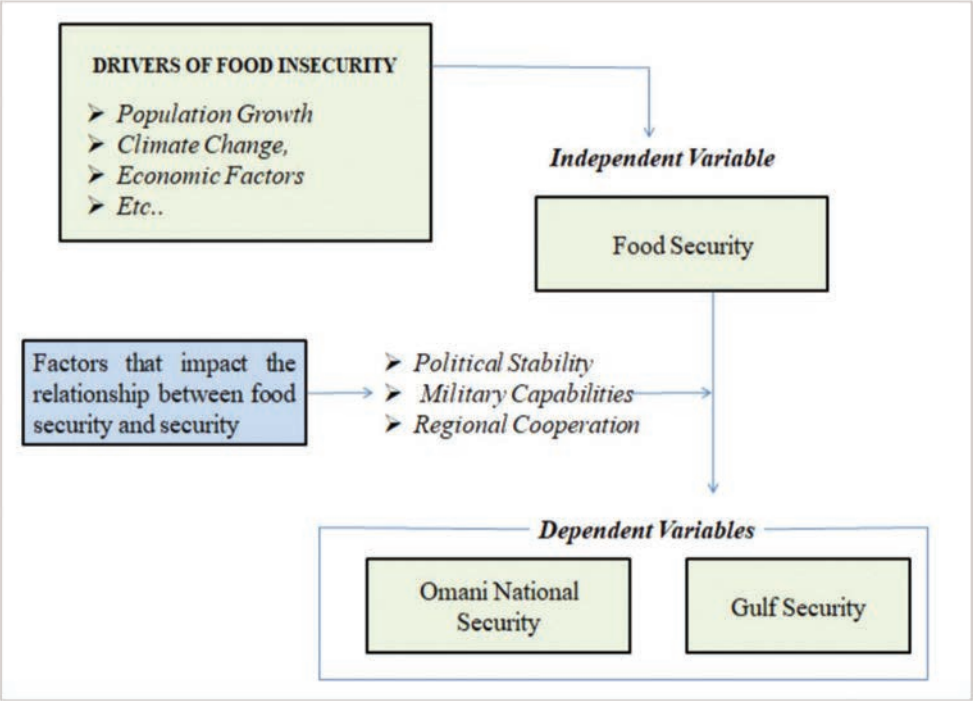


Figure 1 Conceptual Framework (Souce: Author's own work)

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.

This study investigates the complex relationship between food security and national security in Saudi Arabia, with implications for the broader Gulf region. The primary goal is to assess the potential threats to Saudi Arabia's security stemming from food insecurity and to explore strategies to mitigate these risks. Key challenges encountered in this research include the scarcity and inconsistency of relevant data,

the interdisciplinary nature of the topic, the rapidly evolving geopolitical landscape, and ethical considerations. To overcome these challenges, a comprehensive literature review, data triangulation, expert interviews, case study analysis, and statistical analysis were employed. The overarching purpose of this study is to enhance understanding of the food security- national security nexus, identify vulnerabilities, evaluate policy responses, propose recommendations, and inform decision-making for a more secure and sustainable future in Saudi Arabia and the Gulf region.

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 for this study will be obtained from a variety of credible sources, including government reports, academic journals, and research publications. Government reports will provide official statistics and insights into national policies, food security strategies, and relevant socio-economic factors affecting food security in the region. Academic journals and research papers will contribute to a deeper understanding of existing literature on food security, including findings from studies conducted in similar contexts. These sources will offer valuable data on food security patterns, challenges, and responses in the Gulf region and neighbouring countries. Additionally, international organizations and agencies, such as the World Food Programme (WFP) and the Food and Agriculture Organization (FAO), will serve as reliable secondary data sources to assess global trends and best practices in addressing food insecurity.

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 analysed 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.

Evaluating Success and Target Audience

The target audience for this study encompasses a diverse group, including policymakers, government officials, researchers, academics, international organizations, private sector entities, and civil society organizations. To evaluate the success of the activities, several key metrics can be employed. These include the

rigor of methodology and data analysis, the originality of insights, peer review and publication in reputable journals, the adoption of research findings by policymakers, the implementation of evidence-based policies, improvements in food security indicators, the dissemination of research findings through various channels, public awareness and engagement, and international collaboration. By assessing these factors, the overall impact of the study and its contribution to addressing food security and national security challenges can be effectively evaluated.

Results and Discussion

Food Security Categories

Chronic and Transient Food Insecurity in Gulf Countries:
Food security in the Gulf region, including Saudi Arabia, is a multifaceted issue that encompasses chronic and transient food insecurity. Chronic food insecurity refers to long-term, persistent food shortages, often caused by structural issues such as poverty, lack of local agricultural capacity, and economic inequality. In Gulf countries like Saudi Arabia, chronic food insecurity is not widespread but can still affect marginalized populations, particularly lower-income groups. These communities are vulnerable to global market fluctuations and economic shocks, which can affect their ability to access sufficient and nutritious food. Although the governments in the Gulf region have implemented social safety nets and subsidies to mitigate the effects of chronic food insecurity, this problem persists for certain segments of the population who face barriers such as high food costs and limited access to nutritious options. Furthermore, the reliance on food imports makes these nations susceptible to fluctuations in global food prices, which can exacerbate food insecurity for the vulnerable.

On the other hand, transient food insecurity is often temporary and caused by short-term disruptions. This may be due to factors like natural disasters, geopolitical instability, or sudden spikes in global food prices. In Saudi Arabia, transient food insecurity can occur when international trade disruptions affect the country's food supply or when extreme weather events (such as flooding) affect local production. These short-term food security challenges are often managed through emergency relief programs, including food aid and subsidies. However, they highlight the vulnerability of Gulf nations to global food supply chains and the importance of diversifying food sources and developing resilient domestic production systems.

Food Security in Neighbouring Countries:
When examining food security in neighbouring countries in the Middle East and South Asia, the situation varies widely due to differences in local agricultural practices, economic structures, and political stability.
United Arab Emirates (UAE): The UAE faces similar food security challenges to Saudi

Arabia. It is highly reliant on food imports to meet the needs of its population, as it has limited arable land and water resources. The UAE's food security is generally categorized as relative, as the country ensures access to food through strategic imports, but it remains vulnerable to fluctuations in global supply chains. Chronic food insecurity is not widespread, but transient food insecurity could arise in times of crisis, such as the COVID-19 pandemic, when global food supply chains were disrupted. The UAE has responded by investing in innovative agricultural technologies, such as vertical farming and hydroponics, to improve food production domestically.

Oman: Oman faces both chronic and transient food insecurity challenges. While the country does not experience widespread chronic food insecurity, lower-income groups in rural areas may struggle to access sufficient food due to limited infrastructure and high food prices. Transient food insecurity in Oman can occur due to temporary disruptions, such as seasonal price hikes or natural disasters like cyclones, which affect local food production. However, Oman has made strides in improving its food security by implementing policies aimed at diversifying food sources and investing in agricultural research.

Yemen: Yemen faces extreme levels of chronic food insecurity. A combination of conflict, economic instability, and poor agricultural infrastructure has led to widespread food shortages and severe malnutrition. The country relies heavily on food imports, but ongoing conflict has disrupted supply chains, exacerbating the problem. Yemen has one of the highest rates of food insecurity in the Middle East, with millions of people unable to meet their daily food requirements. Humanitarian aid plays a critical role in addressing food insecurity in Yemen, though the situation remains dire and long-term solutions are needed to stabilize the country's food systems.

Kuwait: Similar to its Gulf neighbours, Kuwait is heavily dependent on food imports due to its arid climate and lack of agricultural resources. Chronic food insecurity is not a significant issue, but there are concerns about transient food insecurity during periods of economic downturn or global price hikes. Kuwait has implemented measures to enhance food security, such as establishing food reserves and promoting research into sustainable agricultural practices, but it remains vulnerable to fluctuations in the international food market.

Iran: Iran experiences a mix of chronic and transient food insecurity. Chronic food insecurity is prevalent in rural areas, where poverty, limited access to land, and agricultural inefficiency affect food access. The country's reliance on domestic production and its challenges in importing food due to international sanctions have led to instability in food availability and access. Transient food insecurity in Iran is also a concern, particularly during times of economic sanctions or geopolitical tensions, which disrupt supply chains and inflate food prices. Iran has made efforts

to increase domestic food production, but these challenges continue to affect food security in the country.

Overall, the food security situation in the Gulf and its neighbouring countries highlights the complexities of managing food availability, access, and stability in a region that faces both chronic and transient food insecurity. While Gulf countries like Saudi Arabia and the UAE are generally able to maintain relative food security through imports and strategic policies, they remain vulnerable to global food market fluctuations and short-term disruptions. In contrast, countries like Yemen face more severe challenges, with widespread chronic food insecurity driven by conflict and economic instability. Efforts to improve food security in the region will require a combination of short-term solutions, such as food aid and subsidies, as well as long-term strategies focused on sustainable agricultural practices, diversification of food sources, and enhanced resilience to global disruptions.

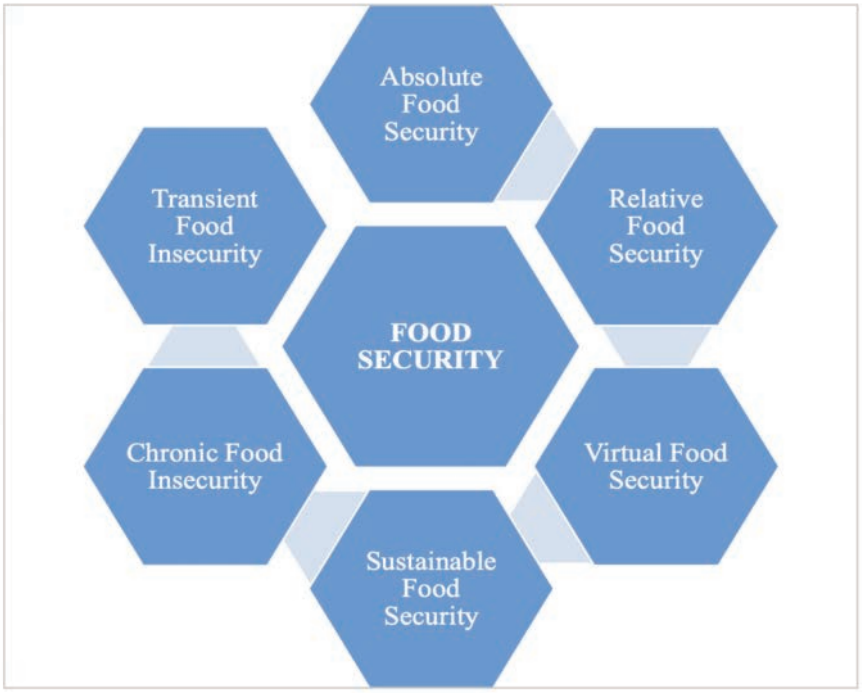


Figure 2 Food Security Categories Diagram (Souce: Author's own work)

Absolute Food Security in the Gulf and Saudi Arabia: Absolute food security in the context of the Gulf countries, including Saudi Arabia, would mean that these nations could meet their food demand entirely through domestic production, without relying on imports. However, this is a challenging goal given the harsh desert climate, limited arable land, and water scarcity in the region. Despite this, there have been efforts to increase agricultural production, particularly through the use of advanced technology such as hydroponics, desalinated water for irrigation, and investment in agricultural innovation. Saudi Arabia, in particular, has been exploring sustainable farming practices to boost local food production, but achieving absolute self-sufficiency remains an aspiration rather than a reality.

Relative Food Security in the Gulf and Saudi Arabia: Saudi Arabia, and the Gulf region more broadly, falls under the category of relative food security. These countries do not rely solely on domestic food production but have systems in place to ensure regular food access, often through strategic imports. Saudi Arabia imports a significant portion of its food, especially staples like grains, meat, and vegetables. The government has developed policies and established partnerships with countries around the world to secure reliable and diverse sources of food. Through strategic investments in agricultural projects abroad and partnerships with global food suppliers, Saudi Arabia maintains a steady food supply and ensures that its population has access to adequate food.

Apparent or Virtual Food Security in the Gulf and Saudi Arabia: While Saudi Arabia may appear to have robust food security, producing a significant amount of some food items, such as wheat or dates, much of the agricultural input comes from imports. For example, Saudi Arabia imports the majority of its fertilizers, seeds, and technology for crop production. In the case of wheat, although Saudi Arabia once produced a substantial portion of its wheat, it has reduced domestic production in favour of importing it due to water scarcity and other environmental constraints. As a result, while domestic production figures may look positive, the country is still heavily reliant on external resources, which means its food security could be vulnerable in the event of global supply chain disruptions.

Sustainable Food Security in the Gulf and Saudi Arabia: Saudi Arabia has recognized the importance of sustainable food security and has started focusing on long-term strategies to enhance agricultural productivity while preserving natural resources. For instance, the country is investing in water-efficient technologies like drip irrigation and desalination, as well as improving soil management practices. Moreover, there is an emphasis on increasing the sustainability of food production systems by supporting the development of aquaculture, greenhouse farming, and vertical farming. Saudi Arabia's Vision 2030 plan highlights sustainable agriculture as a key component in reducing dependence on food imports and improving food security for future generations.

Chronic Food Insecurity in the Gulf and Saudi Arabia: Although Saudi Arabia is generally considered to have adequate food security, chronic food insecurity can still affect certain vulnerable populations, particularly those who are economically disadvantaged or live in rural areas. Due to the country's reliance on imports and the fluctuating prices in global markets, some segments of the population may struggle with consistent access to food. Chronic food insecurity in Saudi Arabia is not widespread, but it is a concern for lower-income groups who are affected by global economic factors, such as rising food prices or regional conflicts that may disrupt supply chains.

Transient Food Insecurity in the Gulf and Saudi Arabia: Transient food insecurity is more likely to occur in Saudi Arabia and other Gulf countries due to short-term

events like fluctuations in global food prices, natural disasters (such as flooding), or temporary disruptions in the food supply chain. For instance, disruptions in food imports due to global crises, such as the COVID-19 pandemic or geopolitical tensions, may temporarily cause shortages or price hikes, affecting the availability and accessibility of food. In such cases, emergency measures like food aid or government subsidies can help mitigate the short-term effects and restore stability.

Dimensions of Food Security in Gulf and Saudi Arabia: In the Gulf region, food security is heavily influenced by the dimensions of availability (access to sufficient food through imports and local production), access (economic and physical access to food despite reliance on imports), utilization (the nutritional value and safety of food), and stability (ensuring consistent food access despite external factors like price volatility or geopolitical instability). Saudi Arabia, for example, has invested in international food security partnerships and technologies to improve food availability and ensure that food meets the nutritional needs of its population. Furthermore, the government focuses on stabilizing food prices and creating mechanisms to address potential disruptions in the food supply, ensuring that citizens have access to food consistently.

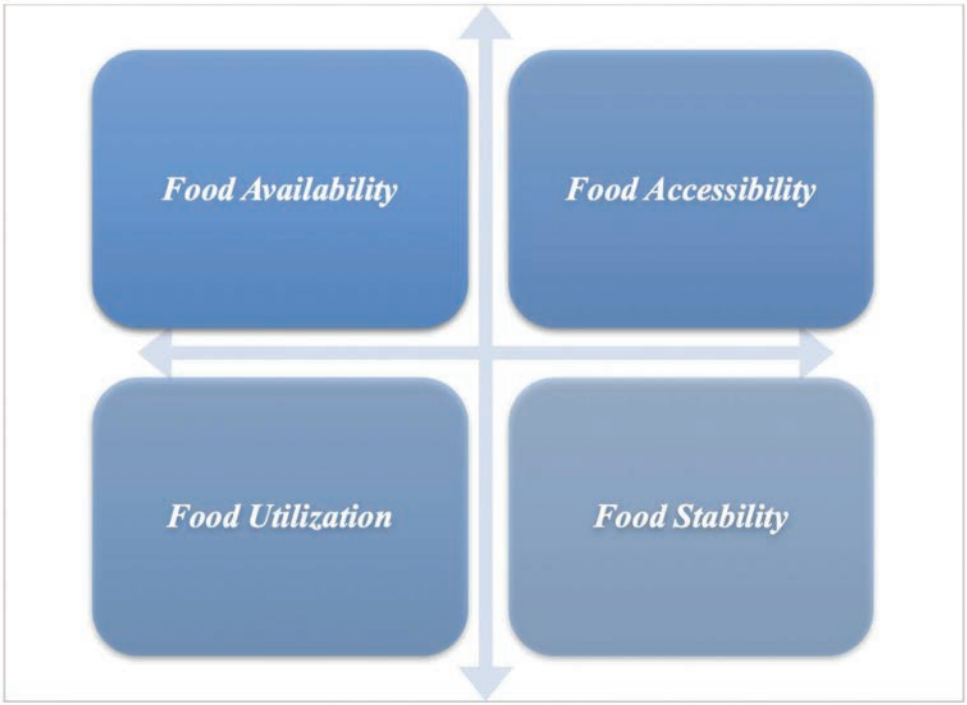


Figure 3 Dimensions of Food Security diagram (Souce: Author's own work)

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 and 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, which is 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, which is 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.

This study indicates 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.

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.

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.

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.

Research Limitations

During the conducting of this thesis and 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.

Assessing Goal Achievement

The success of the study's goals can be evaluated by assessing the quality and sufficiency of data collection and analysis, the impact of research findings on policy decisions, the effectiveness in raising public awareness, the contribution to academic discourse through publications and citations, and the strength of international collaborations.

Future Plans

Building upon the initial research, future plans may involve in-depth exploration of specific subtopics, active engagement with policymakers to advocate for evidence-based policies, capacity-building initiatives for stakeholders, strengthening international collaborations, and establishing a robust monitoring and evaluation system to track the impact of implemented policies and strategies.

References

Al Naimi, S.M. 2022. "Economic diversification trends in the Gulf: The case of Saudi Arabia." *Circular Economy and Sustainability* vol. 2: pp.221-230. https://doi.org/10.1007/s43615-021-00106-0.

Albejaidi, F., and K.S. Nair. 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. https://doi.org/10.1177/0972063421103520.

Alderiny, M.M., K.N. Alrwis, S.B. Ahmed, and N.M. Aldawdahi. 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. https://doi.org/10.1016/j.jssas.2019.09.001.

Alharbi, A.S., G. Halikias, M. Rajarajan, and M. Yamin. 2021. "A review of effectiveness of Saudi E-government data security management." *International Journal of Information Technology* 13: pp.573-579. https://doi.org/10.1007/s41870-021-00611-3.

Al-Khateeb, S.A., A. Hussain, S. Lange, M.M. Almutari, and F. Schneider. 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. https://doi.org/10.3390/su13158402.

Alrobaish, W.S., P. Vlerick, P.A. Luning, and L. Jacxsens. 2021. "Food safety governance in Saudi Arabia: Challenges in control of imported food." *Journal of Food Science* 86 (1): pp. 16-30. https://doi.org/10.1111/1750-3841.15552.

Alrwis, K.N., A.M. Ghanem, O.S. Alnashwan, A.A.M. Al Duwais, S.A.B. Alaagib, and N.M. Aldawdahi. 2021. "Measuring the impact of water scarcity on agricultural economic development in Saudi Arabia." *Saudi Journal of Biological Sciences* 28 (1): pp.191-195. https://doi.org/10.1016/j.sjbs.2020.09.038.

Ayad, A.A., N.M. Abdulsalam, N.A. Khateeb, M.A. Hijazi, and L.L. Williams. 2022. "Saudi Arabia household awareness and knowledge of food safety." *Foods* 11 (7): p. 935. https://doi.org/10.3390/foods11070935.

Bin Sunaid, F.F., A. Al-Jawaldeh, M.W. Almutairi, R.A. Alobaid, T.M. Alfuraih, F.N. Bensaidan, A.S. Alragea, et al. 2021. "Saudi Arabia's healthy food strategy: Progress & hurdles in the 2030 road." *Nutrients* 13 (7): p. 2130. https://doi.org/10.3390/nu13072130.

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

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

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

Haque, M.I., and M.R. Khan. 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. https://doi.org/10.1108/JADEE-06-2020-0127.

Lambert, L.A., and H.B. Hashim. 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.

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


AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2021-2026
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2021-2026

BIROUL EXECUTIV AL CONSILIULUI ARACIS


Institutional Evaluation Programme
Performance in Research, Performance in Teaching – Quality, Diversity and Innovation in Romanian Universities Project

"CAROL I - NATIONAL DEFENCE UNIVERSITY"
BUCHAREST-ROMANIA

EDITOR
„Carol I" National Defence University Publishing House
(Publishing house with recognized prestige validated by the National Council for Attestation of University Degrees, Diplomas and Certificates)
Adress: Panduri Street, no. 68-72, Bucharest, 5th District
e-mail: buletinul@unap.ro
Phone: +4021.319.48.80 / 0365; 0453

Signature for the press: 02.04.2025
The publication consists of 200 pages.

223/02.04.2025

C.80/2025