"CAROL I" NATIONAL DEFENCE UNIVERSITY
Centre for Defence and Security Strategic Studies
&
Interdisciplinary Doctoral School

PROCEEDINGS

STRATEGIES XXI
INTERNATIONAL SCIENTIFIC CONFERENCE

THE COMPLEX AND DYNAMIC NATURE OF THE SECURITY ENVIRONMENT

22nd Edition

EDITORS:
Florian CÎRCIUMARU, PhD
Alexandra SARCINSCHI, PhD

"CAROL I" NATIONAL DEFENCE UNIVERSITRY PUBLISHING HOUSE
BUCHAREST, ROMANIA
February, 26, 2026

INTERNATIONAL SCIENTIFIC COMMITTEE:

Eugen MAVRIȘ, PhD, Commandant (Rector),
"Carol I" National Defence University, Romania
Dan-Lucian PETRESCU, PhD, Deputy Commander,
"Carol I" National Defence University, Romania
Cristian STANCIU, PhD, Prof., Vice-Rector for Education,
"Carol I" National Defence University, Romania
Ștefan-Antonio DAN-ȘUTEU, PhD, Assoc. Prof., Vice-Rector for Scientific Research and Interinstitutional Relations,
"Carol I" National Defence University, Romania
Lucian SCIPANOV, PhD, Prof., President of the Senate,
"Carol I" National Defence University, Romania
Adi MUSTAȚĂ, PhD, Prof., Director of Doctoral School,
"Carol I" National Defence University, Romania
Florian CÎRCIUMARU, PhD, Director, Centre for Defence and Security Strategic Studies, "Carol I" National Defence University, Romania
Marius ȘERBESZKI, PhD, Assoc. Prof., Commandant (Rector), "Henri Coandă" Air Forces Academy, Romania
Toma ALECU, PhD, Assoc. Prof., Superintendent (Rector), "Mircea cel Bătrân" Navy Academy, Romania
Constantin VIZITIU, PhD, Prof. Eng., Commandant (Rector),
"Ferdinand I" Military Technical Academy, Romania
Alan STOLBERG, PhD, RAND Corporation, USA
Timothy DREIFKE, PhD, PfP Consortium, USA
John F. TROXELL, PhD, Visiting Researcher, Army War College, USA
Robert ANTIS, PhD, Prof. Emeritus, Joint Forces Staff College, National Defence University, USA
Pavel ANASTASOV, Operations Division, NATO IS, Belgium
Mariusz SOLIS, Operations Division, NATO HQ, Belgium
Gábor BOLDIZSÁR, PhD, Assoc. Prof., National University of Public Service, Hungary
Péter TÁLAS, PhD, Assoc. Prof., John Lukacs Institute for Strategy and Politics, Hungary
Tamás CSIKI VARGA, PhD, Senior Research Fellow, Institute for Strategic and Defence Studies, National University of Public Service, Hungary
János BESENYŐ, PhD, Assoc. Prof., Óbuda University, Hungary
Stanislaw ZAJAS, PhD, Prof., National Defence University, Poland
Piotr GAWLICZEK, PhD, Dr. Hab., NATO DEEP eAcademy, University of Warmia and Mazury in Olsztyn, Poland
Pavel NECAS, PhD, Prof. Dipl. Eng., Armed Forces Academy of General Milan Rastislav Štefánik, Slovakia
Josef PROCHÁZKA, PhD, Assoc. Prof., National Defence University, Czech Republic
Daniel FIOTT, PhD, Institute for European Studies, Vrije Universiteit Brussel, Belgium
Igor SOFRONESCU, PhD Assoc. Prof., Armed Forces Military Academy "Alexandru cel Bun", Republic of Moldova
Teodor FRUNZETI, PhD, Prof., "Titu Maiorescu" University, Romania
Sorin IVAN, PhD, Prof., "Titu Maiorescu" University, Romania
Florian RĂPAN, PhD, Prof., "Ferdinand I" Military Technical Academy, Romania
Ioan DEAC, PhD, Prof., "Mihai Viteazul" National Intelligence Academy, Romania
Ruxandra BULUC, PhD, Senior Researcher, "Mihai Viteazul" National Intelligence Academy, Romania
Cristina BOGZEANU, PhD, Assoc. Prof., "Mihai Viteazul" National Intelligence Academy, Romania
Alexandru MUNTEANU-LUCINESCU-CASELLA, PhD, Senior Researcher, Ministry of Defence, Romania
Dan GRECU, PhD, President of the Association of Reserve Officers from Romania
Virgil BĂLĂCEANU, PhD, Honorary President, Association of Reserve Officers from Romania
Constantin POSTOLACHE, PhD, Association of Reserve Officers from Romania
Alin BODESCU, PhD, Lect., "Nicolae Bălcescu" Land Forces Academy, Romania
Răzvan BUZATU, PhD, Security Expert, Romania
Elena MATEESCU, PhD, National Meteorological Administration, Romania
Roxana BOJARIU, PhD, National Meteorological Administration, Romania
Maria-Emanuela MIHAILOV, PhD, Development and Innovation Centre, Maritime Hydrographic Directorate, Romania
Stan ANTON, PhD, Visiting Assist. Prof.,
"Carol I" National Defence University, Romania
Cezar VASILESCU, PhD, Prof. Eng., RDDRMS,
"Carol I" National Defence University, Romania
Maria CONSTANTINESCU, PhD, Assoc. Prof., RDDRMS,
"Carol I" National Defence University, Romania
Niculai-Tudorel LEHACI, PhD, Prof.,
"Carol I" National Defence University, Romania
Cristian ICHIMESCU, PhD, Assoc. Prof.,
"Carol I" National Defence University, Romania
Marius-Valeriu PĂUNESCU, PhD, Assoc. Prof.,
"Carol I" National Defence University, Romania
Iulian CHIFU, PhD, Prof.,
"Carol I" National Defence University, Romania
Alba Iulia Catrinel POPESCU, PhD, Assoc. Prof.,
"Carol I" National Defence University, Romania
Dănuț TURCU, PhD, Prof.,
"Carol I" National Defence University, Romania
Elena ȘUȘNEA, PhD, Assoc. Prof.,
"Carol I" National Defence University, Romania
Veronica PĂSTAE, PhD, Assoc. Prof.,
"Carol I" National Defence University, Romania
Adrian MIREA, PhD, Assoc. Prof.,
"Carol I" National Defence University, Romania
Mirela ATANASIU, PhD, Senior Researcher,
"Carol I" National Defence University, Romania
Cristian BĂHNĂREANU, PhD, Senior Researcher,
"Carol I" National Defence University, Romania
Crăișor-Constantin IONIȚĂ, PhD, Researcher,
"Carol I" National Defence University, Romania
Daniela LICĂ, PhD, Researcher,
"Carol I" National Defence University, Romania
Mihai ZODIAN, PhD, Researcher,
"Carol I" National Defence University, Romania

ISSN print: 2668-6511; ISSN on-line: 3045-2309; ISSN L: 3045-2309

CONTENTS

SECTION I
CONTEMPORARY WARFARE AND INTERNATIONAL SECURITY

THE EFFECTIVENESS OF INFRASTRUCTURE DESTRUCTION IN THE RUSSIAN-UKRAINIAN WAR AND ITS IMPACT ON STRATEGIC DECISION-MAKING 9
Artsrun HOVHANNISYAN, PhD

NUCLEAR DIPLOMACY IN THE CONTEXT OF THE RUSSO-UKRAINIAN WAR 19
Mihai ZODIAN, PhD

FROM POST–COLD WAR INTERDEPENDENCE TO STRATEGIC DECOUPLING: REDUCING THE EU'S DEPENDENCE ON ENERGY RESOURCES FROM THE RUSSIAN FEDERATION (2022-2025) 26
Aurel LAZĂR, PhD

PROMOTING STRATEGIC THINKING AND ITS CONTRIBUTION TO STRENGTHENING REGIONAL SECURITY 38
Lucian Valeriu SCIPANOV, PhD
Bogdan Daniel IOSIF

COGNITIVE RESILIENCE AS A STRATEGIC ASSET IN CONTEMPORARY WARFARE: THEORETICAL FOUNDATIONS AND SECURITY IMPLICATIONS 48
Ruslana GROSU, PhD
Cătălin-Victor POPESCU

SHAPING MINDS FOR SECURITY: COGNITIVE RESILIENCE AND THE STRATEGIC ROLE OF UNIVERSITY EDUCATION IN ROMANIA 62
Raluca LUȚAI, PhD
Marius GRAD, PhD

SECTION II
STATE AND NONSTATE ACTORS IN POWER RELATIONS

MANUFACTURING THREAT AND FRIENDSHIP: NORTH KOREAN STATE MEDIA AND THE EMERGENCE OF A STRATEGIC PARTNERSHIP WITH RUSSIA 79
Jana CHAMROVA

STRATEGIC BALANCING IN TRANSITION: REASSESSING
ARMENIA'S FOREIGN AND SECURITY POLICY PARADIGM 89
Rafik AVETISYAN, PhD
Tigran KOCHARYAN, PhD

THE BLACK SEA REGION IN THE CONTEXT OF FOUR YEARS
OF WAR IN UKRAINE. THE GAME OF CHESS BETWEEN
NATO, EU, RUSSIA, AND OTHER RELEVANT ACTORS 99
Daniela LICĂ, PhD
Ana-Maria FLOREA

ROMANIA'S NATIONAL SECURITY BETWEEN THE STRATEGIC
PARTNERSHIP WITH THE USA AND THE EU STRATEGIC AGENDA 114
Sînziana IANCU, PhD

VOLUNTARY RESERVE AS AN INSTRUMENT FOR SOCIAL
COHESION AND EXTENDED NATIONAL RESILIENCE
IN THE BLACK SEA REGION 121
Elena-Adriana BRUMARU

SECTION III
GLOBAL AND REGIONAL TRENDS

THE IMPACT OF AN ARMED CONFLICT ON CHILDREN 129
Marius Gabriel BOBOCEA

SMART INFRASTRUCTURE, SMART DEFENCE: DIGITAL TWINS
AND PREDICTIVE MONITORING FOR RESILIENCE 136
Maria Niamh BRATCOVICI

SECURING THE BLACK BOX: A TECHNO-DIPLOMATIC FRAMEWORK
FOR AI INTEGRATION IN MODERN DEFENSE ALLIANCES 144
Dumitru-Cătălin VASILE

TWO PARADIGMS OF ALGORITHMIC SECURITY GOVERNANCE:
CENTRALISED INTEGRATION AND INTEROPERABLE FRAMEWORKS
IN THE USE OF AI FOR STATE SECURITY 154
Mara-Mihaela MEREANU

THE RISE OF NAVAL DRONES AND THE REDEFINITION
OF THE MARITIME BATTLESPACE 160
Adrian NIȚĂ

INDEX OF AUTHORS 173

SECTION I
CONTEMPORARY WARFARE AND INTERNATIONAL SECURITY

DOI: 10.53477/3045-2309-26-01

THE EFFECTIVENESS OF INFRASTRUCTURE DESTRUCTION IN THE RUSSIAN-UKRAINIAN WAR AND ITS IMPACT ON STRATEGIC DECISION-MAKING

Artsrun HOVHANNISYAN, PhD,
Colonel, Associate Professor RA MOD,
Head of the Command and Staff Institute after Vazgen Sargsyan, Republic of Armenia,
E-mail address: arcrunhovhannisyan@gmail.com

Abstract*: The author examines one of the key innovations of the Russo-Ukrainian war – the launching of massive airstrikes – in an attempt to determine the impact of damage to territorial infrastructure on state strategies and the future of warfare. The ratio of modern airstrikes to their deployment is determined primarily by economic considerations.*

Although the Ukrainian strikes were carried out using relatively inexpensive systems - primarily unmanned aerial vehicles – they reached even the most remote Russian bases and oil terminals, causing colossal damage to the Russian economy.

Small drones, supported by artificial intelligence, are deployed in large numbers before the strike, creating a distributed air presence.

This approach to sequential countermeasures is expected to become more widespread in the future, as it represents one of the most effective ways to maintain air superiority.

Based on an analysis of data from various sources, a number of conclusions are drawn, arguing that the West as a whole continues to fund Ukraine – perhaps not fully, but nevertheless sufficiently and sustainably.

Keywords*: air supremacy; drone warfare; mass strike operations; military decision-making; combined strike operations; sixth generation warfare.*

Introduction

The Russian–Ukrainian war has entered its fourth year, during which multiple operational domains have emerged alongside conventional ground operations. These domains have developed into distinct strategic components of a war of attrition. As attritional ground operations have failed to achieve decisive outcomes, infrastructure-destruction operations have assumed a central role, becoming the most consequential instrument and a primary determinant of strategic success.

The present article focuses on these operations and examines their influence on strategic decision-making. In the current phase of the conflict, they have become increasingly integrated with efforts to counter the “shadow tanker fleet”, and may ultimately prove its decisive factor in shaping the outcome of the war.

1. Mutual large-scale airstrikes

The Russian military began conducting mass airstrikes at the very outset of the war; however, in the initial phase, these strikes were not conducted on a large scale and relied on a limited number of expensive cruise missiles. Over time, however, the Russian side acquired low-cost strike systems from Iran. In May 2023, Russian forces launched approximately 400 Shahed-136/131 (Geran) strike unmanned aerial vehicles, accompanied by only a very limited number of higher-end aerial strike assets.

The tempo continued to increase, and in December of the same year, 780 Shahed-136/131 (Geran) strike UAVs (RBC.UA 2024) were launched, setting a new record. These strikes, however, were neither complex nor combined in nature; beyond the use of UAVs, they did not incorporate other advanced aerial strike assets, nor were they conducted with the integration of air and space reconnaissance and command-and-control systems. On 29 November 2023, the Russian Armed Forces carried out a significant large-scale combined strike**,** launching a total of 158 aerial strike assets**,** of which approximately 40 were strike UAVs**,** while the remainder consisted predominantly of air-launched cruise missiles**.** However, this was an isolated operation in which the emphasis was placed on the employment of high-cost cruise missiles.

The numbers increased rapidly, particularly in 2025, when the scale of these strikes reached unprecedented levels. At the same time, however, strikes by Ukrainian UAVs also intensified. These strikes were conducted using relatively low-cost systems – primarily UAVs – but they reached Russia's most distant bases and oil terminals.

On the night of 8-9 July 2025, the Russian military set a new record, launching 741 aerial strike assets. Of these**,** 728 were strike or fake UAVs**,** 7 were Kh-101/Iskander-K cruise missiles**,** and 6 were aeroballistic Kh-47M2 "Kinzhal" missiles (Prishlyak 2025)**.**

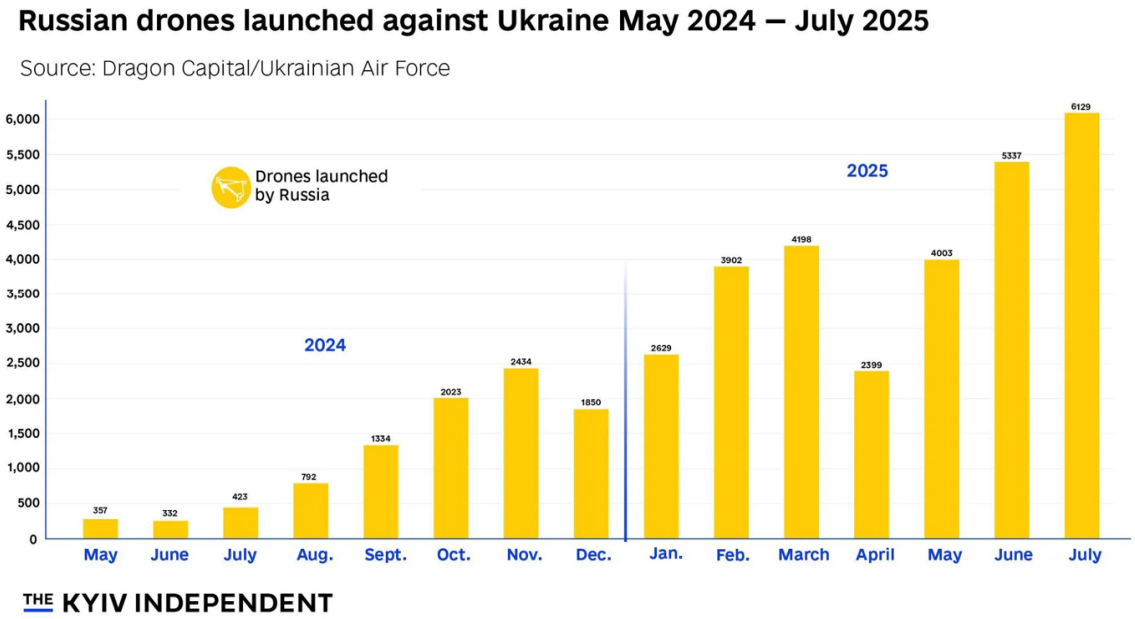

Figure no. 1: Graph illustrating Russian UAV strikes and their monthly growth

On 25 November 2025, the Russian Armed Forces launched a total of 464 UAVs and 22 missiles. Of these, 438 were UAVs**,** 1 Kh-47M2 "Kinzhal"**,** 5 Iskander-K**,** 5 Kalibr cruise missiles**,** and 3 Iskander-M ballistic missiles**.** This strike was notable for the disproportionately small number of high-value missiles compared to UAVs. On the same day, several Russian UAVs reached the airspace of Moldova and Romania**,** highlighting the extended operational reach of these systems (Shenderovskiy 2025).

On the same day, according to official Russian reports, Russian air defence forces intercepted more than 250 Ukrainian UAVs along with several missiles (1tv.ru 2025). According to Ukrainian sources, a successful strike was carried out against the Beriev Aircraft Plant in Taganrog, Russian Federation**,** where unique aircraft are produced and overhauled, including the A-50 airborne command-and-control aircraft**,** the A-60 flying laboratory (Frolov 2025)**,** Tu-95 strategic bombers and others. According to space-based intelligence data, after the strike, the A-60 flying laboratory

and the next-generation A-100 airborne command-and-control aircraft (Defense Express 2025) were set on fire on 29 November 2025, the Russian Armed Forces carried out another large-scale combined strike, during which a total of 632 aerial strike assets were launched. Of these, 596 were strike and fake UAVs, while the remaining 36 were missiles, including 5 Kh-47M2 "Kinzhal" aeroballistic missiles, 23 Kh-101/Iskander-K cruise missiles, 4 Iskander-M ballistic missiles, and 4 Kh-59/69 air-launched missiles (Girnik 2025). Once again, the Kh-47M2 "Kinzhal" proved to be the most effective aerial strike asset. This represented a rare complex and combined strike, characterised by the extensive use of high-value aerial strike systems. Monthly launch figures continued to rise steadily. In September 2025, the Russian Armed Forces launched approximately 6,900 UAVs (Mittal 2025), a pattern that persisted throughout the autumn and winter months.

Throughout 2025, Russia launched a total of 53,732 strike and fake UAVs, primarily Shahed-136/131 (Geran) systems. By comparison, in 2024, the number of such UAVs amounted to 10,849 (Shenderovskiy 2026).

At the same time, the Russian Federation produced approximately 120,000 conventional guided aerial bombs, which are employed by the air force and without which strikes against critical infrastructure targets would be largely ineffective (Hunder 2025).

Within military science, the issue of the large-scale, coordinated employment of UAVs enabled by artificial intelligence is now being actively debated, particularly in the context of the concepts known as the "UAV line" or "UAV wall." Within this conceptual framework, the "UAV wall" may comprise systems of varying types and sizes which, under a unified operational concept, can simultaneously perform different tasks.

While the notion of a "UAV wall" is currently more widely understood in the field of counter-UAS defence than in that of mass strike employment, the successful implementation of large-scale coordinated control would unequivocally enable its application across a wide range of missions.

"In military science, the issue of the large-scale, coordinated employment of UAVs through artificial intelligence is already being widely discussed, within the framework of the concepts of a «UAV line» or a «UAV wall»". "Within the concept of a «UAV wall», systems of various types and sizes may be involved, which, within a single operational design, can perform different tasks. It is true that the concept of a «UAV wall» is currently more readily understood in the field (Gardner) of counter-UAS defence than in that of their massed strike employment; however, if effective coordinated control of such large numbers is achieved, it will undoubtedly be employed for a wide range of purposes".

"During 2025, the Russian side launched a total of 1,898 missiles. Of these, 568 were ballistic and aeroballistic missiles, while 1,330 were cruise missiles and other types, mainly older surface-to-air missiles adapted for strike roles. In 2024, Russia launched 306 ballistic and aeroballistic missiles, along with 1,645 cruise missiles and other missiles (Shenderovskiy 2026).

Among cruise missile systems, the Kh-101 and Iskander-K were the most extensively employed. Over a six-month period, 451 missiles were launched, with their combined cost estimated at approximately 6.2 billion USD (Chernovol 2025).

This shows that in 2025 the use of ballistic and aeroballistic missiles increased, while the employment of cruise missiles and other missile types declined. This trend is primarily explained by the greater effectiveness of ballistic and aeroballistic missiles, whereas cruise missiles have proven less effective. Moreover, the production of cruise missiles is considerably more complex and costly.

As a result, in 2025 the total number of missiles launched by the Russian side, compared with the number of UAVs employed, amounted to an effective ratio of 1 to 28 in favor of UAVs. In 2024, this ratio was 1 to 10.

This ratio in the employment of modern aerial strike systems is primarily driven by economic considerations. The Russian Federation is simply unable to field larger numbers of aircraft with aeroballistic missiles. According to some experts, this ratio also reflects an ongoing shift in tactics. Despite being roughly ten to twenty times fewer in number, these missiles nevertheless pose

significantly greater challenges for Ukrainian air defence (Mittal 2025). Particularly that these missiles continue to be upgraded, becoming more intelligent and more accurate, thereby reducing the effectiveness of Ukrainian air defence from 37 percent to 6 percent (Financial Times 2025).

The table illustrates the launch dynamics of different missile types during Russian mass strike operations (Kulish 2025).

As can be seen from Table no. 1, the overall use of various Russian missiles – which are significantly more capable aerial strike systems – has declined year by year, particularly strategic cruise missiles. However, the use of certain ballistic missiles has increased, partly because they were also supplied from other countries.

This is a very significant fact and arguably the only reliable information provided by this table.

Table nr. 1: Year by Year Trends in Russian Missile Use

Year	**The total number of missiles**	**Ballistic missiles only**	**Ukrainian air defence interception rates (%)**
2022	~3000	~500	60-70%
2023	~5000	~800	70-80%
2024	~2500	~600	75-85%
2025	~1900	~600	80-90%
Year	**The total number of missiles**	**Ballistic missiles only**	**Ukrainian air defence interception rates (%)**
2022	~3000	~500	60-70%
2023	~5000	~800	70-80%
2024	~2500	~600	75-85%
2025	~1900	~600	80-90%

- Cruise missiles (such as the Kh-101, etc.) more than 4,000 units. In smaller quantities, there are also exceptional cruise missiles, such as the Kh-22.
- Ballistic missiles (such as Iskander, Tochka-U, etc.) number over 2,700 units.
- Aeroballistic missiles (such as the Kinzhal) exceeded 100 units in 2025 alone.

2. The execution of the effectiveness of bilateral mass aerial strikes.

In our assessment, this ratio is not optimal for the execution of powerful, large-scale, multi-layered, and combined strike operations. We argue that if the proportion of diverse missile systems does not constitute at least one quarter of the overall strike package, the effectiveness of such operations is reduced – particularly when the total number of aerial attack assets exceeds 500 units. In operations involving smaller numbers, more limited objectives are pursued, and the operational dynamics differ significantly, depending on factors such as strike planning, coordination, and other organisational considerations.

These data show that Russian ballistic missiles, at best, achieve an effectiveness of approximately 50 percent in certain individual months, while their average effectiveness remains around 35-40 percent.

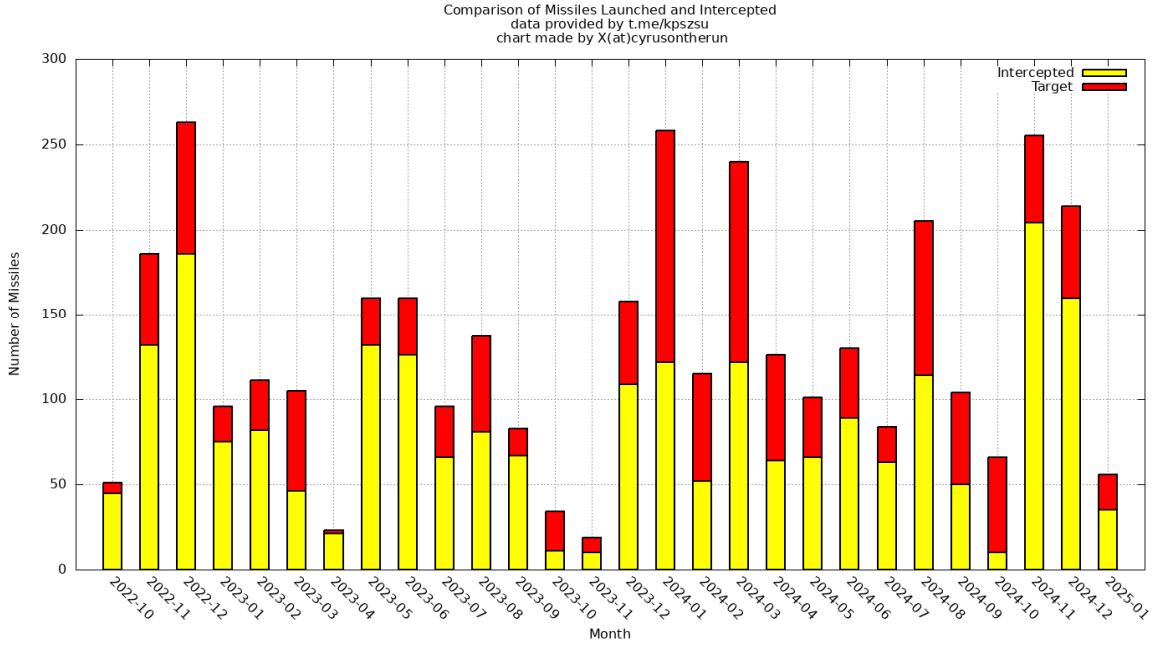

Figure no. 2: Comparison of Missiles Launched and Intercepted

In other cases, U.S.-supplied missile defence systems intercept the ballistic missiles. Among all Russian missile systems, the Kh-47M2 *Kinzhal* aeroballistic missiles demonstrate the highest level of effectiveness. In the field of countering ballistic and aeroballistic missiles, an interesting study suggests that Ukrainian forces were able to neutralise 19 of Russia's most advanced missiles through the use of electronic warfare (EW) capabilities (Kush 2025).

In 2025, Ukrainian air defence operations began to actively employ drones capable of intercepting larger UAVs. In September, one Ukrainian brigade reportedly destroyed 886 Russian UAVs using its counter-drone systems, which is 507 more than were neutralised in June. According to one officer, the counter-drone systems currently achieve approximately 50% effectiveness, compared to just 5% a year earlier (Macdonald 2025). This approach is receiving increasing attention in contemporary military practice. A similar concept has been demonstrated in Ukraine and tested by the French company *Alta Ares*. According to this concept, small drones are deployed in large numbers prior to an incoming strike, creating a distributed aerial presence. Supported by artificial intelligence-based control and coordination software, these small drones are then used to intercept and engage larger strike UAVs (Forbes.ua 2025).

In the future, this approach of sequential countermeasures is expected to become more established, as it represents one of the most effective ways to maintain air superiority. In 2025, only 14 percent of the unprecedented number of strikes against Ukraine were assessed as effective. This figure is, however, subject to debate: open Western and Ukrainian sources often report higher numbers for Russian precision strikes and lower effectiveness of Ukrainian air defences, whereas comparable data from Russian sources is not publicly available. Such data and analyses, when combined with information on the large number of Russian aerial attack assets, may create the impression that Russian strikes are also effective. In reality, however, the situation is markedly different. The overwhelming majority of Russian strikes are ineffective. If they were effective, no supplies would have entered Ukraine from Europe by any route over the past four years, and airports would have been completely paralysed (Zelenskyy 2026). The few strikes that do reach their targets do not inflict damage of a scale sufficient to be decisive. By the end of 2025, the British side has claimed that even the expensive British cruise missiles achieved an effectiveness of approximately 50 percent (Trouncer, Hudson and Boulte 2025, 14), which is entirely natural, as their numbers are

limited, they are not launched in large quantities, and they are not employed within the framework of combined, massed strikes. Consequently, by the end of 2025, in terms of both the number of UAVs deployed and their effectiveness, Ukraine was almost on par with the Russian Federation.

This assessment does not take into account the "Moscow Without Flights" project, which has reportedly caused damages amounting to billions of rubles for the Russian Federation, this assessment also does not take into account disruptions to the Russian logistics system, which has at times been paralysed for several days. Given the number of flights, Russian airlines in this case lose at least $1.5-2 million for every hour the Moscow air hub is down. Overall, if air traffic in Moscow is suspended or significantly disrupted for even one day, it could cost the Russian Federation $10-30 million in direct economic losses, according to estimates by international experts.

For example, following the so-called "Spiderweb" operations, freight transportation by truck reportedly came to a halt for a number of days. Leaving aside the psychological effects on the civilian population of Moscow - such as increased anxiety, stress, and growing uncertainty - and setting aside the heightened vulnerability of Russian military-industrial facilities and strategic infrastructure, a comparison limited solely to cost ratios already places Ukraine in a more advantageous position. A cost ratio of approximately one to ten is significant. This assessment is further reinforced by the fact that Ukraine produces its systems using comparatively lower-cost solutions, largely financed through European funding, whereas for the Russian Federation such production is considerably more complex and costly due to difficulties in procuring critical components. Russian officials and defence industry representatives themselves have repeatedly acknowledged rising costs and challenges associated with acquiring foreign components. At the same time, the damage caused by Russia forces Ukraine to rebuild its infrastructure and simultaneously provides an opportunity to do so better – through decentralisation (Rimutis 2024, 13). Effective implementation of recovery mechanisms – through institutional reforms, reconstruction of critical facilities, increased transparency, and stimulation of private investment – will not only restore lost potential but also strengthen international cooperation and increase the country's investment attractiveness and competitiveness in the post-conflict period (Zahorna and Bidiuk, 2025, 11). The effectiveness of these strikes is most clearly reflected in two indicators. First, according to a survey conducted by the Levada Center, 64 percent of Russians now support 'peaceful dialogue' (Levada Center 2025), representing an increase of 6 percentage points compared to March 2025, prior to the period of mass strikes (Popov 2025).

The second indicator is even more revealing: according to open-source reporting, in September 2025 fuel supply disruptions – particularly shortages of gasoline and diesel fuel – were reported in several regions of the Russian Federation (Gazeta.ru). Fuel prices rose sharply, and in some locations, individuals were reportedly limited to purchasing no more than 30 liters per day. According to open-source assessments, this situation was linked to strikes carried out by Ukrainian aerial attack assets, which reportedly reduced overall gasoline and diesel fuel refining capacity by approximately 18–20 percent (Loginov 2025). The situation continued to deteriorate, and by late October, three additional regions reportedly faced similar constraints, with civilian purchases limited to a maximum of 20 litres (Kanoshuk 2025).

In other words, although the Russian side conducted strikes of an unprecedented scale by its own standards, it was unable to ensure adherence to the six principles identified above (Hovhannisyan 2024, 6). It is therefore unsurprising that these strikes are not accompanied by video documentation or verifiable evidence of accuracy. Claims regarding their effectiveness rely primarily on eyewitness footage and, on occasion, on questionable assertions, such as the alleged destruction of a Ukrainian factory producing military uniforms (Ura.ru).

To summarise the question of the effectiveness of attacks on infrastructure, it should be noted that they have a certain impact on the strategic-political plane. However, they are not decisive for the course of the war.

Conclusions

- When compared with Ukrainian strikes, the data on Russian strikes appear highly impressive at first glance; never before has the Russian air component conducted attacks of such scale. However, a detailed examination of these strikes shows that, as a military operation, they suffer from a number of structural shortcomings and are not effective, in particular.
- In terms of strike density, these attacks are not unprecedented in military history; however, they were conducted over extended time periods, indicating poor synchronisation. This, in turn, provided Ukrainian air defence with the opportunity to organise an effective and coordinated response.
- The strikes were not accompanied by large numbers of decoys, electronic warfare (EW) systems, or anti-radiation missiles. In other words, these were not complex, integrated attacks.
- The strikes were dispersed over a wide area, which consequently reduced their overall effectiveness.
- Naval-launched cruise missiles were frequently not employed in these strikes.
- The strikes were conducted exclusively against fixed targets.
- The strikes were not supported by continuous, accompanying reconnaissance.

In practice, since the end of the Cold War, neither Soviet nor Russian air forces – including during the Russo-Ukrainian wars of 2022-2025 – have conducted a single strategic operation in terms of the level of challenges addressed. Their actions have remained either at the tactical level, or, when they pursued operational and/or strategic objectives, these efforts were partial, incomplete, and ultimately failed to achieve their intended goals.

The forces and assets involved did not operate in a truly combined manner; coordination, interoperability, and command and control were, to put it mildly, deficient. The classical "symphony" of integrated operations – characteristic of U.S. air and naval forces – was absent. This issue has become particularly acute since the first days of January 2026.

Assessing the damage caused by Russian long-range precision strike systems, it can be concluded that Ukraine did not suffer the following types of damage or losses:

- Neither the air force nor the naval forces were neutralised. As of the end of 2025, the Ukrainian Air Force had lost roughly 100 aircraft but continued to maintain approximately 50 combat aircraft and remained operational, with its capabilities expanding due to Western support.
- The air defence forces were not neutralised or degraded to a non-operational level; instead, their capabilities have progressively strengthened due to continuous Western assistance.
- The command-and-control system has not sustained significant damage. There is no recorded instance of the command post of a major Ukrainian force being struck.
- The country's logistics network has not been disrupted and continues to function without major impediments. Western-supplied weapons reach their intended recipients without interruption.
- While the energy sector and economic infrastructure have been affected, the damage has not reached a level that is critical to national functioning.
- No force formation has been taken out of action, and no strategic arsenal has been destructed.

Thus, these mass strikes could become decisive only if their impact on the economy were to increase to such an extent that the financing of the war itself would be significantly undermined. In this respect, Russian strikes have not yet produced effects of strategic significance. While damage has indeed been inflicted, it has not been decisive.

Ukrainian industry is largely either inactive or militarised and relocated underground. Civilian infrastructure, which does suffer damage, is not decisive for the conduct of the war; and even where it is critical, civilian infrastructure can be more easily replenished from Europe, as such assistance is provided more readily under the guise of non-military aid.

As a final conclusion, it can be stated that the collective West continues to finance Ukraine - perhaps not to the full extent required, but nevertheless in a sufficient and sustained manner.

The same cannot be said of the Russian Federation. Even strikes of relatively smaller scale, when combined with sanctions, the seizure or destruction of armored vehicles, and other political measures, produce gradual yet meaningful strategic effects.

Strategic strikes against state infrastructure on both sides are not very effective because they are not organised with the necessary intensity and density. Russian strikes are certainly more massive, but they lack the necessary quantities of heavy strike weapons.

Significantly more ballistic and cruise missiles are required. Most of these are attack drones, which are insufficient to destroy such large targets. As a result, both sides inflict strategic damage on each other, causing inconvenience to the population and creating problems for public life.

However, at the strategic level, this is not a decisive factor: the maneuvers of large military groups, weapons production, and supplies are not significantly affected. Or if they are, they are not significantly affected, since the tempo of the war is so slow that even without them, high-intensity maneuvers are impossible. The war has slowed down for entirely different reasons. Complaints about power outages and cold in large Ukrainian cities are also being voiced by Russian society, but these complaints have no significant impact on the outcome of the war. But in an operational-tactical situation, where its impact is greater, it still negates any advantage. At the operational level, entire forces are deployed, entire military units are created to perform air defence tasks. This means that both sides expend aircraft, air attack assets, and air defence crews and resources that they could otherwise devote to other, more military-oriented tasks that would contribute to the success of the ground forces. However, both sides do this, and their potential is equally reduced, leaving both ground forces in the same state.

In other words, military art confirms the theory that the destruction of strategic infrastructure is a complex and often intractable problem unless significant resources and funds can be allocated to it.

BIBLIOGRAPHY:

1tv.ru.2025. “Rossiyskie sredstva PVO sbili 249 ukrainskih dronov za noch” (Российские средства ПВО сбили 249 украинских дронов за ночь). Accessed 25 November 2025. https://www.1tv.ru/news/2025-11-25/526837rossiyskie_sredstva_pvo_sbili_249_ukrainskih_dronov_za_noch

Chernovol, Katerina. 2025. “S nachala 2025 goda Rossiya potratila na udari po Ukraine okolo $13,4 mlrd,- Forbes” (Черновол Катерина С начала 2025 года Россия потратила на удары по Украине около $13,4 млрд, – Forbes). Accessed 11 August 2025. https://www.unian.net/war/s-nachala-2025-goda-rossiya-potratila-na-udary-po-ukraine-okolo-13-4-mlrd-forbes-13094559.html

Defense Express. 2025. “U Taganrozi vdalos znishiti ne lishe lazerniy A-60, a she y doslidniy A-100 LL, sho dobivae rosiyskiy dovgodub iz zamini A-50" (У Таганрозі вдалось знищити не лише "лазерний" А-60, а ще й дослідний А-100 ЛЛ, що добиває російський "довгобуд" із заміни А-50). Accessed 25 November 2025. https://defence-ua.com/photo/u_taganrozi_vdalos_znischiti_ne_lishe_lazernij_a_60_a_sche_j_doslidnij_a_100ll_scho_tsilkom_dobivaje_rosijskij_dovgobud_iz_zamini_a_50-406.html

Financial times. 2025. **“**Russian missile upgrade outpaces Ukraine’s Patriot defences.” Accessed 01 October 2025 https://www.ft.com/content/078b8e70-a58c-47cc-b573-598850dd5685

Frolov, Bogdan. 2025. “VSU udarili po nositelyu lazernogo oruzhiya Rossii: v Tagnroge porazhen eksperimentalniy A-60” (Фролов Богдан, ВСУ ударили по носителю лазерного оружия России: в Таганроге поражен экспериментальный А-60). Accessed 25 November 2025. https://www.unian.net/war/vsu-porazili-v-taganroge-eksperimentalnyy-samolet-a-60-13206783.html?utm_source=unian&utm_medium=read_more_news&utm_campaign=read_ more_news_in_post

Gardner, Frank. 2025. Protivodronnaya stena Evropi- nuzhna li ona i vozhmozhna li ona.18 noyabrya 2025. (Гарднер, Фрэнк. 2025. «Противодронная стена» Европы – нужна ли она и возможна ли она). Accessed 18 November 2025. https://www.bbc.com/russian/articles/ c8r0667ney3o

Gazeta.ru. 2025. “Glavnoe-ne panikovat: kakim rossiyskim regionam grozyat pereboi s benzinom.” («Главное – не паниковать»: каким российским регионам грозят перебои с бензином). Accessed 01 October 2025. https://www.gazeta.ru/auto/2025/10/01/21780614.shtml

Girnik, Ekaterina, 2025. Pryamoe popadanie raket i desyatkov dronov: Vozdushnie sili raskrili detail rossiyskoy ataki. (Гирнык, Екатерина, Прямое попадание ракет и десятков дронов: Воздушные силы раскрыли детали российской атаки). Accessed 29 November 2025. https://www.unian.net/war/ataka-rossii-v-vozdushnyh-silah-raskryli-detali-13211382.html

Hovhannisyan, Artsrun. 2024. “Perspective Chapter: Basic Rules of Air Supremacy in the Last Thirty Years.” In New Perspectives on Global Peace, 1-13.

Hunder, Max and Anastasiia Malenko. 2025. **“**Exclusive: Russia plans to make up to 120,000 glide bombs this year, Ukrainian intelligence says.**”** Accessed 14 November 2025. https://www.reuters.com/business/aerospace-defense/russia-plans-make-up-120000-glide-bombs-this-year-ukrainian-intelligence-says-2025-11-14/

Konoshuk, Yaroslav. 2025. Krizis isilivaetsya: eshe tri regiona Rossii vveli ogracheniya na prodazhu benzina. Конощук (Ярослав, Кризис усиливается: еще три региона России ввели ограничения на продажу бензина). Accessed 21 October 2025. https://www.unian.net/ economics/energetics/benzin-v-rossii-eshche-tri-regiona-rf-vveli-ogranicheniya-na-prodazhu-topliva-13170345.html

Kulish, Oleksandr. 2025. Skolko raket vipusheno po Ukraine: Detalnaya statistika 2025. (Куліш, Олександр, Сколько ракет выпущено по Украине: Детальная статистика 2025). Accessed 30 October 2025. https://homester.com.ua/ru/skilky-raket-vypushheno-po-ukrayini-detalna-statystyka-2025/

Kush, Sergey. 2025. Ukraina obezvredila 19 “Kinzhalov” pesney “Batko nash-Bandera-The Telegraph” (Кущ, Сергей. Украина обезвредила 19 "Кинжалов" песней "Батько наш - Бандера"- The Telegraph). Accessed 21 November 2025. https://glavred.info/war/ukraina-obezvredila-19-kinzhalov-pesney-batko-nash-bandera-the-telegraph-10717823.html

Levada Center. 2025. Ukraine conflict: attention, support, attitudes toward negotiations and possible scenarios for ending the conflict in September 2025**.** Accessed 17 February 2026. https://www.levada.ru/en/2025/10/22/ukraine-conflict-attention-support-attitudes-toward-negotiations-and-possible-scenarios-for-ending-the-conflict-in-september-2025/

Loginov, Oleg. 2025. Toplivniy krizis v Rossii: deficit benzina i rost cen (Логинов, Олег, Топливный кризис в России: дефицит бензина и рост цен). Accessed 1 October 2025. https://www.dw.com/ru/toplivnyj-krizis-v-rossii-deficit-benzina-i-rost-cen/a-74207416

MacDonald, Alistair and Ievgeniia Sivorka. 2025. **“**Drones Fight Other Drones in the Battle for Ukraine’s Skies**”**. December 3 2025. https://www.wsj.com/world/drones-fight-other-drones-in-the-battle-for-ukraines-skies-aa78dccb

Mittal, Vikram. 2025. “Russia’s New Missile and Drone Strategy Tests Ukraine’s Air Defenses.” Accessed October 07 2025. https://www.forbes.com/sites/vikrammittal/2025/10/07/russias-new-missile-and-drone-strategy-tests-ukraines-air-defenses/?ss=aerospace-defense

Popov, Andrei. 2025. “Total war in the sky: the economics of Ukraine and Russia's new tactics with "long" drones.” (Попов Андрій. 2025. Тотальна війна у небі: економіка нової тактики України та РФ з "довгими" дронами). Accessed 11 June 2025. https://www.unian.ua/economics/other/totalna-viyna-u-nebi-ekonomika-novoji-taktiki-ukrajini-ta-rf-z-dovgimi-dronami-13035438.html

Prishlyak, Nadya. 2025. Bolee 700 celey bilo nad Ukrainoy: v Vozdushnix silah soobshili, skolko udalos sbit (Пришляк Надя, Более 700 целей было над Украиной: в Воздушных силах сообщили, сколько удалось сбить). Accessed 09 July 2025. https://www.unian.net/war/novosti-lucka-seychas-vozdushnye-nazvali-skolko-shahedov-bylo-nad-ukrainoy-13061832.html

RBC-UKRAINE. 2024. **“**Skolko raket I dronov proizvodit RF i chto budet s voynoy v 2024 godu: glavnoe iz intervyu Skibickogo” (Сколько ракет и дронов производит РФ и что будет с войной в 2024 году: главное из интервью Скибицкого). Accessed 15 January 2024. https://www.rbc.ua/ukr/news/skilki-raket-ta-droniv-viroblyae-rf-ta-shcho-1705331213.html

Rimutis, Saulius. 2024. Lessons of War: Ukraine's Energy Infrastructure Damage, Resilience and Future Opportunities. Eastern Europe Studies Centre. Accessed 17 February 2026. https://www.gssc.lt/wp-content/uploads/2024/05/v04_Rimutis_Ukrainos-energetikos-sektoriaus-zala_EN_A4.pdf

Shenderovskiy, Nikita. 2025. “Rossiya atakovala Ukrainu raketami i dronami: v VS VSU rasskazali, skolko celey bylo sbito” (Шендеровский Никита, Россия атаковала Украину ракетами и дронами: в ВС ВСУ рассказали, сколько целей было сбито). Accessed 25 November 2025. https://www.unian.net/war/obstrel-kieva-25-noyabrya-zelenskiy-otreagiroval-na-ocherednuyu-ataku-rf-13206837.html

Shenderovskiy, Nikita. 2026. “Rossiya kardinalno izmenila taktiku vodushnih atak po Ukraine,- CPD” **(**Шендеровский Никита, Россия кардинально изменила тактику воздушных атак по Украине), - ЦПД). Accessed 02 January 2026. https://www.unian.net/war/voyna-v-ukraine-rf-kardinalno-izmenila-taktiku-vozdushnyh-atak-po-ukraine-13243980.html

Sofienko, Nataliya. 2025. “Francuzskaya Sistema protivodeystviya dronam s II uzhe uspeshno sbivayet “Shaxedi” v Ukraine” (Софієнко, Наталія. 2025. Французская система противодействия дронам с ИИ уже успешно сбивает «Шахеды» в Украине). Accessed 17 November 2025. https://forbes.ua/ru/news/frantsuzka-sistema-protidii-dronam-z-shi-vzhe-kilka-misyatsiv-uspishno-zbivae-shahed-v-ukraini-17112025-34185

Trouncer, Alice, Sarah Hudson and Sophie Boulte. 2025 Disrupting Russian Air Defence Production: Reclaiming the Sky. RUSI Research Papers.

Ura.ru. 2024. “Fabrika odezhdi dlya zelesnkogo unichtozhena na Ukraine”. (Фабрика одежды для Зеленского уничтожена на Украине). Accessed 05 January 2024 https://ura.news/news/1052720098.

Usikov A. V., Burutin G. A, Gavrilov V. A. and Tashlikov S. L. 2008. Voennoe iskusstvo v lokalnix voinax i konfliktax. Moscow, Military Publishing House (Усиков А. В, Бурутин Г. А., Гаврилов В. А., Ташликов С. Л., Военное искусство в локальных войнах и в вооруженных конфликтах, Москва, 2008, Военное издательство).

Xodarenok, Mikhail. 2025. Ukraina poluchila stenu dronov. Pomozhet li ona Kievu i chto s ney ne tak? (Ходаренок, Михаил, Украина получила «стену дронов». Поможет ли она Киеву и что с ней не так?). Accessed 13 November 2025. https://www.gazeta.ru/army/2025/11/13/22017746.shtml?utm_auth=false&updated

Zahorna, Viktoriia and Bidiuk Dmytro. 2025. The Impact of the Destruction of Ukraine’s Industrial Infrastructure on International Cooperation and Investment Attractiveness. Public Management and Policy, 10 (14). 1-12

Zelenskiyy, Volodymyr. 2026. The Russians Must Not Get Used to Believing That Their Missiles and “Shaheds” Help Them in Any Way. Accessed 17 February 2026. https://www.president.gov.ua/en/news/rosiyani-ne-mayut-zviknuti-sho-yihni-raketi-j-shahedi-yim-ch-102797

DOI: 10.53477/3045-2309-26-02

NUCLEAR DIPLOMACY IN THE CONTEXT OF THE RUSSO-UKRAINIAN WAR

Mihai ZODIAN, PhD,
Researcher, Centre for Defence and Security Strategic Studies,
"Carol I" National Defence University, Bucharest, Romania,
E-mail address: zodian@gmail.com

Abstract*: The Russian aggression against Ukraine resurrected old nuclear fears from their grave. This is an understandable and somehow unavoidable effect, yet a thorough study of nuclear weapons and the interaction that they enable is important, allowing decision-makers and the public to avoid costly mistakes. This paper is designed as an essay about nuclear weapons, alongside strategic relations as a context for the Russo-Ukrainian War, focusing on nuclear safety, coercive diplomacy and security regimes. The main conclusions are that the risk of accidents remains, the fear of escalation is not always effective as a foreign policy tool, and that international institutions have seriously been weakened.*

Keywords*: nuclear safety; deterrence; compellence; nuclear weapons; nuclear proliferation; security regimes.*

Introduction

Why does the nuclear context matter? Mainstream strategic studies argue that conflicts conducted under the nuclear shadow are restricted by the existence of these arsenals, whether explicitly or tacitly (T. C. Schelling [1966] 2008, George, Simons and Hall 1971). Moreover, coercive diplomacy employs nuclear threats to avoid certain results or to push for specific effects, producing a range of consequences (T. C. Schelling [1966] 2008, George, Simons and Hall 1971). Additional considerations include Moscow's propaganda and cognitive warfare ("the Russian steamroller"), as well as wider implications for global security, taking into account the renewed great power rivalry that contains a nuclear dimension.

This development led to a revival of earlier, Cold War-era ideas within strategic studies. Academic debates over the merits of deterrence and compellence ended in a limbo, following the dissolution of the Soviet Union. Consequently, we are left with serious doubts about the way interests are defined, threats are perceived, and how social representations of hostilities are developed, during periods of intense crisis, and about the best ways to handle these issues. Therefore, to study and enlarge the classical ideas about the use of force as a threat is also useful from a scholarly point of view.

This paper has two goals. The first one is a description of nuclear issues surrounding the Russo-Ukrainian War during the interval winter 2024/2025-winter 2025/2026. The interval was chosen based on the premise that these subjects require more academic attention, and that they may also help the decision-makers and the public to make better informed choices. The other aim is to link contemporary events to wider, theoretical questions about the use of force and threats in world politics, in general.

Several clarifications on conceptual foundations are needed. The study of nuclear topics (such as deterrence, limited war, compellence) is fraught by notorious methodological and descriptive problems, including the difficulty of discerning effects due to counterfactuality and the lack of reliable facts (Starr 2002, loc 1011-1015). Nevertheless, the academic study of security relies on the premise that reason helps us better understand conflicts and the employment of force (Morgenthau 2007[1948], 44-49). Therefore, an essayistic approach that problematizes the nuclear context of the Russo-Ukrainian War remains justifiable, if it relies on accepted intellectual frameworks.

The paper rests on an eclectic conceptual framework. It draws on rational deterrence theory and the literature on international regimes (T. C. Schelling [1966] 2008 , Mayer, Rittberger și Zürn 2002[1993], 391-430, Morgan 2003). The hypothesis is that interest-oriented behavior, and the ability to make calculations under conditions of high uncertainty, can help us to understand several issues in the context of the Russo-Ukrainian War. This perspective is compatible with alternative interpretations of the same topics, close to Weberian ideal-type approach (Weber 2011[1919], Morgenthau 2007[1948], 44-55).

The uncertainty characteristic of conflicts also influences contemporary narrations. The data is gathered from news media and official sources, occasionally combined with expert evaluation and scientific studies where available, covering the period up to February 24, 2026. To materialize the paper two goals of descriptions and theorization, the essay advances three research objectives: first, to clarify the question of nuclear safety taking into account the Russian air campaign against the Ukrainian energy system; second, to examine the practice of coercive diplomacy that reunites issues such as compellence or deterrence (George, Simons and Hall 1971, 18-19, 22-25, Art 1980, 3-35); and third, and to elaborate on wider considerations regarding arms control and disarmament. The structure of the paper reflects these objectives accordingly.

1. Nuclear safety

Nuclear safety remains an issue, in the context of the Russo-Ukrainian War. There are 15 active reactors in 4 functional Nuclear Power Plants (NPP), and one of them, the most important, of Zaporizhzhia is under Russian control since 2022 (WNA 2026). The Chornobyl site was the scene of several fights, with the Russian forces digging trenches in the radioactive zone, until they had to withdraw (Plokhy 2023). Overall, critical infrastructure in Ukraine is at risk, as witnessed by the flooding of the Nova Kakhovka dam (Plokhy 2023).

Since the beginning of the full scale Russian aggression against Ukraine, nuclear safety has been a serious problem and several worrying incidents happened during the last year. On 14 February 2025, a drone hit the New Safe Container that covers the infamous Unit 4 from the Chornobyl NPP. No radiation emission was registered (IAEA 2025). On 4 July 2025, there was a power loss for the Zaporizhzhia NPP (IAEA 2025). And on 23 September 2025, another power loss was registered at the Zaporizhzhia NPP (IAEA 2025).

Lately, these worries have intensified, because of the ongoing Russian campaign against Ukraine’s energy infrastructure. Russia’s advances are very slow (70 meters/day or less), and it compensates by negotiations, and by the renewed air strikes directed towards the civilian power system (Jone and McCabe 2026). The campaign aims to increase the civilian costs of the war, and to press the Ukrainian authorities and the Western countries. It targets the secondary power stations. Many link the NPP to the consumers. Almost half of Ukraine’s energy comes from its NPPs (WNA 2026, Culverwell 2006, Belkour 2026).

From a diplomatic point of view, the problem is that the aggressor is also a permanent member of the UN Security Council. Still, there is the global interest to avoid another Chernobyl disaster, and the nonproliferation regime provides a useful service, in this case. The rule is that the NPP should be safe from attacks. IAEA continued to deploy a team at the Zaporizhzhia NPP, and to maintain contacts with both sides (WNA 2023, IAEA 2025).

2. Coercive nuclear diplomacy

The Russo-Ukrainian War has involved the aggression of a nuclear weapon state against a country that had previously gave up its inherited arsenal. Putin’s regime has also cooperated closely with another nuclear power, China, while the coalition supporting Kyiv included three nuclear weapon states (US, France, and Britain). In addition, North Korea, which has developed these

armaments in the last decades, has helped Moscow during the conflict. It is not surprising that old Cold War concepts, such as nuclear deterrence, compellence, and escalation management, have regained their practical importance (Schelling [1966] 2008 , Powell 2015, Gross Stein 2023).

Several explanations may be advanced. One relates to the ongoing rivalry among great powers, especially between China and the United States. While the tone is more polite since Donald Trump returned to the presidency, the fundamentals remain, one of them being the military modernization and growth promoted by the Beijing leadership. This process entails a salient nuclear dimension, that created worries of China joining US and Russia as a third major nuclear state (Kristensen, et al. 2025, U.S. Department of Defense 2025).

Another explanation derives from the specific context of the Russo-Ukrainian War. Nuclear threats have been made: statements by president Putin, positions taken by Russian public figures, tests, the deployment in Belarus etc. (Brands 2024, 1-14, Perkovich 2026). There is an ongoing debate about their meaning and value, yet some agreement exists that the ones uttered in autumn 2022 may have been serious, following the two successful Ukrainian counteroffensives around Kharkiv and Kherson (Brands 2024, 1-14, Perkovich 2026). It is also reasonable to assume that there may be "known unknowns", discrete or tacit communications between nuclear powers (T. Schelling 2000[1960], Rumsfeld 2002).

The presence of nuclear weapons also structures political and diplomatic setting of the Russo-Ukrainian War. It is reasonable to assume that they define its limits, and fears of nuclear escalation were expressed by officials, especially by the US President, Joe Biden, and by his successor, Donald Trump (Gross Stein 2022, Gross Stein 2023, 29-50, Brands 2024, 1-14, Shake 2024, 156-172, Roth și Gambino 2025). These restrains imply that Russia does not target NATO countries supplying Ukraine, while Western countries do not intervene directly (Gross Stein 2022, Gross Stein 2023, 29-50, Brands 2024, 1-14, Shake 2024, 156-172, Roth și Gambino 2025). For Ukraine, the conflict is a total war (Gross Stein 2022, Gross Stein 2023, 29-50, Brands 2024, 1-14, Shake 2024, 156-172, Roth și Gambino 2025).

Therefore, the American general policy towards supporting Ukraine was structured also as a risk management strategy (Gross Stein 2023, Shake 2024). More than that, it is difficult to prove, and the question of doing too little, or too much will probably remain unanswered for the time being. What is more plausible is that, despite its nuclear threats, Russia has failed to stop the increase in assistance from the West, yet it has probably slowed down the pace, in comparison with a scenario in which such threats were absent (Brands 2024). The question of support was restated during the second Trump administration (NATO 2025).

Other conclusions from the Cold War conflicts were reasserted. For example, nuclear deterrence and compellence face credibility issues, while escalation dominance is difficult to apply since nuclear weapons are blunt instruments, perceived as genocidal weapons (George, Simons and Hall 1971, Tannenwald 2007). This is largely because nuclear coercion is more credible (and presumably more effective) when survival is at stake. It is also easy to overstate the importance of these activities (Perkovich 2026).

The balance of interests, goals and or political will also is important, in this escalation management, a form of coercive diplomacy (Schweller 2012). Russia is more interested in the war than the West (Powell 2015, Snyder 2022, Thayer 2022). For Ukraine, survival is at stake, while for Russia is a war of choice (Powell 2015, Snyder 2022, Thayer 2022, Brands 2024, 1-14). Thus, the result is an equilibrium of will between the West-Ukraine partnership and Russia (Powell 2015, Snyder 2022, Thayer 2022, Brands 2024, 1-14).

3. Nuclear security regimes

International relations are not only patterned but also often normatively regulated. To this end, states have created regimes which are "principles, norms, rules and decision-making procedures in an issue area" (Krasner 1982, 185, Jervis 1982, 357-378, Ungureanu 2006, 233-242). There are two

types of nuclear security regimes, based on their objectives: arms control and non-proliferation (Baylis 2019, 220-237)[1]. The degree of order within these sectors ebbs and flows under the influence of many factors, such as power, interest, and state identities (Krasner 1982, Wendt 1992).

At present, nuclear security regimes are in a state of crisis. Some are still influential (the Non-Proliferation Treaty), even a few of the more specialized still hold (The Partial Test Ban Treaty or the Outer Space Treaty), albeit contested for a variety of political and strategic reasons (Baylis 2019, 233-242, Gray 2007, United Nations Office for Disarmament Affairs 2005). Several treaties have been disbanded (denounced, expired or suspended), including New Start, the ABM Treaty, and the INF Treaty (Baylis 2019, 233-242, U.S Department of State 2022). The nuclear arms control sector, in particular, remains unregulated, reflecting a more general trend of formal regimes weakening.

This crisis has affected the rules, and the decision-making procedures, but not the principles and norms (Krasner 1982, 185-205). No one argues that nuclear strategic instability is a good thing, and even US President, Donald Trump is cautious on the issue of large nuclear arsenal, as discussed above. A general war between great powers is still as unwanted as it was during the Cold War. Therefore, we are witnessing a change within the nuclear security regimes for arms control, and, up to a point, a weakening of these partial orders (the abandoning of INF was a case for both trends) (Krasner 1982, 185-205).

The most invoked causes are changes in the aggregate or sectoral distribution of power and global or regional conflicts. For example, the great power rivalry between US and China, which has led to a renewed arms race in the Asia-Pacific region with a nuclear component, Russia's policies in Europe, especially the aggression against Ukraine, or issues of ideology and prestige. These trends led to the expectations of a "third nuclear age" (Colin Gray), defined by a bipolar or multipolar power distribution and the differentiation between aggregate power and nuclear capabilities, which means that small or medium powers may overcompensate by intensive nuclear armament (Walton 2019, 202-219)[2]. Under these conditions, a threat is the renewed nuclear proliferation (Brands 2024, 1-14)[3].

There is, however, a measure of positive perspective**.** Taking into account that the principles and norms of the arms control regime still holds, making strategic stability the main goal of the nuclear strategies, Thomas Schelling's distinction of tacit versus formal orders sheds more light on the current situation (T. Schelling 2000[1960], Stein 1990, 25-54)[4]. This implies that, with the basic understanding, reasserted in some official documents, that a nuclear war can not be won, a formal agreement may be supplanted, for a while by the convergence of expectations (U.S. Mission Geneva 2022)[5]. The situation is still problematic, as it leaves space for disagreement, while personalists diplomacy is not enduring, therefore, maybe the often proposed trilateral arms control agreement (US, China, Russia) may represent an acceptable solution for long-term stability (Baklitskiy 2020)[6].

[1] Arms control is about restraint, while non-proliferation includes an element of disarmament, therefore, of reduction of abolition of nuclear weapons (Baylis 2019, 222).
[2] Though the ongoing controversies about non-proliferation and the Iran case are closer to the second nuclear age, when the threats were defined in terms of smaller powers and international terrorism (Walton 2019, 202-219).
[3] An alternative explanation is ideological. Nationalist, and populist leaders are skeptical of international organizations and experts (Müller 2017). Simona Soare drew a similar conclusion about theories of hegemonic decline that influenced regime theory (Soare 2013).
[4] During a debate, Diana Mărgărit suggested that liberal distrust of regulations may also be at hand (Mărgărit 2025). Oran Young theorized that self-interest based regimes can be established by spontaneous interaction or negotiations (Young 1989).
[5] An additional factor is the existence of surveillance satellites (Baklitskiy 2020). Another is the nuclear taboo, the moral disgust evoked by the use of nuclear weapons (Tannenwald 2007). That it has effects was made obvious by the reaction, in autumn 2022, at the risk of Russia using tactical nuclear weapons, when the Ukrainian forces made significant gains. Even China and India, its partners and allies, voiced opposition (Brands 2024).
[6] Spontaneous or tacit agreements are vulnerable during periods of instability, or to information and transaction costs (Keohane 1982, Young 1989, 94).

Conclusions

This paper problematized the nuclear issues surrounding the Russo-Ukrainian War. It followed an essayistic approach because the explanations, in this domain, are counterfactual and data is often a matter of speculation. Rational deterrence theory and the international regime studies furnished the intellectual framework that was used to understand this context. The paper aimed at description and generalization, following three objectives.

First, nuclear safety remains a problem. Several incidents were registered during 2025, following similar occurrences since the start of the war. The current Russian air campaign against the Ukrainian energy system targeted power substations, which may put the NPPs in danger. While the AIEA continued its efforts at monitoring and mediations, the fact that the aggressor is a permanent member of the UN Security Council compounds the issue.

Second, the effects of Russia's nuclear coercion are ambiguous. Available evidence is insufficient to ascertain how, and to what extent, the decision-makers were influenced by Moscow's threats, wthe credibility of which was problematic, except maybe for autumn 2022. Western support still goes on today. It represents a relevant factor, but it has not been decisive and it has not brought by itself the territorial gains that Russian leaders may have expected.

Third, the nuclear security regimes are in shambles, although a tacit understanding probably still exists. While the West is preoccupied with European and Middle Eastern topics, China is increasing its nuclear arsenal on a significant scale, alarming the decision-makers in Washington, as Pentagon's report suggest. The major arms control treaties have expired, or have been denounced, and it is uncertain whether they will be renewed soon. The aggression against Ukraine has weakened the non-proliferation regime, showing that a non-weapon state can be attacked by a nuclear owner, placing the UN in a diplomatically difficult position.

Overall, nuclear topics have played a significant role, yet they have formed only the context for the Russo-Ukrainian War. Nuclear weapons have not been used, and this situation will continue in the future, for reasons of prestige (a nuclear strike meaning a conventional failure), and potentially also because of the taboo identified by Nina Tannenwald. In contemporary international politics, these tools have made a partial comeback, as support for deterrent strategies, and as means of arms races. The study of their implications is important, as the world becomes more conflictual.

BIBLIOGRAPHY:

Art, Robert J. 1980. "To What Ends Military Power?" *International Security* 3-35.

Baklitskiy, Andrey. 2020. *The Prospects for U.S.-Russian Arms Control*. electronic, Center for Strategic and International Studies.

Baylis, John. 2019. "The Control of Weapons of Mass Destruction." In *Strategy in the Contemporany World*, by John Baylis, James J. Wirtz and Colin S. Gray, 220-237. Oxford: Oxford University Press.

Belkour, Ann. 2026. "Ukraine's Energy System Near Brink." *Kyiv Independent*. January 18. Accessed February 24, 2026. https://youtu.be/8nKec544SfE?si=SJQPi5mhdxvTGAyZ

Brands, Hal. 2024. "The Ukraine War and Global Order." In *War in Ukraine: Conflict, Strategy and the Return of a Fractured World*, by Hal (ed.) Brands, 1-14. Baltimore: John Hopkins University Press.

Culverwell, Dominic. 2006. "Exclusive: Russia's worst attack on substations halves Ukraine's nuclear power output." *Kyiv Independent*. February 9. Accessed February 24, 2026. https://kyivindependent.com/ukraine-repairs-nuclear-substation-but-situation-remains-critical-after-mass-attack/

George, Alexander L., William E. Simons, and David K. Hall. 1971. *The Limits of Coercive Diplomacy*. Boston: Little, Brown.

Gray, Colin S. 2007. *Another Bloody Century.* Londra: Weidenfeld & Nicolson.

Gross Stein, Janice. 2022. "The Ukraine Dilemma. Can the West Save Kyiv Without Starting a War with Russia?" *Foreign Affairs.* March 2022. Accessed February 24, 2026. https://www.foreignaffairs.com/articles/russia-fsu/2022-03-09/ukraine-dilemma

Gross Stein, Janice. 2023. "Escalation Management in Ukraine «Learning by Doing» in Response to the «Threat that Leaves Something to Chance»". *Texas National Security Review* 6 (3): 29-50.

IAEA. 2025. "Timeline of the IAEA's response activities to the situation in Ukraine". *International Agency for Atomic Energy.* Accessed February 23, 2026. https://www.iaea.org/interactive/timeline/169792

Jervis, Robert. 1982. "Security Regimes". *International Organization,* 36 (2): 357-378.

Jone, Seth G., and Riley McCabe. 2026. *Russia's Grinding War in Ukraine*. electronic, CSIS.

Keohane, Robert O. 1982. "The Demand for International Regimes". *International Organization* 36 (2): 325-355.

Krasner, Stephen D. 1982. "Structural Causes and Regime Consequences: Regimes as Intervening Variables." *International Organization* 36 (2): 185-205.

Kristensen, Hans M., Matt Korda, Eliana Johns, and Mackenzie Knight. 2025. "Chinese nuclear weapons, 2025." *Bulletin of the Atomic Scientists* 81 (3): 135-160. doi:10.1080/00963402.2025.2467011.

Mărgărit, Diana. 2025. "Debate during the conference". Work in Progress/Cercetări în lucru. March 23.

Mayer, Peter, Voker Rittberger, and Michael Zürn. 2002[1993]. "Regime Theory: State of the Art and Perspectives." In *Regime Theory and International Relations*, by Volker Rittberger and Peter (ed.) Mayer, 391-430. Oxford: Claredon Press.

Morgan, Patrick M. 2003. *Deterrence Now.* Cambridge: Cambridge University Press.

Morgenthau, Hans J. 2007[1948]. *Politica între națiuni: lupta pentru putere și lupta pentru pace.* Iași: Polirom.

Müller, Jan-Werner. 2017. *What is populism ("Ce este populismul").* Iași: Polirom.

Perkovich, George. 2026. *How to Assess Nuclear 'Threats' in the Twenty-First Century.* electronic, Carnegie Endowment for International Peace.

Plokhy, Serhii. 2023. *Războiul ruso-ucrainean: Întoarcerea istoriei.* București: Trei .

Powell, Robert. 2015. "Nuclear Brinkmanship, Limited War and Military Power." *International Organization* 69 (3): 589-626.

Roth, Andrew, and Lauren Gambino. 2025. "Ukraine 'gambling with world war three', Trump tells Zelenskyy in fiery meeting." *The Guardian.* February 24. Accessed February 24, 2026. https://www.theguardian.com/us-news/2025/feb/28/trump-zelenskyy-meeting-ukraine-aid-war

Rumsfeld, Donald. 2002. "DoD News Briefing – Secretary Rumsfeld and Gen. Myers". *US. Department of Defense.* February 12. Accessed February 24, 2026. https://web.archive.org/web/20160406235718/http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636

Schelling, Thomas C. [1966] 2008. *Arms and influence.* Kindle edition: Yale University Press.

Schelling, Thomas. 2000[1960]. *Strategia conflictului.* București: Integral.

Schweller, Randall L. 2012. "Noi cercetări realiste asupra alianțelor: rafinarea și nu respingere propoziției lui Waltz referitoare la balansare." In *Realismul și balanța de putere*, by John A. Vasquez and Colin Elman. Iași: Polirom.

Shake, Kori. 2024. "US Strategy in Ukraine." In *War in Ukraine: Conflict, Strategy and the Return of a Fractured World*, by Hal (coord.) Brands, 156-172. Baltimore: John Hopkins University Press.

Snyder, Tymothy. 2022. "How does the Russo-Ukrainian War end?" *Substack.* February 24. Accessed February 24, 2026. https://snyder.substack.com/p/how-does-the-russo-ukrainian-war

Soare, Simona R. 2013. *Sub povara a 90 000 de done de diplomație? Statele Unite ale Americii, strategia hegemonică și declinul relativ de putere.* Edited by hegemonic strategy and relative decline of power Under the weight of 90 000 tonnes of diplomacy? The United States. București: Editura Militară.

Starr, Harvey. 2002. “Cumulation, Synthesis, and Research Design for the Post-Fourth Wave.” In *Evaluating Methodology in International Studies*, by Frank P. Harvey and Michael Brecher, 59-80. Ann Arbor: The University of Michogan Press.

Stein, Arthur A. 1990. “Coordination and Collaboration: Dilemmas of Common Interests and Common Aversions.” In *Why Nations Cooperate. Circumstances and Choice in International Relations*, by Arthur A. Stein, 25-54. Ithaca: Cornell University Press.

Tannenwald, Nina. 2007. *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons Since 1945.* Cambridge: Cambridge University Press.

Thayer, Bradley. 2022. "Russia’s War in Ukraine: A Balance of Power Problem for America?" *1945.* March 7. Accessed February 24, 2026. https://www.19fortyfive.com/2022/03/russias-war-in-ukraine-a-balance-of-power-problem-for-america

U.S Department of State. 2022. *New START Treaty Aggregate Numbers of Strategic Offensive Arms.* septembrie 1. Accessed martie 15, 2024. https://www.state.gov/new-start-treaty-aggregate-numbers-of-strategic-offensive-arms-3/

U.S. Department of Defense. 2025. *Military and Security Developments Involving the People’s Republic of China.* electronic, U.S. Department of War.

U.S. Mission Geneva. 2022. “Join Statement of the Laders of the Five Nuclear-Weapon States.” *U.S. Mission to International Organizations in Geneva*. January 3. Accessed February 24, 2026. https://geneva.usmission.gov/2022/01/03/p5-statement/

Ungureanu, Radu-Sebastian. 2006. “Regimuri de securitate.” In *Manual de relații internaționale*, by Andrei Miroiu and Radu-Sebastian Ungureanu, 233--241. Iași: Polirom.

United Nations Office for Disarmament Affairs. 2005. Treaty on the Non-Proliferation of Nuclear Weapons (NPT)." *United Nations Office for Disarmament Affairs.* Accessed February 23, 2026. https://disarmament.unoda.org/wmd/nuclear/npt/#:~:text=The%20NPT%20is%20a%20landmark,and%20general%20and%20complete%20disarmament

Walton, C. Dale. 2019. “The Second Nuclear Age: Nuclear Weapons in the Twenty-First Century.” In *Strategy in the Contemporary World*, by James J, Wirtz, Colin S. Gray (coord.) John Baylis. Oxford: Oxford University Press.

Weber, Max. 2011[1919]. *Omul de ştiinţă şi omul politic.* București: Humanitas.

Wendt, Alexander. 1992. “Anarchy is what States Make of it: The Social Construction of Power Politics.” *International Organization* 46 (2): 391-425.

WNA. 2026. “Nuclear Power in Ukraine.” *World Nuclear Association*. Accessed February 23, 2026. https://world-nuclear.org/information-library/country-profiles/countries-t-z/Ukraine

—. 2023. “Ukraine: Russia-Ukraine War and Nuclear Energy.” *World Nuclear Association.* octombrie 16. Accessed martie 13, 2024. https://www.world-nuclear.org/ukraine-information/ukraine-russia-war-and-nuclear-energy.aspx

Young, Oran. 1989. “Regime Dynamics: The Rise and Fall of International Regimes.” In *International Cooperation. Buliding Regimes for Natural Resources and Environment*, by Oran Young, 81-103. Ithaca: Cornell University Press.

DOI: 10.53477/3045-2309-26-03

FROM POST-COLD WAR INTERDEPENDENCE TO STRATEGIC DECOUPLING: REDUCING THE EU'S DEPENDENCE ON ENERGY RESOURCES FROM THE RUSSIAN FEDERATION (2022-2025)

Aurel LAZĂR, PhD,
Teaching Assistant, "Petru Maior" Faculty of Science and Letters,
"George Emil Palade" University of Medicine, Pharmacy, Science, and Technology,
Târgu Mureș, Romania,
E-mail address: lazar.a.aurel@gmail.com

Abstract: *This article examines, through the lens of energy security understood as resilience, the European Union's accelerated decoupling from Russian energy resources between 2022 and 2025, against the backdrop of energy's transformation from a largely economic commodity into a geopolitical instrument in post-Cold War Europe. Russia's full-scale invasion of Ukraine in 2022 catalysed a strategic rupture with the interdependence paradigm consolidated over previous decades, prompting the EU to adopt REPowerEU, mandatory storage and coordinated demand-reduction measures, and successive sanctions packages. Empirically, EU imports of Russian gas declined, aggregate gas demand fell over 2021-2024, and Russia's share of EU crude oil imports dropped sharply. The case studies (Germany; Poland and the Lithuania; Italy; and South-Eastern Europe, including Romania) highlight divergent national pathways, while the risk assessment section addresses persistent dependencies (Hungary and Slovakia) and the challenge of circumvention via intermediaries, swaps, and hub-based transactions.*

Keywords*: energy security; dependence; REPowerEU; resilience; Russian Federation; natural gas.*

Introduction

In 2022, energy security became a strategic priority for the EU, against the backdrop of the Kremlin's use of energy as a geopolitical instrument and the disruption of supply chains. The challenge was not merely the level of consumption, but also the configuration of infrastructure. The European energy market was integrated, yet characterised by sharply asymmetric regional dependencies, particularly along the East–West axis. Prior to this shock, Russian gas held a structurally significant share in the EU's import mix, which meant that replacing it required simultaneous interventions on both the supply side (new routes, LNG imports, alternative contracts) and the demand side (conservation measures, energy efficiency, fuel switching). The energy crisis triggered in 2022 underscored the tight linkage between energy security and economic security. It demonstrated how energy price volatility rapidly feeds into inflation, undermines industrial competitiveness, and generates substantial social costs. The relevance of this research is therefore twofold.

Theoretically, the article tests the hypothesis that reducing dependence on a dominant supplier increases the resilience of the energy system, yet may also produce new forms of dependency and transition costs. Practically, its findings can inform the design of more robust energy security policies in a volatile global environment.

Throughout this study, the intention is to provide as precise an answer as possible to the following research question: *To what extent, and through which mechanisms, did the EU succeed in reducing its dependence on energy resources originating in the Russian Federation between 2022 and 2025, and what new vulnerabilities emerged as unintended side effects of this process?* The

analysis proceeds from the hypothesis that EU policies – such as the REPowerEU plan and the emergency measures adopted in the gas market – substantially reduced exposure to supply shocks originating in the Russian Federation, while transferring part of the risk to: (a) the global liquefied natural gas (LNG) market and associated price volatility; (b) infrastructure constraints and administrative-capacity limitations (for example, slow permitting procedures for new projects); and (c) industrial dependencies embedded in the supply chains required for the energy transition (European Commission 2022, 11-12).

From a methodological point of view, the study employs a combined research design. (1) It conducts a documentary analysis of the EU energy security framework, including European Commission communications, relevant regulations, Council of the EU materials, and Eurostat data, complemented by selected national sources. (2) It applies a descriptive statistical analysis of key indicators of energy imports, consumption, and storage in order to capture quantitative developments over 2021–2025. (3) It selects a set of representative national case studies based on the diversity of initial conditions and policy instruments (e.g., LNG infrastructure investment, interconnection levels, the existence of alternative contracts). The research draws on data and reports produced by European and national institutions, regulatory authorities, energy-sector companies and major international news agencies. With respect to limitations, several points should be noted, international trade data are typically released with a time lag and may be subject to subsequent revisions.

Theoretically, the analysis relies on the concept of energy security because reducing the EU's dependence on Russian resources is not simply a question of where the energy is purchased from, but rather a systemic risk issue - namely, how vulnerable a state or the EU as a whole is to supply disruptions, price shocks, or geopolitical pressure. The concept captures the capacity of an energy system to deliver energy reliably and predictably across multiple dimensions: physical availability, geopolitical accessibility, economic affordability (price level and volatility), and acceptability (environmental sustainability and social legitimacy). A key implication is that a given policy can enhance security along one dimension (e.g., greater physical availability) while simultaneously undermining it along another (e.g., higher costs), thereby generating policy dilemmas for decision-makers (Cherp Jewell 2014, 415-421).

In this paper, energy security is treated as resilience: the capacity of an energy system to withstand and adapt to shocks without undermining essential socio-economic functions, while the pre-2022 EU–Russia relationship illustrates how apparent stability was achieved at the cost of elevated geopolitical risk through the concentration of dependence. Energy dependence arises when there are no readily available alternatives to replace a supplier or route and adjustment costs are high; accordingly, what matters is not only the share of imports, but also the underlying infrastructure (pipelines/LNG), contractual arrangements, storage capacity, and the degree of interconnection (European Commission 2022, 11-12). In the EU's approach, diversification and solidarity within the internal market constitute structural instruments of energy security, reflected in the Energy Union strategy and in the legal framework governing solidarity in crisis situations (European Union 2017).

1. The Dynamics of Dependence: From Concentration to Diversification (2021-2025)

A concise indicator of Europe's energy reorientation is the sharp decline in the volume of gas imported from Russia. EU imports of Russian gas fell from more than 150.2 billion cubic metres (bcm) in 2021 to below 51.7 bcm in 2024. Over the same period, EU gas imports from the United States increased from 18.9 bcm to 45.1 bcm, while imports from Norway rose from 79.5 bcm to 91.1 bcm. This shift was enabled in part by the high flexibility of liquefied natural gas (LNG), as the EU rapidly expanded LNG imports, with the United States emerging as the dominant supplier. In Q3 2025, the United States accounted for approximately 59.9% of the EU's total LNG imports, whereas Russia supplied only 12.7%. Compared with Q3 2024, U.S. LNG imports were 19.1% lower and imports from the Russian Federation were 5.2% higher. Despite this decline, the Russian Federation remains

the EU's second-largest LNG supplier, Russia's share of the EU's pipeline gas imports fell to approximately 11%; when LNG is included, Russia accounted for under 19% of the EU's total gas imports, compared with over 40% in 2021. By contrast, Norway became the leading supplier, providing more than one-third of the EU's total gas imports, around 91.1 bcm in 2024 (Council of the European Union 2025a).

The reduction in dependence on Russia was also underpinned by a contraction in domestic demand: EU gas consumption fell by more than 19% between 2021 and 2024. This demand-side adjustment, together with expanded storage capacity and more intensive use of gas stocks, helped strengthen the EU's supply resilience and reduced exposure to Russian deliveries. From a security perspective, lower demand reduces the likelihood of a physical gas shortage and diminishes a dominant supplier's ability to influence prices by constraining supply (European Union 2017).

In the oil segment, the impact of EU sanctions against Russian Federation is particularly pronounced: Russian Federation's share of EU imports of crude oil and petroleum products fell from 28.74% in Q1 2021 to 1.26% in Q3 2025. This indicator captures both the redirection of supply towards alternative producers and the near-complete curtailment of Russian imports in the segments covered by sanctions (Eurostat 2025, "EU Trade with Russia – Latest Developments," 1-3). Nevertheless, a residual dependence on Russian LNG persists: although its share declined – from 22.24% in Q1 2021 to 14.98% in Q3 2025 - Russia remains a relevant LNG supplier for Europe. This residual exposure has led the EU to place the issue on the agenda and to negotiate an explicit phased-out approach to Russian LNG imports (Council of the European Union 2025b).

2. EU Strategy: From the "Energy Union" to REPowerEU and Emergency Regimes

The EU's approach to energy security displays a notable degree of institutional continuity. The Energy Union Strategy (2015) already set out the principal dimensions of European energy policy - energy security, solidarity and trust; an integrated internal energy market; energy efficiency and decarbonisation; and research, innovation, and competitiveness. The 2022 crisis accelerated the pursuit of these objectives and made explicit the nexus between energy policy and the Union's strategic autonomy (European Commission 2015).

In response to the 2022 crisis, the EU entered a new phase with the launch of the REPowerEU Plan (May 2022), which constitutes the strategic framework through which the Union sought to end dependence on Russian energy via an integrated approach combining energy savings, diversification of import sources, and an accelerated shift to clean energy. The document stresses that no single member state can manage such a transformation independently within an interdependent energy market, thereby underscoring the need for EU-level coordination. In practical terms, from 2022 onward the EU simultaneously introduced a package of emergency measures comprising: (a) mandatory rules on gas storage; (b) mechanisms for coordinated demand reduction; and (c) EU-level instruments for cooperation and solidarity (including joint purchasing and demand aggregation platforms, as well as regional support arrangements). Taken together, this package functions as a form of collective insurance against supply-disruption risk and as a tool for mitigating market volatility by disciplining – and, where necessary, reducing – demand (Council of the European Union 2022).

3. National Strategies and Case Studies

The EU provided a common framework through the adoption of rules, coordination mechanisms, and Union-wide targets; however, the effective reduction of dependence on the Russian Federation ultimately materialised through nationally tailored policies implemented by individual member states. Accordingly, some states invested heavily in LNG import infrastructure, others maximised the use of existing pipelines connected to alternative suppliers, while another group prioritised regional interconnections in an effort to "import" energy security from neighbouring

markets. This section offers a comparative analysis of four national and regional case studies (Germany; Poland and Lithuania; Italy; and South-Eastern Europe) in order to highlight divergent approaches and the lessons derived from them.

Germany – LNG as a transitional solution and demand-side management

Germany constitutes a critical case study because, prior to 2022, it was among the EU member states most exposed to Russian pipeline gas; after 2022, it was compelled to replace these volumes rapidly by combining supply-side diversification (above all through LNG imports) with domestic demand reduction measures. The overarching objective was to limit both the risk of supply disruptions and the associated macroeconomic shocks.

In 2023, Germany's total gas imports amounted to approximately 968,000 GWh, with the main suppliers being Norway (about 43% of total imports), the Netherlands (26%), and Belgium (22%). These figures illustrate Germany's capacity to diversify its supply base swiftly and highlight the importance of West European "hubs" (notably the Netherlands and Belgium) in sustaining German supply through cross-border flows. On the LNG dimension, Germany operationalised new import entry points in record time: the floating terminal at Wilhelmshaven became operational in December 2022, followed in early 2023 by terminals at Lubmin and Brunsbüttel, and by Stade in December 2023. In 2023, gas imports via these LNG terminals totalled approximately 69,656 GWh – around 7% of Germany's total gas imports – underscoring LNG's role as a "safety net" in the transition away from Russian gas (Bundesnetzagentur 2024).

In 2024, Germany's total gas imports declined, amounting to 865,000 GWh. The new context shows that, Norway strengthened its position (48%) ahead of the Netherlands (25%) and Belgium (18%); LNG inflows totalled 69,000 GWh (≈8%) via terminals in Wilhelmshaven, Brunsbüttel, Lubmin and Mukran, confirming LNG's consolidation as a structural backstop rather than a short-term emergency measure (Bundesnetzagentur 2025). In 2025, imports increased to 1,031 TWh, with the same supplier triad remaining dominant – Norway (44%), the Netherlands (24%) and Belgium (21%) – while LNG rose to 106 TWh (10.3%), reinforcing the shift toward an LNG-and-hub-based supply architecture (Bundesnetzagentur 2026).

On the demand side, Germany also achieved a substantial adjustment in consumption: in 2023, German gas use was approximately 17.5% below the 2018-2021 average. From an energy-security perspective, this reduction lowers the country's exposure to potential supply disruptions; from an economic perspective, however, it raises questions about the impact on energy-intensive industrial sectors - specifically, whether lower gas consumption reflected reduced output in these industries and what long-term costs such an adjustment may entail.[1]

Poland and Lithuania – rapid exit from Russian gas through infrastructure and political decision-making

Poland illustrates a case in which political will and infrastructural planning aligned effectively under crisis conditions. In 2022, amid contractual tensions with Gazprom (Plucinska and Strzelecki 2022) and the imminent risk of supply disruptions, Polish authorities accelerated measures to eliminate Russian gas (Polish Governement 2022), redirecting the country towards alternative sources and strengthening energy security through diversified supply routes. A key enabler for the wider region (Central and Eastern Europe) was the development of infrastructure that ensured access to alternative sources and to the North European/Atlantic market. In the logic of REPowerEU, projects such as the Baltic Pipe (linking Denmark and Poland) and the Gas Interconnection Poland-Lithuania (GIPL) are highlighted as investments that enhance connectivity and source diversification, thereby reducing the risks associated with dependence on a single dominant supplier (European Commission 2022, 11-12).

Lithuania also provides a striking example of near-complete dependence reduction through LNG. In April 2022, Lithuania announced that it would cease all imports of Russian gas for domestic

[1] *Ibidem*.

consumption, relying instead on its own LNG import terminal at Klaipėda. From an energy-security perspective, the case demonstrates how a strategic investment in LNG import capacity can rapidly eliminate a major geopolitical vulnerability (Lithuanian Government 2024).

The broader regional takeaway from Poland and the Baltic States is that the development of adequate infrastructure – both LNG terminals and gas interconnections -expands supply options and reduces the scope for coercion by a monopolistic supplier. At the same time, these solutions often involve high upfront costs and require coordination with neighbouring markets in order to function optimally, particularly in terms of cross-border flows, capacity allocation, and the harmonisation of market rules.

Italy – "portofolio diversification" strategy

Italy pursued an energy-security strategy centred on maximising the use of its existing import infrastructure and expanding cooperation with alternative suppliers in the Mediterranean. A salient example is the agreement signed in April 2022 between the Italian company Eni and Algeria's Sonatrach to increase natural gas deliveries through the Transmed pipeline, with a gradual additional volume of up to 9 bcm per year in 2023-2024 (Eni 2022a). From an energy-security perspective, the principal advantage of this approach lies in its speed of implementation: leveraging an existing transport route such as Transmed enables a relatively rapid increase in imports, compared to the longer timelines required for building entirely new infrastructure. At the same time, the strategy entails the risk that dependence is merely shifted to another supplier, making long-term success contingent on Algeria's political stability and production capacity.

Italy's post-2022 gas diversification should not be read as a one-for-one "Russia for Algeria" substitution only. Alongside higher Algerian pipeline and LNG inflows, Rome also leaned on other Mediterranean vectors, notably Libya (pipeline) and Egypt (LNG). On the pipeline side, Libya remains a structural option via Greenstream, even if actual flows have been volatile: ARERA/MASE data show Italian gross imports from Libya declining from 2.5 bcm (2023) to 1.4 bcm (2024, pre-final), highlighting the *political-security risk premium* attached to this corridor (ARERA 2025, 62; Honoré 2023, 3-4). On the LNG side, Italy sought to mobilise Egyptian LNG through upstream and liquefaction-linked arrangements. Eni and EGAS agreed in April 2022 to maximise Egyptian gas production and LNG exports, explicitly aiming to support deliveries to Europe "and specifically to Italy," with LNG cargoes in Eni's portfolio "bound to Europe and Italy" for volumes up to ~3 bcm in 2022 (Eni 2022b). A complementary Mediterranean hedge was the effort to underpin future Libyan export availability through new upstream investment - Eni and Libya's NOC launched the "Structures A&E" project (January 2023), framed as increasing gas for Libya and "to ensure export to Europe", with Italy as the most proximate outlet (Eni 2023).

Accordingly, Italy – much like the EU as a whole – has pursued "portfolio diversification", seeking to avoid a one-for-one substitution of one dominant supplier with another and instead to distribute risk across multiple import sources.

South-Eastern Europe – interconnections and LNG access to reduce historically rooted vulnerability

In South-Eastern Europe, reducing dependence on Russian gas depends to a large extent on improving regional connectivity. A flagship project in this regard is the Greece–Bulgaria Interconnector (IGB), designed to diversify supply by providing access to Azerbaijani gas and to LNG imported via Greece. IGB was conceived with an initial capacity of approximately 3 bcm per year (with the possibility of a subsequent expansion to around 5 bcm per year) and represents an important step toward deeper integration of gas markets in South-Eastern Europe (ICGB 2025). In addition, regional FSRU terminals (floating storage and regasification units), such as the project at Alexandroupolis, Greece, are viewed as critical infrastructure for the region because they create alternative entry points for natural gas into countries with limited pipeline-based supply options (Gastrade 2025a); the broader strategic rationale is the continuous increase – within infrastructural

constraints – of the volumes processed and transported (Gastrade 2025b). From an energy-security standpoint, such terminals enhance system redundancy and reduce disruption risk by diversifying available import routes and sources.

Romania started from a relatively favourable position, with net imports around 16% in 2021. However, this came with a structural vulnerability: more than 75% of those imports originated from the Russian Federation (Romanian Government 2023). Nevertheless, in the post-2022 context Romania explicitly frames the reduction of dependence on Russia in terms of diversification, interconnections, and prospective flows from the Black Sea (Transgaz 2020). In present, Romania imports natural gas from Western Europe via Szeged-Arad interconnector and from Southern Europe through the interconnection points with Bulgaria - Kardam1-Negru Voda1 (Trans-Balkan Corridor) and Giurgiu-Ruse (Romanian Government 2024). In the medium and long term, however, the principal "game changer" is Neptun Deep (OMV Petrom–Romgaz): an investment of up to EUR 4 billion, with recoverable volumes estimated at approximately 100 bcm and first production expected in 2027. The project is presented as a "reliable and secure" source for the region and as a factor that would strengthen energy security by reducing the need for imports (OMV 2023).

Overall, the case studies demonstrate that reducing dependence on Russian energy has been achievable through different combinations of supply diversification (LNG and alternative pipeline routes), demand reduction, and investment in interconnections; yet, resilience remains regionally uneven - especially in South-Eastern Europe (including Romania), where energy security depends decisively on connectivity and on new domestic sources such as the Black Sea.

4. Internal Challenges

Although the EU has substantially reduced its energy dependence on Russia, progress is slowed by a small number of member states that remain structurally tied to Russian imports (gas and oil) and to the nuclear supply chain (technology and fuel-cycle services). This creates tensions around solidarity and complicates the implementation of the objective of phasing out Russian energy imports. In addition, the process is hindered by certain transactions that allow hydrocarbons of Russian origin to enter the EU indirectly via intermediaries, swaps[2], or hub-based trading arrangements.[3]

a) From Policy to Implementation: Hungary and Slovakia and the Final Stage of EU Decoupling

Hungary has not only maintained but in fact increased its imports of Russian gas via the TurkStream pipeline. Reuters reports that imports reached approximately 8 bcm in 2025, up from around 6 bcm in 2023, a trajectory underpinned by southern-route infrastructure and the continued reliance on long-term contracting – developments that are likely to slow the EU's decoupling from Russian gas and to generate security-relevant vulnerabilities (Martin Vladimirov 2025). At the declaratory and contractual level, Hungary reinforced this relationship through a 15-year agreement signed in 2021 (4.5 bcm per year); imports were subsequently expanded to roughly 7.5 bcm via TurkStream (with additional volumes routed through the region) in 2024–2025, indicating persistent dependence even during the period of EU-Russia decoupling (Reuters 2025a). Moreover, Prime Minister Viktor Orbán has sought to persuade Ukraine to keep in place the transit arrangements that allow Russian gas crossing Ukrainian territory to reach Hungary (Reuters 2024).

In the oil sector, Hungary's dependence is amplified by exemptions applicable to landlocked states and by the role of the Druzhba pipeline: Hungary's foreign minister indicated that "about 80%" of crude oil imports came from Russia in 2022, helping to explain Budapest's political resistance to

[2] Arrangements through which two traders/companies "swap" between them the delivery right (or ownership) over the same quantity of gas/oil, but at different points in the network, in order to avoid unnecessary physical transportation.
[3] If a buyer purchases gas "at the hub" (i.e., a blended pool of supplies), it may be difficult to determine what share originates in Russia in the absence of clear reporting rules, because the hub aggregates volumes from multiple routes and contracts.

accelerated phase-out measures (Reuters 2023). Furthermore, analytical estimates suggest dependence rose to ~86% în 2024 (Isaac Levi et al. 2025, 3-4, 8-10).

In 2025, Hungary's exposure to Russian crude increased in volume terms, as Russian government data reported 4.78 million tonnes delivered via Druzhba in 2024, while Hungary's foreign minister said Russia would export 5.0-5.5 million tonnes in 2025 – which, against the IMF-cited 86% Russian-oil share in 2024 (International Monetary Fund 2025, 2), implying total crude imports of ~5.56 million tonnes, suggests a 2025 Russian share of roughly ~90% if overall import volumes remained comparable (Komuves 2025, Astakhova and Soldatkin 2025).

In the nuclear domain, the challenge is one of long-term structural dependence: the Paks II project involves Russian participation (Rosatom) and associated financing, and the EU's top court has criticised the manner in which the approval framework was handled, underscoring the dossier's legal and political sensitivity (Reuters 2025b). Even though steps toward nuclear-fuel diversification have been taken - most notably a contract with the French company Framatome to supply fuel to the Paks reactors starting in 2027 – the nature of the infrastructure and ongoing projects means that full decoupling is likely to proceed more slowly than in other member states (World Nuclear News 2024).

Slovakia remains highly exposed in terms of gas imports, as it receives the "majority" of its gas from Gazprom under a long-term contract running until 2034 for approximately 3.5 bcm per year; following the termination of transit via Ukraine at the end of 2024, Slovakia began receiving volumes through TurkStream, via Hungary (Reuters 2025c). This dependence is also evident in logistical adjustments: in 2025, Slovakia's state-controlled gas importer Slovenský plynárenský priemysel reported that Gazprom would raise deliveries to Slovakia routed via TurkStream to "several times" the volumes shipped in the preceding two months (with no absolute volumes disclosed), enabled by capacity reallocations and flows facilitated by Hungary – an evolution that points to a reconfiguration of routes rather than an elimination of the underlying source (Reuters 2025d).

Quantitatively, the post-Ukraine rerouting is not merely symbolic. By early September 2025, Slovakia had already imported around 1.7 bcm via Hungary – its most direct link to the TurkStream corridor - based on data from the Slovak transmission operator Eustream as reported by Reuters; this scale is material relative to the ~3.5 bcm/year long-term contractual baseline and suggests that the southern route can cover a substantial share of Slovak needs even in the absence of Ukrainian transit (Reuters 2025e). At the operational level, early-2025 nominations underscore the rapid stabilisation of this corridor: shortly after the Ukraine route stopped, daily inflows from Hungary into Slovakia reached 87 GWh/day, the highest since the start of January, indicating that replacement flows were being re-established through the Hungary-Slovakia interconnection (Lopatka 2025). Importantly, the route is also being structurally "locked in" through capacity upgrades: a project is under way to raise cross-border capacity from 3.5 bcm to 4.4 bcm, increasing the system's ability to accommodate Russian-origin volumes entering via TurkStream (Reuters 2025e).

In the oil sector, Slovakia - like Hungary - remains tied to the Druzhba pipeline and has benefited from derogations intended to facilitate a gradual transition, thereby preserving a "hard core" of residual Russian dependence within the EU (Gizińska and Wankiewicz-Kłoczko 2024). A key difference from Hungary, however, is that Slovakia has taken more explicit steps in the nuclear domain, lowering the risk of long-term technological dependence. Slovenské elektrárne, the country's largest electricity producer, concluded agreements for alternative VVER-440 nuclear fuel with the U.S. company Westinghouse (2023) and with Framatome (2024), with deliveries planned from 2027 (Slovenské elektrárne 2023) is an approach that reflects a structured substitution strategy encompassing testing, licensing, and contracting (Slovenské elektrárne 2024).

From an EU perspective, Hungary and Slovakia constitute an internal challenge not only in technical terms but also politically. Budapest and Bratislava have invoked economic costs and risks to oppose certain sanctions packages and/or efforts to accelerate decoupling, a stance that can slow down - or fragment - the implementation of common measures (Reuters 2025f).

b) Security Risk: "Disguised" Purchases of Russian Gas and Hydrocarbons via Intermediaries

Even as direct imports decline, the EU faces the risk that gas or hydrocarbons of Russian origin may still enter the market indirectly – via intermediaries, swaps, or hub-based transactions – thereby sustaining revenue flows to the Kremlin and weakening the effectiveness of decoupling policies. The gas market provides a clear illustration. The European Commission notes that in 2024 the EU still imported 52 bcm of Russian gas, including LNG, and that some member states may be supplied indirectly through wholesale market purchases; hence the growing policy emphasis on transparency, monitoring, and traceability (European Commission 2025a).

In oil and refined products, a recurrent circumvention pattern involves processing Russian-origin crude in third countries and then exporting the resulting fuels to the EU as ostensibly "non-Russian" commodities; within this architecture, so-called "ghost tankers" – often associated with the "shadow fleet" – can reinforce opacity in upstream logistics and provenance attribution, thereby complicating traceability before refining and enabling subsequent re-entry of refined outputs into EU markets. To curb such practices, the EU has issued prohibitions and compliance guidance that place the burden on importers to furnish documentary evidence and robust due-diligence demonstrating that Russian crude was not used in the refining chain for imported products (European Commission 2025b, 1-2).

In energy-security terms, circumvention through intermediaries has three principal effects: (1) it undermines the EU's strategic objectives by sustaining a de facto dependence; (2) it distorts progress indicators by rendering true origin opaque; and (3) it generates legal and reputational risks for importers. For these reasons, traceability – through origin certification, auditing, and customs cooperation – becomes an indispensable component of any credible policy to phase out Russian energy imports.

Conclusions and Recommendations

Building on the research question - namely, to what extent and through which mechanisms the European Union succeeded in reducing its dependence on energy resources from the Russian Federation between 2022 and 2025, and what new vulnerabilities emerged as a result - the findings indicate that decoupling was real, rapid, and, as a strategic direction, quasi-irreversible. However, selective re-coupling cannot be ruled out if political constraints loosen and price incentives re-emerge. The critical inflection point was 2022: the Russian Federation's military intervention in Ukraine reframed energy from a predominantly economic issue into a matter of security, accelerating decisions that, under the pre-2022 logic, would likely have unfolded far more slowly. Put differently, 2022 functioned as a systemic shock that compressed political timelines and generated the consensus required for exceptional measures at both EU and member-state levels.

With respect to the stated hypothesis – that post-2022 policies reduced structural dependence on Russia and constrained its capacity for energy coercion, while transferring part of the risk to LNG, critical infrastructure, and the industrial supply chains underpinning the transition – the analysis broadly confirms it. Dependence on Russia declined across the main segments, and the geopolitical leverage exercised through energy was substantially weakened. Yet risk did not disappear; it was reconfigured. Today's vulnerabilities are less concentrated in a single actor and more dispersed throughout the system – manifesting in global market volatility, infrastructural constraints, and institutional capacity to manage overlapping crises.

In terms of mechanisms, decoupling operated through a mutually reinforcing policy mix: demand reduction, supply diversification, storage management, and EU-level coordination. The core conclusion is that no single instrument would have sufficed; effectiveness stemmed precisely from the EU acting simultaneously on "need" (demand), "source" (supply), and "buffer" (storage), in parallel with the strengthening of common governance. Against this background, member states adjusted at different speeds depending on infrastructure, geography, and strategic culture: where LNG

terminals, interconnections, and industrial flexibility were available, adaptation was faster; where systems were rigid and dependent on a single route, the transition proved more costly and slower.

The case studies also support a second key conclusion: decoupling is not merely a technical process, but a political one. The persistence of dependencies in certain member states can generate internal frictions and slow the Union's strategic convergence. In particular, multi-layered dependencies (gas, oil, nuclear) raise the complexity of decision-making and increase the temptation of derogations, potentially turning decoupling into a "multi-speed" process. At the same time, these cases demonstrate that diversification is feasible, but it requires time, planning, and administrative capacity – especially where energy infrastructure is inherited from earlier decades.

Finally, the answer to the second part of the research question – new vulnerabilities -points to two broad directions. The first concerns market and economic exposure: reliance on hubs, LNG, and intensified global competition can generate volatility and exert pressure on industrial competitiveness. The second concerns governance and traceability: as direct imports decline, the significance of circumvention risk via intermediaries grows, alongside the difficulty of tracking origin in integrated markets. In energy-security terms, "decoupling" is not simply about switching suppliers; it also entails the capacity to verify, control, and manage the entire supply chain in a complex operating environment.

Accordingly, the overarching conclusion is twofold. On the one hand, the EU has demonstrated an ability to respond coherently and rapidly when energy is treated as a security issue, with 2022 acting as the decisive catalyst for this strategic shift. On the other hand, the success of decoupling generates a new set of challenges. Energy security becomes less a matter of "dependence on the Russian Federation" and more a question of resilience in an era shaped by global markets, critical infrastructure constraints, and technological transition. The next stage, therefore, is not only to maintain the trajectory of decoupling, but also to strengthen the EU's capacity to manage emerging risks without undermining internal cohesion, competitiveness, or the objectives of the energy transition.

BIBLIOGRAPHY:

ARERA, 2025, "Relazione Annuale sullo Stato dei Servizi e sull'Attività Svolta nel Corso del 2024", Accessed January 29, 2026. https://www.arera.it/fileadmin/allegati/relaz_ann/25/Sintesi_Relazione_Annuale_2025_10settembre.pdf. (In-text citation: ARERA 2025, 62).

Astakhova, Olesya, and Soldatkin, Vladimir. 2025. "Hungary attacks EU energy policy at Moscow conference", Reuters, October 15, accessed January 29, 2026. https://www.reuters.com/business/energy/hungary-attacks-eu-energy-policy-moscow-conference-2025-10-15/.(In-text citation: Astakhova and Soldatkin 2025).

Bundesnetzagentur. 2024. "Bundesnetzagentur Publishes Gas Supply Figures for 2023." January 4. Accessed December 19, 2025, https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2024/20240104_Gasversorgung2023.html. (In-text citation: Bundesnetzagentur 2024).

Bundesnetzagentur. 2025. "Bundesnetzagentur publishes gas supply figures for 2024." January 8. Accessed February 6, 2026. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2025/20250108_GAS.html. (In-text citation: Bundesnetzagentur 2025).

Bundesnetzagentur. 2026. "Bundesnetzagentur publishes gas supply figures for 2025". January 12, accessed February 6, 2026, https://www.bundesnetzagentur.de/SharedDocs/Pressemittei lungen/EN/2026/20260112_GAS.html?nn=694186. (In-text citation: Bundesnetzagentur 2026).

Cherp, Aleh, and Jewell, Jessica. 2025. "The Concept of Energy Security: Beyond the Four As". *Energy Policy* 75 (2014): 415-421. accessed December 16. https://doi.org/10.1016/j.enpol. 2014. 09.005. (In-text citation: Cherp and Jewell 2025, 415-421).

Council of the European Union. 2022. "Council Regulation (EU) 2022/1369 of 5 August 2022 on coordinated demand-reduction measures for gas". August 8. Accessed December 18, 2025. https://eur-lex.europa.eu/eli/reg/2022/1369/oj/eng. (In-text citation: Council of the European Union 2022).

Council of the European Union. 2025a. "Where Does the EU's Gas Come From?". November 13, accessed December 17, 2025. https://www.consilium.europa.eu/en/infographics/where-does-the-eu-s-gas-come-from/. (In-text citation: Council of the European Union 2025a).

Council of the European Union. 2025b. "Council and Parliament Strike a Deal on Rules to Phase Out Russian Gas Imports for an Energy Secure and Independent Europe." December 3. Accessed December 18, 2025. https://www.consilium.europa.eu/en/press/press-releases/2025/12/03/council-and-parliament-strike-a-deal-on-rules-to-phase-out-russian-gas-imports-for-an-energy-secure-and-independent-europe/. (In-text citation: Council of the European Union 2025b).

Eni. 2022a. "Eni and Sonatrach Agree to Increase Gas Supplies from Algeria through Transmed". April 11. Accessed December 21, 2025. https://www.eni.com/en-IT/media/press-release/2022/04/eni-and-sonatrach-agree-to-increase-gas-supplies-from-algeria-through-transmed.html. (In-text citation: Eni 2022).

Eni. 2022b. "Eni and EGAS agree to increase Egypt's gas production and supply" April 13, Accessed January 29, 2026. Available at: https://www.eni.com/en-IT/media/press-release/2022/04/eni-and-egas-agree-increase-egypt-s-gas-production-and-supply.html. (In-text citation: Eni 2023).

Eni. 2023. "Eni launches a major gas development project in Libya", January 28, Accessed January 29, 2026. https://www.eni.com/en-IT/media/press-release/2023/01/eni-launches-a-major-gas-development-project-in-libya.html. (In-text citation: Eni 2023).

European Commission. 2015. "A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy". Brussels, February 25. Accessed February 6, 2026. https://data.consilium.europa.eu/doc/document/ST-6594-2015-INIT/en/pdf. (In-text citation: European Commission 2015).

European Commission. 2022. "REPowerEU Plan. COM(2022) 230 final". Brussels, May 18. Accessed December 16, 2025, https://eur-lex.europa.eu/resource.html?format=PDF&uri=cellar% 3Af c930f14-d7ae-11ec-a95f-01aa75ed71a1.0001.02%2FDOC_1. (In-text citation: European Commission 2022).

European Commission. 2025a. "Roadmap towards Ending Russian Energy Imports." Brussels, May 6. Accessed January 8, 2026. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0440. (In-text citation: European Commission 2025a).

European Commission. 2025b. "Import Ban on Refined Products Obtained from Russian Crude Oil". October 16. Accessed January 9, 2026. https://finance.ec.europa.eu/document/download/dc76791c-72aa-4fd5-b82f-ae13a42e93c0_en?filename=faqs-sanctions-russia-oil-import-ban_en.pdf. (In-text citation: European Commission 2025b).

European Union. 2017. "Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 on measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010", Accessed December 16, 2025. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02017R1938-20250101. (In-text citation: European Union 2017).

Gastrade. 2025a, "The Project (FSRU Alexandroupolis)." Accessed December 22, 2025, https://www.gastrade.gr/en/the-project/. (In-text citation: Gastrasde 2025a).

Gastrade. 2025b. "Further Increase in Maximum Regasification Capacity." October 21, 2025. Accessed January 5, 2026. https://www.gastrade.gr/en/2025/10/21/further-increase-in-maximum-regasification-capacity/. (In-text citation: Gastrasde 2025b).

Gizińska, Ilona, and Wankiewicz-Kłoczko, Paulina. 2024. "Better from Russia than via Croatia? The Future of Oil Supplies to Hungary and Slovakia," OSW, September 9, accessed January 1, 2026, https://www.osw.waw.pl/en/publikacje/analyses/2024-09-09/better-russia-via-croatia-future-oil-supplies-to-hungary-and. (In-text citation: Gizińska and Wankiewicz-Kłoczko 2023).

Honoré, Anouk. 2023. "Italy and its North African Gas Interconnections: A Potential New Mid-Mediterranean Gas Hub", Oxford Institute for Energy Studies, March, 3-4, Accessed January 29, 2026. https://www.oxfordenergy.org/wpcms/wp-content/uploads/2023/03/Italy-and-its-North-African-gas-interconnections.pdf (In-text citation: Honoré 3-4).

ICGB. 2025. “ICGB Launches Market Demand Assessment for Capacity Expansion of the IGB Pipeline.” July 7, Accessed December 22, 2025. https://www.icgb.eu/news/icgb-launches-market-demand-assessment-for-capacity-expansion-of-the-igb-pipeline/. (In-text citation: ICGB 2025).

International Monetary Fund. 2025. “Hungary: Selected Issues, IMF Country Report No. 25/251”. July 25. p. 2. Accessed January 29, 2026. https://www.imf.org/-/media/files/publications/cr/2025/english/1hunea2025002-source-pdf.pdf. (In text citation: IMF 2025, 2).

Isaac Levi et al. 2025. “The Last Mile: Phasing Out Russian Oil and Gas in Central Europe. Center for the Study of Democracy and Centre for Research on Energy and Clean Air”, May, 3–4, 8–10, Accessed January 4, 2026, https://energyandcleanair.org/wp/wp-content/uploads/2025/05/CSD_CREA_HU_SK_05_25.pdf. (In-text citation: Isaac Levi et. al. 2025, 3-4, 8-10).

Komuves, Anita. 2025. “Russian oil flows to Hungary and Slovakia halted after Ukrainian attack,” Reuters, August 18, accessed January 29, 2026. https://www.reuters.com/business/energy/russian-oil-flows-hungary-slovakia-halted-after-ukrainian-attack-2025-08-18/. (In-text citation: Astakhova and Soldatkin 2025).

Lithuanian Government. 2024. “Lithuania Completely Abandons Russian Gas Imports.” April 2. Accessed December 21, 2025. https://enmin.lrv.lt/en/news/lithuania-completely-abandons-russian-gas-imports/. (In-text citation: Lithuanian Government 2024).

Lopatka, Jan. 2025. “Central Europe gas flows adjusted after Ukraine transit ends,” Reuters, January 6, accessed January 29, 2026. https://www.reuters.com/business/energy/central-europe-gas-flows-adjusted-after-ukraine-transit-ends-2025-01-06/. (In-text citation: Lopatka 2025).

OMV. 2023. “OMV Announces Final Investment Decision Taken by OMV Petrom for Natural Gas Deep-Water Project Neptun Deep.” June 21. Accessed December 22, 2025. https://www.omv.com/en/media/press-releases/2023/230621-omv-announces-final-investment-decision-taken-by-omv-petrom-for-natural-gas-deep-water-project-neptun-deep. (In-text citation: OMV 2023).

Plucinska, Joanna, and Strzelecki, Marek, 2022. “Russia Warns Poland, Bulgaria of Gas Supply Cuts on Wednesday.” Reuters, April 26. Accessed December 21, 2025. https://www.reuters.com/world/europe/russian-gas-supplies-poland-halted-polish-media-reports-2022-04-26/. (In-text citation: Plucinska and Strzelecki 2022).

Polish Government. 2022. “Poland Terminated the Gas Agreement on the Yamal Gas Pipeline.” May 27. Accessed December 21, 2025. https://www.gov.pl/web/climate/poland-terminated-the-gas-agreement-on-the-yamal-gas-pipeline. (In-text citation: Polish Government 2022).

Reuters. 2023. “Hungary Agrees on Option for More Russian Gas Shipments, Oil Transit Fees.” Reuters, April 11. Accessed December 24, 2025. https://www.reuters.com/business/energy/hungary-agrees-option-more-russian-gas-shipments-oil-transit-fees-2023-04-11/. (In-text citation: Reuters 2023).

Reuters. 2024 “Hungary in Talks on Russian Gas Shipments via Ukraine, PM Orban Says.” Reuters, December 21, Accessed December 23, 2025. https://www.reuters.com/business/energy/hungary-talks-russian-gas-shipments-via-ukraine-pm-orban-says-2024-12-21/. (In-text citation: Reuters 2024).

Reuters. 2025a. “Turkey to Guarantee Flow of Russian Gas to Hungary, Orban Says.” Reuters, December 8. Accessed December 23, 2025. https://www.reuters.com/business/energy/turkey-guarantee-flow-russian-gas-hungary-orban-says-2025-12-08/. (In-text citation: Reuters 2025a).

Reuters. 2025b. “EU’s Top Court Rules against Hungary’s Nuclear State Aid.” Reuters, September 11, Accessed December 24, 2025. https://www.reuters.com/business/energy/eus-top-court-rules-against-hungarys-nuclear-state-aid-2025-09-11/. (In-text citation: Reuters 2025b).

Reuters. 2025c. “Slovakia Aims for Agreement by Tuesday on End of Russian Gas Supplies, Sanctions.” Reuters, July 12. Accessed January 2, 2026. https://www.reuters.com/business/energy/slovakia-aims-agreement-by-tuesday-end-russian-gas-supplies-sanctions-2025-07-12/. (In-text citation: Reuters 2025c).

Reuters. 2025d. "Gazprom to increase gas supplies through TurkStream from April, Slovak SPP says." Reuters, March 31, 2025. Accessed January 31, 2026. https://www.reuters.com/business/energy/gazprom-increase-gas-supplies-through-turkstream-april-slovak-spp-says-2025-03-31/. (In-text citation: Reuters 2025d).

Reuters. 2025e. "Slovakia wants to normalise relations with Russia, ramping up gas imports, PM Fico says," Reuters, September 2, Accessed January 29, 2026. Available at: https://www.reuters.com/business/energy/slovakia-wants-normalise-relations-with-russia-ramping-up-gas-imports-pm-fico-2025-09-02/. (In-text citation: Reuters 2025e).

Reuters. 2025f. "Hungary and Slovakia Block Russian Sanctions Package, Budapest Says." Reuters, June 23. Accessed January 6, 2026. https://www.reuters.com/business/energy/hungary-slovakia-block-russian-sanctions-package-budapest-says-2025-06-23/. (In-text citation: Reuters 2025f).

Romanian Government. 2023. "Draft Updated Integrated National Energy and Climate Plan (NECP) 2021-2030". 2023. Accessed December 22, 2025. https://commission.europa.eu/system/files/2023-11/ROMANIA%20-%20DRAFT%20UPDATED%20NECP%202021-2030.pdf. (In-text citation: Romanian Government 2024).

Romanian Government. 2024. "Strategia energetică din 21 noiembrie 2024 a României 2025-2035, cu perspectiva anului 2050". Portal Legislativ, Accessed February 6, 2026, https://legislatie.just.ro/Public/DetaliiDocumentAfis/293734. (In text citation: Romanian Government 2024).

Slovenské elektrárne. 2023. "Strengthening Slovakia's Energy Security: Slovenské elektrárne Concluded a Fuel Supply Agreement with Westinghouse." August 25. Accessed January 3, 2026. https://www.seas.sk/en/press-releases/slovenske-elektrarne-nuclear-fuel-westinghouse/. (In-text citation: Slovenské elektrárne 2023).

Slovenské elektrárne. 2024. "Nuclear Fuel Supply Agreement with Framatome.", July 23. Accessed January 3, 2026. https://www.seas.sk/en/press-releases/slovenske-elektrarne-framatome-nuclear-fuel-contract/. (In-text citation: Slovenské elektrárne 2024).

Transgaz. 2020. "Consolidated Report Issued by the Board of Administration". December 31, Accessed December 22, 2025. https://www.transgaz.ro/sites/default/files/Art.3% 20engleza_8.pdf. (In-text citation: Transgaz 2020).

Vladimirov, Martin. 2025. "TurkStream Gas Pipeline Could Slow EU, Russia Decoupling." May 7, 2025. Accessed January 5, 2026. https://www.reuters.com/business/energy/turkstream-gas-pipeline-could-slow-eu-russia-decoupling-vladimirov-2025-05-07/. (In-text citation: Vladimirov 2025).

World Nuclear News. 2024. "Framatome to Supply Hungarian Plant with Nuclear Fuel." October 28, Accessed January 2, 2026. https://www.world-nuclear-news.org/articles/framatome-to-supply-hungarian-plant-with-nuclear-fuel. (In-text citation: World Nuclear News 2024).

DOI: 10.53477/3045-2309-26-04

PROMOTING STRATEGIC THINKING AND ITS CONTRIBUTION TO STRENGTHENING REGIONAL SECURITY

Lucian Valeriu SCIPANOV, PhD,
Captain (OF-5), Professor, "Carol I" National Defence University, Bucharest, Romania,
E-mail: shcipio@yahoo.com

Bogdan Daniel IOSIF
Commander (OF-4), PhD Candidate, "Carol I" National Defence University, Bucharest,
Chief of Staff, 50th Corvette Squadron, Constanța, Romania,
E-mail: bogdan.iosif@navy.ro

Abstract: *The paper draws the attention of military leaders to their role in contributing to the strengthening of regional security. The authors identify the need to develop the strategic thinking of future military leaders in the context of the geopolitical, technological, and social transformations shaping the regional security environment, with the aim of fostering a school of thought adapted to these changes. Against the backdrop of an increasingly unstable security environment and emerging challenges, such as security risks and hybrid threats, the necessity of shaping resilient military leader profiles becomes evident, capable of thinking and acting strategically from the earliest levels of command. The study includes an analysis of the regional security environment and examines ways to promote critical thinking based on leadership models advanced by the Black Sea littoral actors, in order to formulate recommendations for the effective integration of strategic thinking into the military system of continuing education, thereby contributing to the development of future military leaders.*

Keywords: *regional security; strategic thinking; soft capability; leadership; resilience.*

Introduction

Over the past decade, the security environment in the Black Sea region has undergone profound transformations, driven by the overlap of the strategic interests of littoral states, regional actors, and great powers, as well as by the intensification of geopolitical competition in proximity to the Eastern flank of the Euro-Atlantic area. The events initiated by the Russian Federation, culminating in the war of aggression against Ukraine beginning on 24 February 2022, have produced a major rupture in the European security architecture and have amplified vulnerabilities related to maritime, energy, commercial, and food security. In this context, the Black Sea can no longer be analysed exclusively as a regional space, but rather as a strategic node with direct relevance for global stability and security, where risks and threats manifest simultaneously across multiple domains.

Against this backdrop, the response of Euro-Atlantic actors has been characterised by cohesion, adaptability, and the expansion of the politico-military toolkit designed for deterrence and collective defence. Beyond structural and operational measures, such as the deployment of multinational capabilities, the strengthening of interoperability, and the maintenance of a credible naval presence, the determining role of the conceptual dimension of security has become increasingly evident. Strategies, doctrines, operational concepts, as well as the use of soft instruments, including naval diplomacy, reflect the outcomes of strategic thinking processes aimed at integrating available means with long-term political objectives and with the specific features of the Black Sea operational environment.

Within this framework, the paper seeks to analyse the relationship between the regional security environment, the leadership models promoted by the principal littoral actors, and the role of

strategic thinking as the foundation of the politico-military decision-making process. The approach is structured around three main directions: defining the regional security environment and its associated risks, identifying the dominant leadership models manifested in the Black Sea region, and examining strategic thinking as an essential cognitive and organisational capability for managing contemporary conflicts. Through this integrated approach, the study aims to highlight the necessity of the deliberate development of strategic thinking among future military leaders, as an adaptive response to the complexity and unpredictability of the regional security environment.

1. Defining the Regional Security Environment

The Black Sea region, by virtue of its geographical configuration and strategic relevance, constitutes a complex security space characterised by the overlapping interests of littoral states, regional partners, and international actors (Popa and Chiorcea 2024). This region goes beyond the status of a sensitive Eastern frontier, functioning instead as an essential strategic hub for the European Union's energy security, trade routes, and food supply chains.

The regional security environment prior to the Russian Federation's invasion of Ukraine could not be considered stable, primarily as a result of Moscow's policy aimed at exploiting and amplifying the effects of frozen conflicts in the Wider Black Sea Region. In this context fall the conflict for the defence of the territorial integrity and sovereignty of the Republic of Moldova (1992), the war in Georgia (2008), as well as the invasion and annexation of the Crimean Peninsula in 2014. Following the annexation of Crimea, the regional security situation deteriorated significantly, against the backdrop of hostile actions conducted in the maritime domain, manifested through the restriction of maritime communications along the Istanbul – Crimea axis and in the Sea of Azov. The construction of the bridge across the Kerch Strait contributed to this strategic imbalance, constituting an additional manifestation of the unilateral alteration of the regional status quo.

Regional security dynamics were further intensified with the unanimous condemnation of the invasion of Ukraine launched by the Russian Federation on 24 February 2022. In this regard, it is relevant to note that as early as the 2021 OSCE Annual Security Conference, the European Union's statement delivered during the session dedicated to ensuring regional security and stability identified a series of threats attributed to the actions of the Russian Federation vis-à-vis Ukraine (EU 2021). These included restrictions on access for commercial vessels, and in particular military vessels, in certain areas of the Black Sea; the extensive militarisation of the Crimean Peninsula; the construction of the bridge over the Kerch Strait without Ukraine's consent; limitations on freedom of navigation to Ukrainian ports; and the significant concentration of military capabilities in proximity to Ukraine's borders.

Following 24 February 2022, these threats materialised as a series of concrete effects, ranging from the westward expansion of the conflict through the occupation of additional territories in Ukraine to its major impact on global food security. This situation led to the launch of the United Nations Initiative on the Export of Grain through the Black Sea, using the maritime solidarity corridors established in 2022 (UNO 2022). The fact that the initiative was guaranteed by the signatory parties, the Russian Federation, Ukraine, and Türkiye, under the auspices of the United Nations, acting as a guarantor of food security, constitutes further evidence of the role and strategic importance of the Black Sea region within the regional and global security architecture.

The position of the allied states has been, and continues to be, characterised by a high degree of cohesion and resolve, reflected within Euro-Atlantic institutions through the activation of a broad spectrum of instruments designed to manage and counter emerging risks and threats. These instruments include both diplomatic measures, such as political dialogue, consultation, and conciliation mechanisms, and military measures, materialised through enhanced cooperation, interoperability, and the maintenance of a credible collective defence capability.

Countering risks requires, in addition to adapting existing instruments enshrined in the Alliance's foundational documents (NATO 1999), the integration of measures appropriate to the current security

environment, which has been profoundly influenced by the conflict in Ukraine. In this context, relevant risks include the expansion of territories occupied by force, the possibility of other geographical areas being targeted, restrictions on access to strategic resources, control over the mouths of rivers flowing into the Black Sea, the establishment of naval blockades and the disruption of maritime commercial flows, as well as other forms of strategic pressure with regional and global impact.

With regard to threats, the collective defence posture is articulated through a coherent set of structural and procedural measures. Structural-organisational measures are reflected in flexible command-and-control arrangements, the deployment of multinational capabilities, and the enhanced forward presence of allied forces on the Eastern flank of the Euro-Atlantic area. Complementarily, procedural measures are implemented through mechanisms of joint operational planning, crisis management, permanent political consultation, standardisation, training through multinational exercises, as well as through ensuring access to infrastructure, the provision of military capabilities, and integrated logistical support.

To reduce the identified risks and to deter or neutralise existing or potential threats, it has become necessary to adapt and expand the spectrum of maritime missions and operations with defensive and deterrent roles. In this regard, a set of measures complementary to the collective effort aims at developing counter-unmanned aerial system capabilities, adapting and integrating short and medium-range missile defence systems, protecting critical infrastructure, ensuring freedom of navigation, securing maritime lines of communication, maintaining energy security, protecting subsea infrastructure, and exercising control over maritime spaces of strategic interest.

Based on recent developments, the Russian Federation can be identified as a direct and significant threat to regional security and stability, through both the strategic objectives it pursues and the means employed to achieve them. Among the most relevant objectives are attempts to establish regional and global spheres of influence, to exercise control over occupied territories, and to maintain coercive influence in areas affected by frozen or active conflicts in the Wider Black Sea Region. Through its aggressive military posture, violations of international law, including maritime law, its coercive rhetoric, and its demonstrated willingness to resort to force in order to achieve political and military objectives, the Russian Federation is perceived as the principal risk factor to individual freedoms, human rights, democracy, and the rule of law, as well as to peace and stability on the Eastern flank of the Euro-Atlantic area, with direct implications for global security.

Without doubt, it can be stated that the regional security environment is currently defined by the war of aggression launched by the Russian Federation against Ukraine, an event that has produced a major rupture in the European security architecture. This action constitutes a serious violation of established norms and practices of international diplomacy, of maritime law, as well as of the fundamental principles of the Charter of the United Nations and of the values underpinning the North Atlantic Alliance.

In this context, the strengthening of regional security requires the adoption and implementation of measures adapted to the specific characteristics of the Black Sea operational environment, namely politico-military measures. Among these are initiatives undertaken by Romania, aimed at reinforcing NATO's deterrence and defence posture, contributing to the establishment of a Recognized Maritime Picture (RMP), developing real-time situational awareness capabilities, and maintaining the rule of law and freedom of navigation. These actions reflect Romania's active role within the regional security architecture and in the collective Euro-Atlantic effort to manage emerging risks.

The authors argue that, alongside measures taken at the strategic and operational levels, action-oriented measures aimed at strengthening the deterrence and defence posture, conceptual measures can also be identified. These include strategies, doctrines, concepts, national resilience, multi-domain integration, interoperability, and diplomacy, among others. Conceptual measures represent the essence and product of the strategic thinking promoted by the authors. Within this approach, strategic thinking defines how modern conflict is addressed and how doctrinal instruments are integrated into the mechanisms of the allied response to threats within the regional security environment. In the authors' view, the driving force behind conceptual measures is the ability of leaders to promote and develop strategic thinking.

2. The dominant leadership model promoted in the Black Sea region

Taking into account the main characteristics of the regional security environment and the manner in which strategic thinking is manifested in the region, the following section analyses the leadership models promoted by the Black Sea littoral actors. Depending on these models, the paper proposes the identification of those components of strategic thinking, such as systems thinking, foresight, ethical reasoning, creativity, and synthesis, that can be demonstrated by future military leaders in order to contribute to the strengthening of regional security through the decisions they will make. This analytical endeavor starts with the statement of the Romanian Chief of the Navy: *"Regional political leaders are the first to perceive threats to the security of the region"* (Panait 2024, 139).

In the authors perspective, the diplomatic instrument is the domain of the strategic thinker and represents the primary means through which regional leadership is asserted in the context of the predominantly maritime profile of the Black Sea region. The conceptual link between strategic thinking and naval diplomacy manifests itself through a dual, complementary approach.

Naval diplomacy represents an applied expression of strategic thinking in the maritime domain, as it entails the alignment of political objectives with the deliberate use of naval means, the coherent integration of the instruments of power – diplomatic, informational, military, and economic - and the anticipation of the behavior of other international actors in order to shape the security environment without resorting to lethal force. Decisions regarding the deployment of naval forces in presence or cooperative missions thus reflect a strategic assessment of the geopolitical context and national interests, aimed at generating long-term political and security effects.

Moreover, naval diplomacy can be understood as a strategic instrument integrated into states' maritime policy, forming part of a broader maritime strategy toolkit. In this regard, Kevin Rowlands (2019) argues that naval diplomacy transcends the traditional dimensions of coercion or mere presence, functioning instead as a strategic activity oriented toward the construction and influence of international relationship networks during peacetime. In a convergent manner, Christian Le Mière (2014) highlights the flexible nature of naval diplomacy as an instrument that combines elements of hard and soft power within contemporary foreign policy, thereby requiring robust strategic thinking for mission planning, risk management, and the integration of other instruments of power. Naval diplomacy "encompasses actions of national representation, as well as a component of diplomacy also referred to as a naval strategy of influence (…) today, naval diplomacy is understood as the use of naval power, a core component of maritime power, to support a state's position in negotiations" (Scipanov 2024, 30). This perspective is further reinforced by Geoffrey Till's (2013) analysis, which emphasises that naval forces should be examined not exclusively as instruments of warfare, but as strategic entities operating at the intersection of diplomacy, security, and influence.

Under these conditions, the authors emphasise that naval diplomacy assumes a central role in the ability of Black Sea littoral actors to manage regional security, while also becoming a key area of focus for future leaders in the development of this strategic skill set. Accordingly, it can be argued that military leadership can contribute to the promotion of security through the effective use of naval diplomacy.

The promotion of leadership among decision-makers and within the professional training of future leaders involves solutions aimed at shaping the profile of future decision-makers, such as multidisciplinary education, personal development, professional training, and the development of emotional intelligence. In this context, regional leadership and naval diplomacy represent "soft" solutions contributing to regional security, alongside defence diplomacy, security culture, and maritime awareness. All of these represent, in the authors' view, means of fostering critical thinking (Scipanov 2024), a fundamental component of strategic thinking.

With regard to the allied approach to regional security, it can be noted that NATO constitutes a pillar of stability in the region and is expected to remain so by responding to challenges related to collective defence, crisis management, and cooperative security (Panait 2024, 149). The type of leadership manifested under these conditions is Collaborative Leadership, or Collective Security

Leadership. The main characteristics of collaborative leadership include shared responsibility (decisions are taken by consensus), interdependence (the success of the Alliance depends on the contributions of its members), and mutual trust (the harmonisation of common interests).

From the perspective of the European Union, the core reference points of security are democracy, the standard of living, and the freedom of the European population and of those living in proximity to the EU's borders. Within the balance of regional security, the European Union remains a guarantor of security in the Black Sea. Under these conditions, the leadership model promoted by the European Union through its policies and community principles is democratic (or participatory) leadership; however, due to its social orientation, influences of transformational leadership can also be identified. The characteristics of democratic leadership are grounded in the will of the people and respect for human rights, participation in the decision-making process, equality before the law, the guarantee of fundamental freedoms, consensus-based cooperation, and open dialogue.

Türkiye has prompted the Euro-Atlantic community to reconsider its security strategies in the Black Sea, particularly from the perspective of the application of the Montreux Convention. In response, the Alliance and the European Union seek to identify appropriate diplomatic, political, and military responses to the real threats posed by the Russian Federation to regional security. Nevertheless, Türkiye remains an important contributor to strengthening the Alliance's position in the region.

The Russian Federation demonstrates through its behavior that it is an unpredictable and irrational actor in the Black Sea region. The mindset of Russian leadership perceives the Black Sea as an area of paramount interest in which its will should be imposed without regard for the positions of the Black Sea littoral actors. An intolerant attitude can be observed toward all littoral actors that seek to defend their interests in the Black Sea region, particularly through the minimisation of the political and military influence of the Euro-Atlantic bloc.

Considering the main models through which leadership is asserted in the context of regional security strategies, the authors propose several leadership models expressed at the strategic, operational, and tactical levels:

- *Integrated Security Leadership* – the leadership of international organisations and major regional actors;
- *Normative–Strategic Leadership* – strategic leadership at the politico-military level;
- *Situational Leadership* – the leadership of commanders at the tactical-operational level.

At the political level, the leadership of international organisations and major regional actors must capitalise on economic opportunities in the Black Sea by identifying mechanisms for exploiting economic resources (hydrocarbons), renewable energy, maritime trade, biological resources, and tourism, within the framework of restoring the balance of regional security. The authors define this type of leadership as *Integrated Security Leadership*, characteried by geostrategic vision, a comprehensive approach, strategic resilience, and regional cooperation.

At the strategic (politico-military) level, regional leadership must leverage and promote European values and, when opportunities arise, facilitate the transformation and adaptation of the European Union's command-and-control structure to the regional security situation in relation to imminent threats and risks. Equally important is the adaptation of existing European capabilities and the development of new capabilities capable of responding to the threats of the regional security environment. The authors consider this model to be transformational in nature and refer to it as *Normative–Strategic Leadership*.

At the tactical-operational level, leadership specific to senior commanders must be manifested in understanding security risks and in making decisions that support the politico-military decisions taken at the strategic level, as well as the intent of commanders at the operational level. The authors draw on research findings indicating that "in the military system, leaders predominantly adopt behaviors and attitudes specific to transformational leadership, with some presence of those related to transactional and laissez-faire leadership, but to a lesser extent" (Cioranu, Cucinschi and Scipanov 2024, 509-541). Considering the transformational nature of leadership with transactional influences,

the authors argue that the promotion of strategic thinking among future leaders should be grounded in these dominant forms of leadership. The symbiosis between the two leadership models (transformational and transactional) is situational in nature and represents the ideal balance between vision and execution. At the tactical level, the effect of this symbiosis is increased tactical flexibility, whereby the leader employs the transformational dimension to strengthen group culture under conditions of resilience, while also engaging the transactional dimension to manage resources and comply with constraints under conditions of efficiency. The analysis concludes with a proposed introspection into strategic thinking in relation to the promoted regional leadership models and the regional security framework.

3. Promoting Strategic Thinking

Strategic thinking is distinct from, yet interconnected with, strategic, operational, and tactical reasoning. Tactics address immediate actions, while operations focus on campaigns and combat actions at the level of the theatre of operations. These are the elements that put strategy into motion. Strategy represents a long-term plan of action designed to achieve the purpose of an undertaking, for which specific objectives are established at the operational and tactical levels.

Starting from the premise that strategic thinking refers to the alignment of military activity with national security policy and long-term objectives (Gray 2010), and taking into account the intrinsic link between the strategic, operational, and tactical levels, it can be stated that strategic thinking may also be applied at the operational and tactical levels. In this sense, it represents the alignment of military actions with the objectives and tasks specific to an operation or action.

The core components of strategic thinking include systems thinking, foresight, ethical reasoning, creativity, and the ability to synthesise complex information across diverse domains (Freedman 2013). Carl von Clausewitz emphasised the importance of “genius” in war, referring to an intellectual quality that enables commanders to grasp simultaneously both the whole and the particular. Contemporary theorists such as Colin Gray and Lawrence Freedman extend this idea into the realm of strategic culture and institutional pedagogy. Thus, strategic thinking is both an individual and an organisational competence. Also within the field of strategic management, Kenichi Ohmae (1982) describes strategic thinking as an intuitive understanding of strategy, emphasising abilities such as creativity, intuition, and an inclination toward innovative methods. Henry Mintzberg (1994) confirms the same approach, suggesting that strategic thinking combines intuition, creativity, and foresight in order to synthesise the analysis indispensable to the development of an integrated perspective on an organisation’s future direction. Ken Haycock, Anne Cheadle, and Karla Bluestone (2012) view strategic thinking as a tool that enables organisations to move, innovate, and achieve significant improvements in productivity. From another perspective, strategic thinking is described as a process of innovation and creative reasoning that leads to solutions for addressing challenges. Particularly noteworthy is the analysis of the evolution of the concept between 1978 and 2015 conducted by Major Leon Young of the Australian Army, using a cluster analysis of the literature. This approach delineates strategic thinking as a mode of reasoning oriented toward the means-ways-ends relationship, with an emphasis on the future and on the creation of value or advantage for the system (Young 2016). This perspective aligns with the defence and national security-centered paradigm, as it simultaneously highlights the existence of a distinct cognitive process and an anticipatory outcome, expressed through the generation of strategic value.

Organisational leaders have continuously sought ways to develop strategic thinking skills both in themselves, and in others as well (Adzeh 2017, Bajkar 2020). An analysis of the specialised literature reveals that most works dedicated to strategic thinking include, in their recommendations or concluding sections, explicit calls for the development of this competence, indicating the topicality and relevance of the subject.

The ability to quantify strategic thinking represents an essential undertaking; however, the fundamental objective remains the development of this competence at both the individual and organisational levels. Achieving this objective requires the simultaneous fulfillment of two essential conditions:

- the possibility of individual development of each constitutive characteristic of strategic thinking;
- the capacity to identify and shape the factors that influence strategic thinking.

The possibility of individually developing each constitutive characteristic of strategic thinking is extensively addressed in the specialised literature. A solid theoretical and practical foundation can be identified that supports individual development (Sadowski and Connolly 2009, Waldman 2007, Sinclair and Ashkanasy 2005). Moreover, John Pisapia and his collaborators, based on a robust theoretical framework, identified and described three essential metacognitive skills-systems thinking, reframing, and reflection-as well as a dedicated assessment instrument, the *Strategic Thinking Questionnaire* (Pisapia, et al. 2011). Similarly, other characteristics of strategic thinking, such as creativity (Shah, et al. 2012), critical thinking (Watson and Glaser. 2010), and systems thinking (Dolansky, et al. 2010, Pisapia, et al. 2011), have been extensively studied, with numerous validated indicators available for use in research.

The capacity to identify and shape the factors that influence strategic thinking has been addressed by a number of scholars who argue that it is strongly conditioned by external events and contexts (Dragoni, et al. 2011, Daghir and Zaydie 2005, Boyett and Currie 2004). The mapping of domains with the potential to influence strategic thinking highlights factors such as general cognitive ability, organisational culture, and personality (Dragoni, et al. 2011), which may function both as predictors and as influencing variables of strategic performance. The relevance of these factors lies in the possibility of deliberate intervention in each of them, as all are susceptible to development and systematic training. While general cognitive ability, associated with initial individual predispositions and personality can be influenced primarily through processes of selection and shaping, culture, through its constitutive components, namely education, experience, and doctrine, represents a fundamentally trainable dimension with significant potential for long-term institutional shaping. By fulfilling these conditions, namely, the existence of opportunities for the development of the constitutive and generative abilities of strategic thinking, as well as the capacity to influence its determining factors, the trainable nature of strategic thinking can be theoretically supported, understood as a cognitive capability susceptible to systematic formation and consolidation.

Considering the security situation in the Black Sea region and the leadership models promoted by the main regional actors, in relation to the three leadership models identified at the political, politico-military, and tactical-operational levels, proposals can be formulated for leveraging the characteristics of strategic thinking manifested by emerging leadership:

- Integrated Security Leadership – within this model, military institutions and organisations must capitalsze on the practical experience of strategists (strategic leaders) in complementarity with the conceptualisation provided by theorists (theoretical leaders);
- Normative-Strategic Leadership – within this model, politico-military strategic leadership must acknowledge that strategic thinking is not an activity reserved exclusively for the highest levels of command. Normative aspects, doctrines, and identified lessons constitute the foundations for the development of knowledge and the formation of the philosophical profile of the strategic thinker;
- Situational Leadership – within this model, leadership is oriented toward long-term results through the development of cognitive abilities and behaviors. Because there is no perfect leadership model, this model is an adaptive one based on direction, coaching, support and delegation. This model is based on the capacity for diagnosis, evaluation, flexibility and participation. (Paul Hersey 1969).

When related to the domain of regional security, transforming strategic thinking into an organisational capability presupposes the existence of a functional aptitude to exist, to act, and to

produce effects relevant to the field. Given the previous definition of strategic thinking as a mode of reasoning oriented toward the means–ways-ends relationship, projected toward the future and focused on generating value or systemic advantage, the outcome of this capability-building process materialises in the production of future value.

Strategic thinking is thus identified by the authors as a soft capability, characterised by intangibility and by direct dependence on the human factor. Strategic thinking capacity falls within this category of soft capabilities (Young 2015); however, despite its abstract nature, it can be created and developed through a structured approach. The main conclusion advanced in this endeavor concerns the *integration of strategic thinking into the military system of continuing education*. Despite the progress achieved over recent decades, the full integration of strategic thinking into military education systems continues to be constrained by a number of structural and cultural challenges.

A study published in 2015 in the *Strategic Direction* journal identifies several major obstacles affecting the coherent development of this capability within professional military education programs (Goldman, Scott and Follman 2015). The study notes the fragmented and uncoordinated nature of educational initiatives dedicated to this field, as well as the absence of rigorous mechanisms for assessing the development of strategic thinking, reflecting the difficulty of correlating the educational methods employed with the effectiveness of the outcomes achieved. At the same time, there is a confirmed tendency toward the persistence of a traditional form of anti-intellectualism, specific to certain military organisational cultures (Brown 2013).

Under these conditions, the authors argue that the military education system represents the primary institutional frontier for promoting strategic thinking. The manner in which the strategic thinker is developed must be aligned with the complexity of the regional operational environment and designed to support the progressive development of officers' decision-making capabilities at the tactical, operational, and strategic levels, each of these levels involving distinct cognitive requirements.

Conclusions

The need to develop strategic thinking is evident in both the public and private sectors, being driven, on the one hand, by organisations' requirement to formulate and sustain viable strategies and, on the other hand, by the perception of insufficient depth in strategic processes at the organisational level. This situation is further amplified by the lack of theoretical consensus regarding the delimitation of the concept and the identification of the defining traits of the strategic thinker. In this context, the paper has identified the role of strategic thinking - approached as a mode of cognitive processing by future military leaders - in relation to the operational environment of the Black Sea region, as a function of prevailing schools of thought and regional leadership models.

The analysis has shown that the profile of the strategic thinker is characterised by a set of essential cognitive traits, namely systems perspective, creativity, and visionary capacity. A systems perspective facilitates an understanding of the effects of change over time and of the interdependencies among the elements of a system, aspects that are indispensable to strategic construction. Creativity supports the identification of original solutions in ambiguous contexts, while the visionary dimension provides direction, coherence, and meaning to the strategic endeavor. These characteristics are not only identifiable and measurable, but also susceptible to deliberate development, thereby opening the possibility of intentionally building an organisational capability for strategic thinking.

From the perspective of capability theory, strategic thinking is more appropriately situated within the category of non-technical capabilities, whose defining features are intangibility and dependence on the human factor as the primary source of value. The use of a conceptual framework specific to "soft" capabilities allows strategic thinking to be modeled as an organisational phenomenon, highlighting both its enabling components and the rationale for configuring dedicated institutional structures.

At the same time, the analysis reveals a clear need to strengthen strategic thinking among future military commanders and decision-makers, strategists and strategic planners, a need that is not yet addressed in a coherent and systematic manner by current military education systems. In response to this gap, the paper proposes the identification of a generalised model for the development of strategic thinking, grounded in deliberate pedagogy and supported by a coherent set of educational activities adapted to the stages of officers' careers. This approach provides both a conceptual and practical framework for the progressive integration of strategic thinking into professional military education and for the consolidation of an organisational culture oriented toward anticipation, adaptation, and long-term competitive advantage.

Given the extended relevance of strategic thinking at the operational-tactical level, it is treated as one of the fundamental characteristics that must be cultivated from the early stages of a military career. Complementarily, the ability to generate original solutions to highly unique problems confers upon strategic thinking both a creative and a critical role.

With regard to the strategic level, visionary thinking, highly applicable at the operational level but more limited at the tactical level, becomes essential, as it enables leaders and organisations to act in the absence of explicit guidance.

Finally, the manner of approaching problems, whether holistic or inferential, is formed predominantly through experience. Although tactical decision-making relies primarily on well-founded professional judgment, future military leaders at the beginning of their careers must simultaneously build as diverse a range of experiences as possible, necessary for consolidating a holistic perspective on the operational environment.

BIBLIOGRAPHY:

Adzeh, K.J. 2017. "Strategic leadership: An empirical study of factors influencing". *American Journal of Business and Management*, 1-15.

Bajkar, Beata. 2020. "Development and validation of a new tool to measure the profile of." *40th Anniversary International Conference on.* Wroclaw: Advances in Intelligent Systems and Computing. 299-309.

Boyett, Inger, and Graeme Currie. 2004. "Middle Managers moulding international strategy: An Irish start-up in Jamaican Telecoms." *Long Range Planning, Vol 37* 51-66.

Brown, James. 2013. "Fifty Shades of Grey: Officer Culture in the Australian Army". *Australian Army Journal, Vol 10, No. 3* 244-255.

Cioranu, Ionut, Alexandru-Lucian Cucinschi, and Lucian Valeriu Scipanov. 2024. "Professional Training and Personal Development: Essential Complementarity in the Military Educational Process". *Revista Romaneasca pentru Educatie Multidimensionala, Volumul 16*, 12 04: 509-541.

Daghir, M. M., and K.I.H.A Zaydie. 2005. "The measurement of strategic thinking type for top managers in Iraqi public organizations-cognitive approach". *International Journal of Commerce and Management, Vol 15, Iss 1* 34-46.

Dolansky, Mary A, Shirley M. Moore, Patrick A. Palmieri, and Mamta K Singh. 2010. *The Systems Thinking Scale.* Cleveland: Bolton School of Nursing.

Dragoni, Lisa, In-Sue Oh, Paul Vankatwyk, and Paul Tesluk. 2011. "Developing Executive Leaders: The relative contribution of cognitive ability, personality, and the accumulation of work experience in predicting strategic thinking competence". *Personnel Psychology* 829-864.

EU. 2021. "EU Statement on Special Session: Ensuring security and stability in the OSCE region in light of developments with respect to Ukraine". www.osce.org. August 31. Accessed January 31, 2026. https://www.osce.org/sites/default/files/f/documents/7/d/497530.pdf?

Freedman, Lawrence. 2013. *Strategy. A history.* New York: Oxford University Press.

Goldman, Ellen F., Andrea R. Scott, and Joseph M. Follman. 2015. "Organizational practices to develop strategic thinking". *Journal of Strategy and Management, Vol. 8 Issue: 2* 155-175.

Gray, Colin S. 2010. *He Strategy Bridge: Theory for Practice*. Oxford University Press.

Haycock, Ken, Anne Cheadle, and Karla Spence Bluestone. 2012. "Strategic thinking. Lessons for leadership from the literature". *Library leadership&management vol.26, nr. 3/4*, 1-23.

Mière, Christian Le. 2014. *Maritime Diplomacy in the 21st Century Drivers and Challenges*. Abingdon, New York: Routledge.

Mintzberg, Henry. 1994. "The Fall And Rise of Strategic Planning". *Harvard Business Review*, ianuarie- februarie.

NATO. 1999. *The Alliance's Strategic Concept (1999)*. April 24. Accessed February 01, 2026. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1999/04/24/the-alliances-strategic-concept-1999

Ohmae, Kenichi. 1982. *The mind of the strategist. The art of a japanese business*. Yokohama: McGraw-Hill Book Company.

Panait, Mihai. 2024. *Leadership și securitate la Marea Neagră.* Constanța: Editura Academiei Navale "Mircea cel Bătrân".

Paul Hersey, Ken Blanchard. 1969. "Life Cycle Theory of Leadership". *Training and Development Journal* 26-34.

Pisapia, John, John Morris, Gesulla Cavanaugh, and Linda Ellington. 2011. "The strategic thinking questionnaire: Validation and confirmation of constructs". *Strategies for a multi-polar world*. Miami: Strategic Management Society.

Popa, Nicolae-Silviu, and Ion Chiorcea. 2024. "Strategia de securitate pentru regiunea Mării Negre: cooperare, stabilitate și dezvoltare durabilă". *Gândirea militară românească,* nr. 1, 36-57.

Rowlands, Kevin. 2019. *Naval Diplomacy in the 21st Century A Model for the Post-Cold War Global Order*. London, New York: Routledge.

Sadowski, Mary A., and Patrick E. Connolly. 2009. "Creative thinking: The generation of new and occasionally useful ideas". *Engineering Design Graphics Journal*, Vol 63, No 1, 20-25.

Scipanov, Lucian Valeriu. 2024. "Contribuția diplomației navale la securitatea maritimă regională". *Gândirea militară românească*, 30-33.

Shah, 41. Jami J., Roger E. Millsap, Jay Woodward, and S. M. Smith. 2012. "Applied tests of design skills - part 1: Divergent thinking". *Journal of Mechanical Design*, 134(2) 1-10.

Sinclair, Martha, and Niel Ashkanasy. 2005. "Intuition myth or a decision-making tool?" *Management Learning*, Vol 36, No 3, 353-370.

Till, Geoffrey. 2013. *Seapower A Guide for the Twenty-first Century, Fourth Edition*. London, New York: Routledge.

UNO. 2022. "United Nations Organization". *Black Sea Grain Initiative Joint Coordination Centre*. July 27. Accessed January 31, 2026. https://www.un.org/en/black-sea-grain-initiative/background

Waldman, Deane. 2007. "Thinking systems need systems thinking". *Systems Research and Behavioural Science*, Vol 24, No 3, 271-284.

Watson, Goodwin, and Edward M. Glaser. 2010. *Technical manual and user guide: Watson-Glaser II Critical Thinking Appraisal*. San Antonio USA: Pearson.

Young, Leon. 2015. "Defining and Developing Soft Capabilities in Defence". *21st International Congress on Modelling and Simulation (MODSIM2015)*. Queensland: Modelling and Simulation Society of Australia and New Zealand Inc. (MSSANZ). 876-882.

Young, Leon. 2016. "Towards a more comprehensive understanding of Strategic Thinking". *Australian Defence Force Journal*, Vol 199, 55-64.

DOI: 10.53477/3045-2309-26-05

COGNITIVE RESILIENCE AS A STRATEGIC ASSET IN CONTEMPORARY WARFARE: THEORETICAL FOUNDATIONS AND SECURITY IMPLICATIONS

Ruslana GROSU, PhD,
Associate Professor, Armed Forces Military Academy "Alexandru cel Bun",
Chisinau, Republic of Moldova,
E-mail address: ruslana.grosu@gmail.com

Cătălin-Victor POPESCU,
PhD Student, Armed Forces Military Academy "Alexandru cel Bun",
Chisinau, Republic of Moldova,
E-mail address: popescuvictor546@gmail.com

Abstract*: Contemporary warfare is increasingly shaped by cognitive dynamics that influence perception, decision-making, and strategic behaviour across state and non-state actors. While traditional security studies have emphasised kinetic capabilities and material resources, less attention has been paid to cognitive resilience as a strategic asset in modern conflict environments. This paper advances a conceptual and analytical framework that positions cognitive resilience as a core component of contemporary security and warfare.*

Building on interdisciplinary literature, the paper clarifies the concept of cognitive resilience and differentiates it from adjacent constructs. The analysis situates cognitive resilience within contemporary warfare environments characterised by hybrid conflict and prolonged strategic competition. It demonstrates how cognitive vulnerabilities such as rigidity, cognitive overload, and susceptibility to disinformation can undermine strategic effectiveness even in technologically advanced actors.

The paper further conceptualises cognitive resilience as a strategic asset by linking it to security culture and leadership, proposing an analytical framework outlining key dimensions of cognitive resilience and their relevance for defence policy, military education, and security governance. By doing so, the paper contributes to ongoing debates on cognitive security and offers a theoretically grounded foundation for future empirical and comparative research. Overall, the study positions cognitive resilience as a critical yet under-theorised pillar of international security in contemporary warfare contexts across evolving conflict domains.

Keywords*: cognitive resilience; cognitive security; hybrid warfare; information warfare; strategic adaptability; security culture.*

Introduction

Cognitive resilience refers to the capacity to preserve essential cognitive functions, such as perception, attention, situational assessment, reasoning, and decision-making, under conditions of physiological strain, psychological pressure, or environmental disruption. Initially developed within psychology, neuroscience, and mental health research, the concept has undergone substantial theoretical refinement. In line with clinical and neuropsychological literature, *cognitive resilience* is understood as the capacity to sustain better-than-expected cognitive functioning despite the presence of adverse factors, reflecting an individual's ability to maintain cognitive performance under conditions of vulnerability or decline (Elman et al. 2022).

Early interpretations framed resilience as a relatively stable individual trait; contemporary approaches, however, conceptualize it as a dynamic and adaptive process emerging from the interaction of genetic predispositions, environmental conditions, and individual cognitive-emotional resources, which can be developed and strengthened over time. *Cognitive resilience* is defined as the capacity of individuals and systems to sustain adaptive reasoning, tolerate ambiguity, resist manipulation, and maintain *strategic coherence* under conditions of cognitive stress, uncertainty, and information saturation. These capacities are no longer merely individual traits, but collective and institutional resources with direct strategic value.

The significance of *cognitive resilience* has been well documented in relation to mental health outcomes, cognitive aging, and educational performance, where it is associated with sustained functioning and adaptive capacity in the face of adversity (Parsons, Kruijt & Fox 2016, 296-299). Foundational research conducted in the mid-twentieth century marked a turning point in *resilience* studies, as scholars began to move beyond deficit-oriented models focused on vulnerability and pathology. Influential contributions redirected attention toward strengths-based perspectives, emphasising positive adaptation, learning, and proactive coping mechanisms. This shift laid the groundwork for contemporary understandings of *resilience* as a continuum shaped by both protective and risk factors, including social support networks, emotional regulation abilities, and biological predispositions.

Despite this expanding body of research, persistent challenges remain regarding the operationalisation and measurement of *cognitive resilience*. The absence of standardised assessment frameworks and the coexistence of diverse conceptualisations continue to generate ambiguity, particularly when the concept is applied beyond individual-level analysis. These limitations become especially salient when *cognitive resilience* is invoked in contexts characterised by high uncertainty, strategic competition, and deliberate attempts to influence cognition and behaviour.

In parallel with these conceptual developments, the contemporary security environment has undergone a profound transformation. The proliferation of hybrid threats, information warfare, and digitally mediated influence operations, often enhanced by artificial intelligence, has shifted the locus of strategic competition toward the cognitive domain. Rather than targeting material capabilities alone, adversaries increasingly seek to disrupt perception, distort situational awareness, fragment judgment, and undermine decision-making processes at individual, institutional, and societal levels. Decision-makers, military personnel, and civilian populations alike are exposed to sustained cognitive pressure aimed at eroding coherence, trust, and adaptive capacity.

Research Problem

Although recent literature increasingly acknowledges the importance of *cognitive resilience,* the concept remains fragmented across psychological, organisational, and security-oriented approaches. *Cognitive resilience* is often treated either as an individual psychological trait or as a loosely defined societal capacity, while its strategic relevance in contemporary warfare remains insufficiently conceptualised. In particular, there is a lack of integrated theoretical frameworks explaining how and under what conditions *cognitive resilience* can function as a *strategic asset,* capable of mitigating *cognitive warfare* effects and supporting *adaptive deterrence* and decision security.

The core research problem addressed in this study therefore lies in the insufficient conceptualisation of *cognitive resilience* as a governable strategic resource, situated at the intersection of behavioural sciences, security studies, organisational governance, and contemporary warfare. The present study seeks to address this gap by clarifying the conceptual foundations of *cognitive resilience* and articulating its relationship to *cognitive security*, decision integrity, and strategic performance in modern conflict environments.

Research Objectives

The *general objective* consists of analysis and conceptualising of *cognitive resilience* as a *strategic asset* in contemporary warfare by integrating insights from behavioural sciences, security studies, resilience governance, and *cognitive warfare* literature.

Several *specific objectives* follow: to provide conceptual clarification of *cognitive resilience* by distinguishing it from related concepts such as general *psychological resilience*, information security, and *cyber resilience*; to identify and analyse active and passive cognitive stressors relevant to contemporary warfare and assess their impact on individual and organisational cognitive functioning; to examine the relationship between *cognitive resilience* and *cognitive security*, with a particular focus on organisational and institutional dimensions; to evaluate the role of *cognitive resilience* in *adaptive deterrence*, decision coherence, and the reduction of adversarial strategic advantage. The study develops an integrated theoretical framework enabling the operationalisation of *cognitive resilience* in military, institutional, and societal contexts.

Methodology

This study adopts a qualitative, theory-driven research design grounded in conceptual analysis and integrative literature review. Given the exploratory and foundational nature of the research question, namely, the conceptualisation of *cognitive resilience* as a *strategic asset* in contemporary warfare, the methodology prioritises theoretical coherence, analytical rigour, and interdisciplinary synthesis rather than empirical testing. The research is structured as a conceptual-analytical study, drawing on established approaches in security studies and *resilience* research that aim to clarify concepts, integrate fragmented literature, and generate theoretically grounded frameworks applicable to complex security environments.

1. Literature Review

The literature employed in this study was selected based on conceptual relevance, academic rigour, and strategic applicability, reflecting the inherently interdisciplinary nature of *cognitive resilience* as a research area. The reviewed works are structured into five interrelated problem blocks, each contributing a distinct analytical dimension to the study.

The first block, which concerns *cognitive warfare and the transformation of the security environment*, addresses the conceptual emergence of *cognitive warfare* as a defining feature of contemporary conflict. Key authors emphasise that modern adversaries increasingly target perception, judgment, and decision-making rather than exclusively physical assets. Foundational contributions include military and policy-oriented analyses that frame *cognitive warfare* as operating within the digital gray zone and aiming at cognitive effects rather than kinetic outcomes (Cheatham et al. 2024; Ariton 2025). A comparative and NATO-aligned conceptual work stresses the need to delimit *cognitive warfare* analytically, warning against conceptual overstretch and terminological inflation (Deppe & Schaal 2024; Deppe, Fotescu & Schaal 2024). Claverie and Du Cluzel (2022) do not provide an explicit definition of *cognitive resilience*; instead, *resilience* is implicitly framed as a defensive and preventative capacity within *cognitive warfare*, associated with the protection of perception, judgment, and decision-making processes at individual and societal levels (Claverie & Du Cluzel 2022).

The second block, which elucidates *cognitive security* and the protection of cognitive assets, focuses on the transition from describing cognitive threats to defining what must be protected, namely cognitive assets such as attention, judgment, trust, and decision-making capacity.

Cognitive security scholarship reframes the human mind as a security-relevant asset exposed to both adversarial and systemic degradation (Ask et al. 2025). Architecture-informed and human-factors approaches advance this perspective by proposing design and governance mechanisms that protect cognition without compromising democratic norms (Doherty 2023; Tossell et al. 2025).

The block referring to *resilience* theory, governance, and *strategic deterrence* situates *cognitive resilience* within broader debates on *resilience* as a *security* concept, emphasising both its analytical value and its political implications. Critical security scholarship highlights that *resilience* is not neutral, warning against its performative and responsibilising effects (Brassett & Vaughan-Williams 2015). Governance-oriented literature reframes *resilience* as an institutional capability requiring coordination, accountability, and policy design (Linkov & Trump 2019; Heinimann & Hatfield 2017). Strategic analyses further conceptualise *resilience* as *adaptive deterrence*, directly linking it to strategic competition and security outcomes (Laine & Petersson 2025; Ziehr & Merkt 2024).

The block about disinformation, psychological operations, and cognitive stressors examines *cognitive resilience* in relation to disinformation, psychological operations, and influence campaigns, which represent key operational tools of *cognitive warfare*. Empirical studies on *resilience* to disinformation identify cognitive and social correlates that shape susceptibility and resistance (Mider & Żółtowski 2025). Educational and diagnostic interventions demonstrate that *cognitive resilience* can be deliberately cultivated at societal and organisational levels (Molek-Kozakowska 2024; Bebber 2025). Analyses of cyber-enabled psychological operations emphasize the convergence of informational and cognitive attack vectors (Mlejňková 2022; Meghraoui & Belkhamza 2025).

The final block, which approaches organisational, military, and whole-of-society perspectives, expands *cognitive resilience* beyond individual and unit-level considerations toward organisational, national, and whole-of-society frameworks. Military-focused research provides rare attempts to assess *cognitive resilience* among personnel and link it to operational effectiveness (Kosárová, Bízík, & Potočňák 2024). European and regional security analyses highlight the role of *cognitive resilience* in defence challenges and societal preparedness (Senčar 2021; Hansen 2017). Policy-oriented and institutional reports emphasise cross-sector coordination and societal cohesion as essential components of *resilience* against hybrid threats (Wigell, Mikkola, & Juntunen 2021; Teperik et al. 2018; Semenenko et al. 2025).

The selection of 45 sources reflects a deliberate methodological choice to combine theoretical depth with strategic relevance. Behavioural science literature provides the foundational understanding of *resilience* and cognitive adaptation, while security and defence studies contextualise the *cognitive resilience* within contemporary warfare. Governance and organisational scholarship enable the treatment of *cognitive resilience* as a managed institutional capability, and recent work on AI, disinformation, and hybrid threats situates the analysis in the current operational environment. Together, these sources support a coherent argument that *cognitive resilience* constitutes a strategic asset only when it is governed, designed, and operationalised across individual, organisational, and societal levels, thereby preserving decision integrity and constraining adversarial influence in contemporary warfare.

2. Conceptualizing Cognitive Resilience in the Context of Contemporary Warfare

Cognitive resilience originates in *resilience* research within the behavioural sciences, where *resilience* has traditionally been understood as a dynamic process involving exposure to adversity and the capacity for positive adaptation in response to that adversity (Luthar & Cicchetti 2000). Early formulations positioned *resilience* primarily within trait psychology and individual coping capacities, emphasizing psychological robustness and recovery following stress or disruption. Within this tradition, *cognitive resilience* was defined as the "capacity to overcome the negative effects of setbacks and associated stress on cognitive function and performance" (Staal et al. 2008, p. 260). While analytically useful, such definitions largely reflect individual-level adaptation and remain insufficient for explaining *resilience* in strategically contested environments.

More recent research has extended *resilience* theory beyond individual traits toward systemic, organisational, and security-oriented interpretations. The relationship between *cognitive resilience* and military personnel has been examined through a performance-oriented lens, highlighting how the

ability to maintain cognitive functioning under stress, fatigue, and operational pressure is critical for sustaining effectiveness in demanding military environments (Staal et al. 2008, as discussed in Flood & Keegan 2022, p. 8). When cognition becomes a target, *resilience* becomes a security capability.

This evolution is particularly relevant in the context of contemporary warfare, where cognitive processes themselves such as perception, judgment, attention, sensemaking, and decision-making have become deliberate targets of adversarial action. From this perspective, *cognitive resilience* must be understood not merely as psychological endurance, but as a security-relevant capability that safeguards cognitive functioning under conditions of persistent pressure, uncertainty, and hostile influence. *Cognitive resilience*, which is the ability of systems and societies to resist manipulative exploitation and the distortion of perception, is a fundamental issue to be considered in the field of cybersecurity (Bierecki, Gaie, Karpiuk & Langlois-Berthelo 2025, pp. 139-140).

Within the emerging field of *cognitive security*, stressors affecting *cognitive resilience* are conceptualised as both *active* and *passive*. *Active stressors* arise from intentional adversarial efforts aimed at accessing, degrading, or manipulating cognitive assets, including individuals, groups, and decision-making structures (Masakowski & Blatny 2022). Such stressors are characteristic of *cognitive warfare*, disinformation campaigns, psychological operations, and influence strategies designed to distort judgment, erode trust, or disrupt strategic coherence. Building on NATO conceptualisations of *cognitive warfare*, *active stressors* can be understood as intentional adversarial efforts aimed at accessing, degrading, or manipulating cognitive assets, ranging from individual cognition to collective decision-making structures (Claverie & Du Cluzel 2022). In contrast, *passive stressors* refer to the natural and cumulative degradation of cognitive performance over time, independent of direct adversarial intent. These include prolonged workload, cognitive fatigue, stress accumulation, information overload, and environmental pressures that reduce attentional control and decision accuracy. Although Vrijkotte et al. (2016) do not explicitly conceptualise *passive stressors*, their analysis provides strong empirical evidence for cumulative, non-adversarial stressors that progressively degrade cognitive performance through sustained workload, fatigue, sleep deprivation, and environmental pressure (Vrijkotte et al. 2016). Importantly, *passive stressors* do not merely coexist with active threats; rather, they amplify vulnerability to hostile cognitive influence. Extended sustained operational tempo, diminished motivation to engage in security-enhancing behaviours, or heightened emotional strain can significantly weaken cognitive acuity and increase susceptibility to manipulation. *Cognitive resilience* therefore emerges at the intersection of internal cognitive resource management and external threat exploitation.

The maintenance of *cognitive resilience* over time depends on the balance between *passive coping* and *active engagement* with these stressors. *Passive coping strategies*, such as avoidance, or emotional numbing, may offer short-term relief but ultimately erode *cognitive resilience* and impair decision-making capacity. In contrast, *active coping* involves the deliberate application of cognitive strategies, training, and organizational measures that sustain cognitive performance and adaptive capacity under pressure. From a *cognitive security* perspective, *active engagement* is not an individual responsibility alone but an organisational obligation, requiring deliberate design, coordination, and governance.

In this respect, *cognitive resilience* parallels the evolution of *cyber resilience* as an organisational state rather than a purely technical or individual attribute. *Cognitive resilience* entails a holistic and comprehensive response to cognitive threats, in which individuals at all levels of an organisation or institution possess a shared understanding of the threat landscape and their role within it (Ask et al. 2024b). Procedures for anticipating, absorbing, and adapting to harmful situations must be embedded structurally, reflecting the expectation that unexpected and disruptive cognitive challenges will inevitably occur. *Resilience*, therefore, is not the absence of vulnerability, but the capacity to function, decide, and adapt despite it.

Within contemporary warfare, this organisational framing has critical strategic implications. Individuals constitute cognitive assets whose degradation can generate cascading effects across units, organisations, and even national systems. Targeting a single individual through biological,

psychological, or informational means may significantly impair collective decision-making if that individual occupies a strategic or operationally central role. Similarly, coordinated influence operations targeting multiple members of a subgroup or society can generate social incoherence, erode institutional trust, and weaken *national cognitive security*, thereby reducing a state's capacity to respond effectively to subsequent adversarial actions.

Accordingly, *cognitive resilience* must be conceptualised as *a strategic asset*: a collective, governed, and deliberately cultivated capability that protects the cognitive foundations of military effectiveness, societal cohesion, and strategic decision-making. In contemporary warfare, characterised by hybrid threats, persistent competition, and AI-enabled influence, *cognitive resilience* is not merely a protective mechanism but a determinant of strategic advantage. Its absence magnifies adversarial payoff; its presence constrains hostile influence, preserves decision integrity, and enhances *adaptive deterrence*.

The academic debate on *cognitive resilience* emerges from a broader attempt to conceptualise how modern warfare increasingly targets, not only forces, platforms, and infrastructure, but also perception, judgment, attention, trust, and decision cycles. In EU-oriented discussions, *cognitive warfare* is framed as a security-policy challenge produced by digital acceleration, narrative contestation, and the strategic exploitation of societal vulnerabilities (Ariton 2025). Military-oriented analyses similarly emphasise that the "battlefield" expands into the digital gray zone, where adversaries seek decision disruption, behavioural steering, and legitimacy erosion rather than immediate kinetic outcomes (Cheatham et al. 2024). Yet an important limitation in this emerging literature is conceptual "inflation": *cognitive warfare* can become an umbrella label for disinformation, psychological operations, cyber disruption, and influence campaigns. Comparative syntheses warn that without careful boundary-setting, the concept risks losing analytic value and collapsing into older categories under a newer name (Deppe, Fotescu, & Schaal 2024). This is why conceptual work grounded in NATO's exploratory framing is pivotal: it clarifies *cognitive warfare* as a strategic logic oriented toward *cognitive effects*, not merely the circulation of content (Deppe & Schaal 2024). Even when NATO-derived definitions remain exploratory, their value lies in establishing a minimum conceptual discipline: (1) identify the intended cognitive effect, (2) distinguish vectors from outcomes, and (3) connect tactical influence to strategic decision consequences.

From this conceptual baseline, the literature increasingly pivots from "what *cognitive warfare* is" to "what must be protected", giving rise to the notion of *cognitive security*. *Cognitive security* reframes the human mind and other cognitive assets as objects of protection, proposing that hostile influence constitutes a security threat when it measurably degrades cognitive integrity and decision reliability (Ask et al. 2025). This move is theoretically productive because it connects security studies to cognitive science, but it also raises a critical normative question: the protection of cognition should not become a pretext for intrusive governance or ideological control. A more defensible direction is offered by architecture-informed approaches that translate *cognitive security* into design principles: how systems, interfaces, training, and governance can reduce cognitive attack surfaces while preserving democratic constraints (Doherty 2023). The human-factors perspective strengthens this line by arguing that *cognitive security* must be operationalised through attention to workload, bias, trust calibration, and decision-making conditions, some areas where empirical measurement and intervention are plausible (Tossell et al. 2025). Taken together, these works imply that *cognitive resilience* can be treated as a *strategic asset* only if it is linked to measurable *cognitive performance* and *decision integrity*, rather than remaining at the level of metaphor.

A coherent theoretical framework must therefore integrate *cognitive security* with the broader and contested concept of *resilience*. In security studies, *resilience* is not simply a benign capacity; it is also a political and performative discourse that can shift responsibility onto individuals and communities while obscuring the structural origins of risk (Brassett & Vaughan-Williams 2015). This critique is essential for *cognitive resilience* research: "be resilient" can become an implicit demand that soldiers and citizens absorb informational violence and adapt to manipulation rather than

preventing it. To avoid that trap, governance-centered accounts argue for *resilience* as a managed, institutionalised capability, assessed, coordinated, and continuously improved through policy, accountability, and cross-sector design (Linkov & Trump 2019; Heinimann & Hatfield 2017). Complexity-informed models add an important nuance: *resilience* is not stable "hardening", but the capacity to navigate dynamic order/disorder transitions, where a rigid control may fail and adaptive mechanisms matter (Normandin & Therrien 2016). Because the *cognitive warfare* thrives on ambiguity, overload, and uncertainty, these complexity insights are not peripheral, they are directly relevant to how *cognitive resilience* should be conceptualised as an operational capability rather than a generic psychological virtue.

The *strategic asset* claim becomes most convincing where *resilience* is linked to *deterrence* and *strategic competition*. *Resilience* is theorised as *adaptive deterrence*, shaping adversary calculations by reducing the payoff of coercion and influence operations (Laine & Petersson 2025). This reframing is valuable: *cognitive resilience* is not only defensive recovery, but a capability that can deny strategic effects by preserving decision coherence and societal trust under pressure. However, this *deterrence* argument must be anchored in mechanisms rather than slogans. *Organisational resilience* scholarship supports that anchoring by focusing on the cognitive dimension of *resilience* capacity, emphasizing sensemaking, attention control, and interpretive processes that shape how systems adapt (Lengnick-Hall, Beck & Woznyj 2023). At the human performance level, *strategic resilience* is also discussed as an enabling condition for sustained performance in high-stakes environments, suggesting that *cognitive resilience* has implications for training, education, and performance governance (Ziehr & Merkt 2024). The conceptual synthesis here is straightforward: *cognitive resilience* becomes *strategic* when it demonstrably protects the cognitive prerequisites of *deterrence*: credible signaling, coherent decision cycles, and institutional legitimacy.

A decisive contribution of the recent literature is the explicit coupling of the cognitive domain with *cyber governance* and *technological architectures*. Rather than treating cyber and cognition as separate domains, governance-oriented accounts argue that *cognitive resilience* is necessary for cyber governance itself, because security decisions depend on trust, judgment, and the management of information overload (Grobler & Aamir 2024). Technology-architecture approaches go further by proposing integrated governance models for cyber and *cognitive resilience*, which is an important move for operational environments where digital systems, AI-enabled media, and human cognition form a single socio-technical system (Kaleeva, Blagoev & Shalamanov 2025). Conference-based contributions similarly interpret *cyber resilience* as a prerequisite for confronting *cognitive warfare*, but they are strongest when they specify the chain from technical vector to cognitive effect and decision disruption (Radu 2025; Meghraoui & Belkhamza 2025). In parallel, broader security literature on hybrid threats provides the strategic context in which such convergence matters: hybrid environments blend military and nonmilitary means, making it increasingly artificial to separate "technical" from "cognitive" lines of effort (Kaczmarek & Cholewińska 2024). A national-level discussion of AI as a vector of insecurity reinforces the same logic: AI scales persuasion, deception, and targeting, making cognitive vulnerabilities strategically exploitable (Peptan 2025).

The most operationally consequential sub-field concerns *disinformation*, *psychological operations*, and *cognitive inoculation*. Military-facing work on "information inoculation" argues for preparing warfighters to resist manipulation through preemptive cognitive training, which is an approach aligned with psychological inoculation theory, but requiring careful implementation to avoid indoctrination dynamics (Bebber 2025). Empirical work on *resilience* to disinformation is particularly valuable because it identifies correlates and countermeasures, offering a bridge between concept and measurement (Mider & Żółtowski 2025). Education-based interventions likewise demonstrate that *resilience* can be built through diagnostic and training programs, especially in contexts of war-related disinformation (Molek-Kozakowska 2024). At the operational edge, cyber-enabled psychological and information operations show how influence campaigns are increasingly fused with digital vectors, reinforcing the need for integrated threat models (Mlejňková 2022). A

recurring limitation across this cluster, however, is the tendency to treat *disinformation resilience* as a proxy for *cognitive resilience* overall. A stronger theoretical framework should treat disinformation as one pathway among several, alongside overload, fear induction, identity polarisation, trust erosion, and decision paralysis, and explicitly show how these pathways degrade strategic decision-making.

Recent work on *AI-driven disinformation* further intensifies this imperative. Policy-oriented analyses argue that AI changes the scale, speed, personalisation, and credibility of manipulative content, requiring *democratic resilience* measures that span regulation, platform governance, and societal preparedness (Romanishyn, Malytska & Goncharuk 2025). Yet, the strategic relevance of this literature depends on linking policy prescriptions to cognitive mechanisms: how deepfakes, synthetic persuasion, and coordinated inauthentic behaviour affect trust calibration, epistemic vigilance, and institutional legitimacy. Complementing these discussions, broader treatments of *psychological warfare* in the digital age provide descriptive taxonomies of strategies and impacts, though they vary in rigor and should be used selectively where they add conceptual clarity rather than repetition (Nawaz 2025).

The military specificity of *cognitive resilience* is reinforced where studies address *personnel factors* and *human-AI teaming*. Assessments focused on military personnel identify critical factors shaping *cognitive resilience*, offering a rare step toward operationalisation in defence contexts (Kosárová, Bízík & Potočňák 2024). In future force design, the challenge is not only to "train resilient minds", but to design socio-technical teams whose interfaces and adaptive systems protect decision quality under adversarial conditions. Neuroadaptive and human-AI teaming perspectives explicitly connect *cognitive resilience* to operational integrity and decision superiority, implying that *resilience* must be engineered into the system rather than treated as an individual trait (Picchi 2025). Service and staff papers can add context for doctrine and professional military education, but their theoretical value depends on whether they contribute unique operational logic rather than reiterating general claims (Delmonte 2024). Military-oriented analyses demonstrate that *cognitive warfare* directly targets command-and-control effectiveness by exploiting cognitive biases, information overload, and digitally mediated manipulation, thereby degrading sensemaking and decision-action cycles before kinetic engagement occurs. Drawing on the Canadian Armed Forces context, Delmonte shows that systematic training in media and information literacy and critical thinking constitutes a core mechanism for strengthening *cognitive resilience*, positioning it as a prerequisite for *cognitive security* and decision integrity in multi-domain operations (Delmonte 2024).

Finally, a strategic framework must position *cognitive resilience* within *whole-of-society and national resilience architectures*. European security discussions emphasise *cognitive resilience* as part of broader *resilience* agendas and geopolitical contestation, including region-specific insights that show how societal context shapes cognitive vulnerabilities and defences (Hansen 2017; Senčar 2021). Policy and best-practice reports emphasise institutional coordination, public communication, and cross-sector measures for countering hybrid threats, some elements that directly support the claim that *cognitive resilience* has strategic effects beyond the military (Wigell, Mikkola & Juntunen 2021; Teperik et al. 2018). Contemporary Ukrainian recommendations provide a particularly relevant illustration of how *cognitive resilience* can be embedded into national security planning, including links to defence-economic dimensions and state capacity (Semenenko et al. 2025). Youth-oriented *resilience* initiatives in the Baltics highlight intergenerational and societal dimensions, though their integration into a warfare-focused argument must be carefully justified to avoid drifting into general social policy (Teperik, Denisa-Liepniece & Bankauskaitė 2025). *Socioeconomic resilience* comparisons can also supply contextual variables, such as trust, cohesion, and sustainability conditions, that shape a society's baseline vulnerability to cognitive operations (Šimelytė, Vveinhardt & Deikus 2025). Where regionally specific analyses frame *cognitive resilience* against *cognitive warfare* targeting a particular state, the contribution is strongest when it offers transferable components and enhancement strategies rather than purely national narratives (Torabi & Ahmadi 2025). Works that attempt to synthesise "*societal resilience* through education vs. war" can be conceptually useful, but while societal, state, and *military resilience* are conceptually developed in existing literature, the *cognitive resilience* remains under-theorised and

insufficiently operationalised, despite being implicitly acknowledged as a critical dimension of contemporary security (Lesenciuc, Nagy & Lesenciuc 2022).

Overall, the reviewed sources justify a consolidated theoretical claim: *cognitive resilience* functions as a *strategic asset* when it is treated as a governed, designed, and measurable capability that protects decision integrity across military and societal levels. The strongest trajectory in the literature moves from definitional clarity (Cheatham et al. 2024; Deppe & Schaal 2024.), to *cognitive security* architecture (Ask et al. 2025; Doherty 2023), to *resilience governance* and *deterrence* (Brassett & Vaughan-Williams 2015; Laine & Petersson 2025), and finally to operationalisation through human factors, personnel assessment, and socio-technical design (Tossell et al. 2025; Kosárová, Bízík & Potočňák 2024; Picchi 2025). The main constructive gap remains methodological: the field still needs more explicit indicators and evaluation designs that can demonstrate how *cognitive resilience* reduces adversary payoff, stabilises decision cycles, and strengthens *deterrence* under conditions of hybrid and AI-enabled influence.

3. Security Implications

The conceptualisation of *cognitive resilience* as a *strategic asset* carries significant implications for contemporary security policy, military doctrine, and institutional governance. As recent literature on *cognitive warfare* and *cognitive security* demonstrates, modern adversaries increasingly target cognitive processes rather than exclusively physical assets, seeking to degrade perception, judgment, trust, and decision-making coherence (Cheatham et al. 2024; Deppe & Schaal 2024). In this context, security is conceptualised as a multidimensional construct that has long transcended purely military and state-centric interpretations, incorporating the societal and human dimensions, as reflected in established approaches such as the Copenhagen School and the human security paradigm. From this perspective, the cognitive and perceptual factors extend beyond explanatory variables, positioning the integrity of cognition itself as an emerging security concern (Ask et al. 2025).

At the strategic level, *cognitive resilience* reshapes prevailing understandings of *deterrence*. Classical *deterrence* models focus on material capabilities and credible threats of retaliation, yet hybrid and *cognitive warfare* strategies aim to circumvent these mechanisms by undermining decision cycles, institutional confidence, and societal cohesion (Ariton 2025; Kaczmarek & Cholewińska 2024). As argued in recent *resilience* scholarship, *resilience* functions as a form of *adaptive deterrence*, reducing the strategic utility of coercive influence by denying adversaries the cognitive effects they seek to achieve (Laine & Petersson 2025). *Cognitive resilience*, understood in this sense, signals that attempts to manipulate perceptions or destabilise decision-making will fail to produce strategic gains, thereby constraining adversarial behaviour.

At the *operational and organisational level*, the findings imply a necessary shift away from viewing *resilience* as an individual psychological trait toward treating it as an *institutionally governed capability*. Research on *cognitive security* and human factors underscores that decision quality depends not only on individual robustness but on organisational design, workload distribution, information management, and shared situational awareness (Doherty 2023; Tossell et al. 2025). Governance-oriented approaches to *resilience* further emphasise that institutions must embed procedures for anticipating, absorbing, and adapting to cognitive disruption as a routine element of security practice (Linkov & Trump 2019; Heinimann & Hatfield 2017). Without such institutionalisation, even cognitively capable individuals remain vulnerable within poorly designed systems.

The study also highlights the security relevance of *passive cognitive stressors*, which are often underestimated in strategic planning. Prolonged operational tempo, cognitive fatigue, emotional strain, and sustained exposure to contested information environments gradually erode cognitive performance and increase susceptibility to hostile influence (Vrijkotte et al. 2016; Flood & Keegan 2022). Empirical and conceptual work indicates that such passive stressors significantly amplify the effectiveness of active cognitive operations, including disinformation and psychological pressure (Mider & Żółtowski 2025;

Mlejňková 2022). Consequently, security policies that focus exclusively on countering external adversaries while neglecting internal cognitive conditions risk unintentionally enhancing adversarial impact.

From a *whole-of-society security perspective*, *cognitive resilience* extends beyond military and governmental institutions to encompass societal trust, communication ecosystems, and civil-military relations. Hybrid threat research consistently shows that *cognitive warfare* frequently targets social cohesion and institutional legitimacy rather than immediate physical damage (Wigell, Mikkola & Juntunen 2021). Case-based analyses from Europe and Ukraine further demonstrate that societies with higher levels of *cognitive preparedness*, manifested in credible public communication, critical information literacy, and institutional coordination, are better positioned to withstand sustained influence campaigns (Hansen 2017; Teperik et al. 2018; Semenenko et al. 2025). *Cognitive resilience* thus becomes a prerequisite for maintaining national security under conditions of persistent informational pressure.

The convergence of *cognitive, cyber, and AI-enabled threats* introduces additional governance challenges. Recent studies emphasise that AI-driven disinformation and automated influence operations accelerate the scale, personalisation, and credibility of cognitive attacks, blurring traditional boundaries between cyber security and psychological operations (Romanishyn, Malytska & Goncharuk 2025; Meghraoui & Belkhamza 2025). Governance models that integrate *cyber* and *cognitive resilience* highlight the necessity of combining technological safeguards with organisational and cognitive defences, rather than treating these domains in isolation (Grobler & Aamir 2024; Kaleeva, Blagoev & Shalamanov 2025).

Finally, the study implies a need to rethink security preparedness and evaluation metrics. Conventional indicators, such as force structure, response time, or technological inventories, fail to capture vulnerabilities in the cognitive domain. Emerging research on human performance and *military personnel resilience* suggests that cognitive robustness, decision integrity, and adaptive capacity under informational stress should be incorporated into security assessments (Kosárová, Bízík & Potočňák 2024; Ziehr & Merkt 2024). Although the present study remains conceptual, it provides the theoretical basis for developing such indicators in future empirical research.

In sum, the security implications of *cognitive resilience* are both structural and strategic. Treating *cognitive resilience* as a *strategic asset* requires a shift from reactive countermeasures toward proactive governance of cognitive capacity, from individual coping toward institutional design, and from narrow threat mitigation toward sustained decision integrity (Brassett & Vaughan-Williams 2015). In contemporary warfare environments, where influence, ambiguity, and perception increasingly determine outcomes, *cognitive resilience* emerges as a decisive enabler of security, stability, and strategic autonomy.

Conclusions

This conceptual and theoretical analysis builds on and systematises existing strands of the literature to articulate an integrated analytical framework for understanding cognitive resilience as a strategic asset in contemporary warfare. First, the reviewed studies consistently indicate that cognitive resilience acquires strategic relevance primarily when it is conceptualised, governed, and operationalised at the organisational and institutional level, rather than approached solely as an individual psychological capacity. Second, the literature converges on the view that passive cognitive stressors, such as fatigue, information overload, and prolonged uncertainty, constitute enabling conditions that amplify the impact of active cognitive warfare stressors, thereby increasing the vulnerability to manipulation and decision degradation.

This study has argued that *cognitive resilience* must be understood as a security-relevant, governable capability that protects the cognitive foundations of decision-making, institutional legitimacy, and *strategic coherence* in contemporary warfare. By integrating behavioural science insights with security studies, governance theory, and *cognitive warfare* literature, the analysis

demonstrates that *resilience* is not merely a reactive coping mechanism but a proactive strategic resource that constrains adversarial influence and supports *adaptive deterrence*. *Cognitive resilience* becomes strategically meaningful when it preserves decision integrity under pressure, stabilizes sensemaking processes, and reduces the strategic payoff of cognitive attacks.

A central contribution of this research lies in its systematic distinction between active and passive cognitive stressors, and in demonstrating their interactive effects on cognitive vulnerability. While *cognitive warfare* literature often focuses on intentional influence operations, this study shows that unmanaged internal conditions, such as organisational overload, sustained stress, and cognitive depletion, can be equally decisive in shaping security outcomes. Consequently, *cognitive resilience* cannot be achieved through counter-disinformation measures alone but requires institutional design, workload governance, and sustained cognitive capacity management.

The study further advances the field by linking *cognitive resilience* to *cognitive security* and *adaptive deterrence*, positioning it within broader strategic competition rather than treating it as a peripheral psychological concern. In doing so, it reframes *resilience* from a discourse of endurance and responsibilisation into one of strategic governance and institutional responsibility. This reframing is particularly relevant in hybrid and AI-enabled conflict environments, where adversaries increasingly seek to disrupt decision cycles and societal trust without crossing traditional thresholds of armed conflict.

From a security policy perspective, the analysis underscores the necessity of integrating *cognitive resilience* into military doctrine, organisational governance, and whole-of-society security frameworks. Protecting cognitive assets, such as attention, judgment, trust calibration, and decision coherence, emerges as a prerequisite for effective deterrence, crisis management, and strategic autonomy. The study therefore provides a theoretical foundation for future empirical research, capability development, and policy design aimed at operationalising *cognitive resilience* across military, governmental, and societal levels.

BIBLIOGRAPHY:

Ariton, Lorina. 2025. Cognitive Warfare In The Digital Age: Implications For Eu Security Policy. In: International Conference Knowledge-Based Organization, pp. 1-9. doi: 10.2478/kbo-2025-0001.

Ask, T. F.; Sütterlin, S.; Müller, M.; Lugo, R. G.; Saari, D.; Grahn, H.; Canhame, M.; Hermansen, D. and Knox, B.J. 2025. Cognitive Security: The study and practice of protecting the human mind and other Cognitive Assets from cognitive threats. PsyArXiv preprint. doi: 10.31234/osf.io/2ftqc_v1.

Bebber, R. 2025. Information inoculation: preparing US warfighters for cognitive war. Hudson Institute.

Bierecki, Dominik; Gaie, C.; Karpiuk, M. and Langlois-Berthelot, J. 2025. Creating Resilient Artificial Intelligence Systems. A Responsible Approach to Cybersecurity Risks. Prawo i Więź, nr. 5 (58) październik, 131-149.

Brassett, J. and Vaughan-Williams, N. 2015. Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness. Security Dialogue, 2015, 46(1), 32–50. doi:10.1177/0967010614555943.

Cheatham, Michael J.; Geyer, Angelique M.; Nohle, Priscella A. and Vazquez, Jonathan E. 2024. Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone. Joint Force Quarterly 114 (3rd Quarter 2024), 83-91, https://digitalcommons.ndu.edu/joint-force-quarterly/vol114/iss2/15 (21.12.2025)

Claverie, B. and Du Cluzel, F. 2022. “Cognitive warfare”: The advent of the concept of “cognitics” in the field of warfare. Cognitive Warfare: the future of cognitive dominance, 2-1, 1-7, 2022, 978-92-837-2392-9. ffhal-03635889f.

Delmonte, Major Alexandra L. 2024. JCSP 51 - PCEMI n° 51 Service Paper Étude militaire. 2024-2025.

Deppe, Christoph; Fotescu, Alexandru and Schaal, Gary S. 2024. The Understanding of Cognitive Warfare in Comparative Perspective Taking Stock and Bridging the Gap to Extant Literatures. Helmut-Schmidt-University/University of the Federal Armed Forces, Hamburg Germany: NATO S&T.

Deppe, Christoph and Schaal, Gary S. 2024. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. Frontiers in Big Data, 2024, 7: 1452129. https://doi.org/10.3389/fdata.2024.1452129

Doherty, G. 2023. Cognitive Security: An Architecture Informed Approach from Cognitive Science. In: Schmorrow, D.D., Fidopiastis, C.M. (eds) Augmented Cognition. HCII 2023. Lecture Notes in Computer Science, vol 14019. Springer, Cham. https://doi.org/10.1007/978-3-031-35017-7_25

Elman, J. A., Vogel, J. W., Bocancea, D. I., Ossenkoppele, R., van Loenhoud, A. C.; Tu, X. M. and Kremen, William S. 2022. Issues and recommendations for the residual approach to quantifying cognitive resilience and reserve. Alzheimer's research & therapy, 14(1), 102. doi:10.1186/s13195-022-01049-w.

Flood, A. and Keegan, R. J. 2022. Cognitive resilience to psychological stress in military personnel. Frontiers in psychology, 13, 809003. doi: 10.3389/fpsyg.2022.809003.

Grobler, Marthie and Aamir, Tooba. 2024. Building cognitive resilience for enhanced cyber governance. In: Psybersecurity. CRC Press, pp. 52-72. http://hdl.handle.net/102.100.100/637002?index=1

Hansen, Flemming Splidsboel. 2017. Cognitive Resilience in Central Asia. In: N. Popescu, & F. Gaub (eds.), After the EU Global Strategy – Building Resilience European Union Institute for Security Studies, 2017, pp. 73-75. http://www.iss.europa.eu/publications/detail/article/after-the-eu-global-strategy-building-resilience/ (13.01.2026)

Heinimann, Hans R. and Hatfield, Kirk. 2017. Infrastructure resilience assessment, management and governance–state and perspectives. In: Linkov, I., Palma-Oliveira, J. (eds) Resilience and Risk. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht, pp. 147-187. https://doi.org/10.1007/978-94-024-1123-2_5

Kaleeva, Tiana; Blagoev, Ivan and Shalamanov, Velizar. 2025. Governance Model and Technology Architecture in Developing Cyber and Cognitive Resilience. In: Digital Technologies for Enhancing Resilience. IOS Press, pp. 227-243.

Kaczmarek, Krzysztof and Cholewińska, Dagmara. 2024. Security and Hybrid Threats. Przegląd Nauk o Obronności, (20):91-100. https://doi.org/10.37055/pno/208458

Kosárová, Dominika; Bízik, Vladimír and Potočňák, Adam. 2024. Cognitive Resilience: Assessing Critical Factors in Military Personnel. Univerzita Obrany. Ustav Strategickych Studii. Obrana a Strategie, 2: 133-156.

Laine, Jussi P. and Petersson, Bo. 2025 Resilience as Adaptive Deterrence in an Era of Strategic Uncertainty. In: Resilience as Deterrence: Towards a Comprehensive Security Panorama, Jussi P. Laine and Bo Petersson (eds.), NATO science for peace and security series. Sub-series E, Human and societal dynamics, ISSN 1874-6276, E-ISSN 1879-8268; 159, IOS Press, pp. 1-19.

Lengnick-Hall, Cynthia; Beck, Tammy and Woznyj, Haley Myers. 2023. What are you Thinking?: Understanding the Cognitive Dimension of Resilience Capacity. In: Resilience in Modern Day Organizations. Routledge, pp. 7-25.

Lesenciuc, Adrian; Nagy, Daniela and Lesenciuc, Simona. 2022. Societal Resilience. Between Resilinece Through Education and Resilience Through War. Redefining Community in Intercultural Context, 10(1), 25-31.

Linkov, I. and Trump, B.D. Resilience and Governance. 2019. In: The Science and Practice of Resilience. Risk, Systems and Decisions. Springer, Cham. https://doi.org/10.1007/978-3-030-04565-4_5

Meghraoui, Loukmane and Belkhamza, Zakariya. 2025. Cognitive Warfare and Cybersecurity: Strategic Implications for Global Security. In: Proceedings of the 19th International Conference on Cyber Warfare and Security 2025, editors Stephanie J. Blackmonand and Saltuk Karahan, pp. 257-264.

Mider, Daniel and Żółtowski, Marcin. 2025. Correlates of Poles' Resilience to Disinformation – Opinions and Countermeasures. Democracy and Security, 1-30. https://doi.org/10.1080/17419166.2025.2525756

Mlejnková, Petra. 2022. Issues of resilience to cyber-enabled psychological and information operations. Vojenské rozhledy, 31.1: 38-50.

Molek-Kozakowska, Katarzyna. 2024. Enhancing Resilience Against War-Related Disinformation: Insights from Diagnostic Studies and Interventions at Polish Schools. Revista Transilvania, 9, 65-76. https://doi.org/10.51391/trva.2024.09.07.

Nawaz, Faisal. 2025. Psychological Warfare in the Digital Age: Strategies, Impacts, and Countermeasures. Journal of Future Building, 2.1: 21-30.

Normandin, Julie-Maude and Therrien, Marie-Christine. 2016. Resilience Factors Reconciled with Complexity: The Dynamics of Order and Disorder. Journal of Contingencies and Crisis Management, 2016, 24(2), 107-118. doi:10.1111/1468-5973.12107.

Parsons, S., Kruijt, A. W., and Fox, E. 2016. A cognitive model of psychological resilience. Journal of Experimental Psychopathology, 7(3), 296-310.

Peptan, Cătălin. 2025. Romania Facing New Vectors of Insecurity: Hybrid Warfare and Artificial Intelligence, Research and Science Today, 2(30), 87-106, doi: 10.38173/RST.2025.30.2.8:87-106.

Picchi, Andrea. 2025. Designing for Cognitive Resilience in Human-AI Teams: A Neuroadaptive Approach to Operational Integrity and Decision Superiority. https://www.researchgate.net/publication/392933806_Designing_for_Cognitive_Resilience_in_Human-AI_Teams_A_Neuroadaptive_Approach_to_Operational_Integrity_and_Decision_Superiority (27.12.2025)

Radu, Raluca.2025. Building Cyber Resilience to Face the Challenges of Cognitive Warfare. In: European Conference on Cyber Warfare and Security. Academic Conferences International Limited, pp. 803-810.

Romanishyn, Alexander; Malytska, Olena and Goncharuk, Vitaliy. 2025. AI-driven disinformation: policy recommendations for democratic resilience. Frontiers in Artificial Intelligence, 8: 1569115. doi:10.3389/frai.2025.1569115.

Semenenko, Oleh; Kin, Oleksandr; Semenenko, Liliia; Remez, Volodymyr; Serhii Mytchenko and Rybak, Dmytro. 2025. Ключові кроки України в системі воєнної та національної безпеки щодо підвищення когнітивної стійкості (2025-2028 рр.): рекомендації у когнітивній та воєнно-економічній сфері/ Key Steps of Ukraine in the Military and National Security System to Increase Cognitive Resilience (2025-2028): Recommendations in the Cognitive and Military-Economic Spheres. Social Development and Security, 15.4: 36-49. https://doi.org/10.33445/sds.2025.15.4.4

Senčar, Igor. 2021. Kognitivni Vidiki Evropskih Varnostnih In Obrambnih Izzivov/ The Cognitive Aspects of Europe's Security and Defence Challenges. Contemporary Military Challenges/ Sodobni Vojaški Izzivi, 23.3. doi:10.33179/BSV.99.SVI.11.CMC.23.3.1.

Šimelytė, Agnė; Vveinhardt, Jolita; Deikus, Mykolas. 2025. Socioeconomic Resilience in The Context of Sustainability: A Comparison of the Nordic and Baltic States. Management Theory and Studies for Rural Business and Infrastructure Development, 47.2: 187-204. ISSN 2345-0355 https://doi.org/10.15544/mts.2025.15.

Staal, M. A., Bolton, A., Yaroush, R., and Bourne, L. 2008. Cognitive performance and resilience to stress. In: Biobehavioral Resilience to Stress. eds. B. J. Lukey and V. Tepe (Boca Raton, FL: CRC Press), 259-299.

Teperik, Dmitri; Jermalavičius, Tomas; Senkiv, Grigori; Dubov, Dmytro; Onyshchuk, Yevhen; Samus, Mykhailo, and Pokalchuk, Oleh. 2018. A Route to National Resilience. Building. Whole-of-Society Security in Ukraine. URL: https://uploads.icds. ee/ICDS_Report_A_Route_oilience-Building. (12.01.2026)

Torabi, Hassan and Ahmadi, Fatemeh. 2025. Cognitive Resilience against Cognitive Warfare Targeting Iran: Components, Analysis, and Enhancement Strategies. Cognitive research of political studies, 2.1: e219219. (09.01.2026)

Teperik, Dmitri; Denisa-Liepniece, Solvita and Bankauskaitė, Dalia. 2025. GLUED: Linking Resilience and Youth Futures in the Baltics. Report. Tallinn Riga Vilnius. 10.13140/RG.2.2.12470.77125, ISBN 978-9908-9709-1-2.

Tossell, C. C.; Spencer, C. A.; Endsley, M. R.; Canham, M.; Steckman, L.; Hayman, A. and Hirshfield, L. 2025. Charting New Frontiers in Cognitive Security: A Human Factors Call to Action. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 0(0). https://doi.org/10.1177/10711813251369366

Vrijkotte, S., Roelands, B., Meeusen, R., and Pattyn, N. 2016. Sustained military operations and cognitive performance. Aerospace medicine and human performance, 87(8), 718-727.

Wigell, Mikael; Mikkola, Harri and Juntunen, Tapio. 2021. Best Practices in the whole-of-society approach in countering hybrid threats. European Parliament Coordinator: Policy Department for External Relations Directorate General for External Policies of the Union. doi:10.2861/379.

Ziehr, S. and Merkt, P.H. 2024. Strategic resilience in human performance in the context of science and education - perspective. Front. Psychiatry, 15:1410296. doi: 10.3389/fpsyt.2024.1410296.

DOI: 10.53477/3045-2309-26-06

SHAPING MINDS FOR SECURITY: COGNITIVE RESILIENCE AND THE STRATEGIC ROLE OF UNIVERSITY EDUCATION IN ROMANIA

Raluca LUȚAI, PhD,
Lecturer, Babeș-Bolyai University, Cluj Napoca, Romania.
E-mail address: raluca.lutai@ubbcluj.ro

Marius GRAD, PhD,
Lecturer, Babeș-Bolyai University, Cluj Napoca, Romania.
E-mail address: marius.grad@ubbcluj.ro

Abstract**:** *In the context of hybrid threats, information warfare, and increasing societal polarisation, cognitive resilience has become a critical dimension of national and societal security. This paper explores the role of university-level security studies programs in building cognitive resilience, with a focused case study on Romania. It argues that higher education institutions, particularly those delivering security and defence-related curricula, function not only as professional training environments but also as strategic actors in strengthening society's resistance to disinformation, manipulation, and hostile influence. The study analyses how cognitive resilience is reflected in the structure, content, and learning outcomes of selected Romanian academic programs in security studies, international relations, and defence education. Using qualitative content analysis of curricula, course descriptions, and institutional mission statements, the research identifies the extent to which these programs address critical thinking, media and information literacy, understanding of hybrid threats, strategic communication, and democratic values. Particular attention is paid to the integration of interdisciplinary approaches that connect security studies with education sciences, psychology, communication, and information technology.*

The findings suggest that while Romanian university programs increasingly incorporate elements related to information security and hybrid threats, cognitive resilience is often addressed indirectly rather than as an explicit educational objective. The paper concludes by proposing a framework for integrating cognitive resilience more systematically into security-related higher education.

Keywords: *cognitive resilience; education; Romania; security studies; undergraduate programs.*

Introduction

The contemporary security environment expanded beyond traditional military confrontation and includes the cognitive domain as a central arena of strategic competition. Scholars emphasise that cognitive warfare targets perception, decision-making, and collective sense-making, using disinformation, narrative manipulation, and hybrid instruments to exploit cognitive vulnerabilities. In this context, cognitive resilience has emerged as a core component of national and societal security, understood as the capacity of individuals and institutions to critically evaluate information, resist manipulation, and formulate coherent responses to complex threats.

Education is increasingly recognised as a primary mechanism for cultivating this resilience. Universities, particularly those offering programs in security studies, play a strategic role in shaping the analytical, normative, and adaptive capacities of future professionals in the security field. In Romania, the evolution of security studies from a predominantly militarised model to a civilian-

academic framework raises an important question: *to what extent do contemporary university programs actively contribute to the development of cognitive resilience?*

This paper addresses this question through a qualitative content analysis of Romanian undergraduate security studies programs. Operationalising cognitive resilience through four analytical dimensions: critical thinking, media and information literacy, understanding hybrid threats, and strategic analysis capacity, the study evaluates how these competencies are integrated into curricula. The findings suggest that while important foundations exist, the articulation of cognitive resilience remains uneven, highlighting the need for a more explicit and coherent curricular integration.

The paper is structured as follows: first section outlines the theoretical framework on cognitive resilience and its relationship to national and societal security, the second section presents the research design, including case selection and methodological approach and the third section maps the institutional landscape of security studies in Romania and analyses the four analytical dimensions within university curricula. The final section discusses the implications of the findings for higher education policies and cognitive resilience, highlighting limitations and directions for future research.

1. Literature review

The contemporary security environment has fundamentally transformed in the last decades. Threats are increasingly targeting the cognitive domain, with all its components - the realm of human perception, decision-making and collective sense-making. Cognitive warfare is seen as "not limited to information operations, social engineering, or a struggle for "hearts and minds", but it should be extended to all areas of activity of individuals and societies, where ideological attacks are possible" (Reczkowski and Lis 2022, 56). Thus, the human mind itself becomes the battlefield, imposing new approaches to building state resilience against cognitive operations. This conceptualisation has been further developed. Ask et al. (2025, 20), propose a unified definition of cognitive security as "the state of having trusted boundaries protecting cognitive assets against all forms of unauthorised influence or access", identifying four interdependent cognitive resilience factors: cognitive agility, machine psychology, neurosecurity, and systems engineering.

Cognitive resilience in the context of national security extends beyond individual psychological resilience to encompass collective cognitive capacities that underpin national sovereignty and societal stability. Moleka (2025, 4) introduces the concept of "Metawar" as a new domain of warfare that synergises cyber, information, psychological, and algorithmic operations to dominate cognitive landscapes, arguing that national security must incorporate cognitive sovereignty and mental-informational resiliency to counter these stealthy, pervasive cognitive operations. Similarly, Taranenko (2024, 382) identifies cognitive security as a crucial dimension of the Russia-Ukraine war, where cognitive warfare aims to affect human cognition, critical thinking, and decision-making, with the goal of building resistance to harmful informational and psychological influences.

The integration of cognitive resilience into security frameworks reflects a recognition that contemporary conflicts operate across multiple domains simultaneously. Recent research demonstrates how cognitive warfare infiltrates and shapes mindsets through reflexive control strategies, undermining resilience and resistance by conveying specially prepared information to adversaries to incline them toward predetermined decisions (Tsikhelashvili 2023, 6). This approach exploits cognitive biases and provokes distortions in decision-making processes, operating covertly to cause distrust and fragmented awareness within target populations.

The urgency of addressing cognitive resilience as a security dimension has been amplified by recent geopolitical developments and technological advances. Senčar (2021, 17) emphasises that an effective response to current security challenges requires a mental shift and strengthening cognitive resilience alongside solidarity, noting that information warfare targeting the cognitive sphere poses particular challenges to open, democratic societies. It is argued that strengthening cognitive resilience

involves enhancing societal situational and threat awareness through critical thinking and democratic deliberation, enabling stronger identification with security strategies.

Empirical evidence from conflict zones underlines the practical importance of cognitive resilience. Semenenko, Kin, Remez et al. (2025, 42-44) outline key steps for Ukraine to enhance cognitive resilience within its society and defence sector from 2025-2028, considering threats from the Russian-Ukrainian war, global information confrontation, and economic challenges. Their research establishes a system of military-economic consequences of cognitive influence and describes measures for Ukraine to increase its cognitive resilience while lawfully influencing adversarial consciousness.

The challenge extends beyond traditional warfare contexts. Grahn, Häkkinen and Taipalus (2024, 170) examined citizen perceptions of cognitive security during Finland's NATO joining process, finding that individuals observed increased attempts at malign influence and internet malfunctions alongside a diminished overall sense of security, though trust in Finnish defence forces remained consistently high. The findings highlight the complex interplay between geopolitical events and cognitive security, emphasising the need for nuanced security approaches in an era of what the authors term "gray instability" (Morris, Mazaar, Hornung et. al. 2019, 7-13).

On the other side, cognitive resilience has emerged as a fundamental component of national sovereignty in the 21st century. A decision-making model to ensure national resilience in the context of hybrid threats is highlighting that such threats specifically target decision-making mechanisms and defining resilience within national security frameworks (Karpenko, Boniar, Semenchuk et. al 2025, 449-452). Their model addresses current vulnerabilities, hostile actors, and risks to national security, offering policy steps to enhance cognitive resilience through robust decision-making processes.

The concept of cognitive sovereignty has gained particular traction in discussions related to national security. Moleka (2025) argues that "not so traditional" security paradigms focused on cyberspace are insufficient, proposing instead a doctrinal framework with five pillars: anticipation, strategic narrative protection, coordinated counter-influence, cognitive recovery, and interagency integration. This framework includes recommendations for creating specialised *Metawar units* and regional coordination mechanisms, particularly for vulnerable regions like Africa, to strengthen defence architectures against evolving cognitive threats.

A different approach provides theoretical insights into building psychological resilience in smaller nations using Significance Quest Theory, exploring individual psychological motivations and capabilities to strengthen national resilience before, during, and after potential invasions (Houck 2024, 5-10). Using Mongolia as a case study with quantitative survey data, Houck demonstrates how smaller nations can preserve sovereignty against stronger powers through strategic cultivation of psychological and cognitive resilience at the population level.

Military organisations have increasingly recognised cognitive resilience as essential to operational effectiveness. Daskalov (2018, 201-202) highlights that hybrid warfare necessitates mental agility and adaptability, making psychological resilience a critical concept for security policy and advocating for resilience training in the Bulgarian military to foster psychological health. It is emphasised a shift from traditional warrior ethos to a comprehensive approach that includes self-awareness, self-regulation and mental agility, aligning with broader NATO military practices. The pedagogical dimensions of cognitive resilience training have also received attention. Hardy (2024, 84-85) examines wargaming as a pedagogical tool for developing cognitive resilience, finding that wargaming as a co-construction process between designers and players fosters reflexive thinking and adaptation crucial for cognitive security. As such, open game design can explore information analysis, communication, decision-making, and resilience both individually and collectively, offering a ludo-pedagogical and strategic research tool for military and security applications. Ducourneau (2024, 90-91) advocates for a design lab approach to cognitive security based on six principles, emphasising that cognitive operations must be founded on an emic understanding of target populations within constrained timeframes for effective deterrence. The author highlights that cognitive resilience requires robust tools for knowledge, training, and exercise, addressing the multi-scale and

interdisciplinary nature of cognitive warfare through design thinking that emphasises creativity, collective intelligence, and cognitive tools.

At national level, there are several nations that have developed comprehensive frameworks integrating cognitive resilience into national security strategies. Hyvönen & Juntunen (2020, 160-169) trace the evolution from "spiritual defence" to robust resilience in the Finnish comprehensive security model, demonstrating how Finland has systematically integrated cognitive and psychological dimensions into its whole-of-society security approach. This model emphasises the importance of societal cohesion, shared values, and collective will as foundations for national resilience. On the other hand, Keinonen (2023, 567-574) explores the concept of comprehensive security as a tool for cyber deterrence, arguing that cognitive resilience forms a critical component of deterrence strategies in the digital age. The author demonstrates how comprehensive security frameworks that integrate cognitive, cyber, and traditional security dimensions create more robust deterrence postures than approaches focused solely on technical or military capabilities.

Wibisono et al. (2025, 3744) examine Indonesia's Sishanta (Universal Defense System) as a whole-of-nation defence strategy rooted in collectivist culture, religiosity, and local wisdom, providing a unique psychological foundation for societal resilience and national unity. The study proposes integrating digital literacy into "Bela Negara" (Defend the State) education and leveraging AI for threat detection to cultivate societal resilience against digital threats like disinformation and psychological operations, though it notes challenges including slow regulatory adaptation and weak non-military coordination (Wibisono, Purwantoro, Duarte 2025, 3745).

Cognitive resilience also plays a crucial role in maintaining democratic institutions and processes. The 2023 report on building resilience in the European Union in times of polycrisis emphasises that cognitive domain challenges - including disinformation, perception management, and psychological manipulation - undermine trust in democratic institutions. The report recommends building resilience through education, media literacy, critical thinking, digital competencies, and mental toughness, alongside applying exponential design to strategic thinking and fostering multilateralism and close cooperation with NATO. Senčar (2021, 18) contrasts the Kantian tradition of thought characterising the European post-Cold War order (democracy, human rights, cooperation) with a Hobbesian or realist vision emphasising systemic competition and conflict. Cognitive resilience is identified as the initial resistance to information warfare, strengthened by critical thinking and societal awareness, and argues that informing and involving electorates in security discussions fosters identification with strategies and strengthens domestic resilience and geopolitical solidarity. Also, cognitive security is defined as both a state and process where malign influence or manipulation cannot alter human cognition, including opinion formation and decision-making (Grahn, Häkkinen, Taipalus 2024, 172). Their research on Finnish citizen perceptions highlights psychological information influence as a crucial aspect within the cognitive dimension, aiming to shape attitudes, emotions, opinions, and decision-making processes. The study reveals that while geopolitical changes may temporarily diminish security perceptions, strong institutional trust can buffer these effects.

Cognitive resilience at the societal level depends fundamentally on social cohesion and community bonds. Zarghooni-Hoffmann and Ylönen (2023, 3549-3552) conceptualise societal security as a system-of-systems, examining customs agencies' cross-sectoral contributions to societal resilience. This systems perspective emphasises the interconnected nature of societal security, where cognitive resilience in one sector can enhance or undermine resilience in others, necessitating coordinated, whole-of-society approaches.

Overall, cognitive resilience has emerged as a critical dimension of both national and societal security in the contemporary threats and vulnerabilities environment. The literature reviewed demonstrates that cognitive resilience operates at multiple levels - individual, community, and national – with each level contributing to overall security capacity. Ultimately, cognitive resilience represents not merely a defensive capability, but a fundamental attribute of healthy, functioning democracies. In an era where the human mind has become a contested domain, cognitive resilience emerges as essential infrastructure for national sovereignty, democratic governance, and social cohesion.

2. Research design

This research has a qualitative design based on content analysis and institutional documentary analysis. This methodological choice is appropriate to the normative and multidimensional nature of the concept of cognitive resilience, which has been established in recent literature as an essential component of national and societal security in the context of the expansion of cognitive warfare and hybrid threats.

Given the growing relevance of cognitive resilience in contemporary security architecture, the research aims to answer the following research question: *To what extent do Romanian university programs in the field of security integrate the concept of cognitive resilience?* Based on an analysis of the specialised literature, the concept is operationalised through four analytical dimensions considered relevant for capturing educational expression.

Firstly: (a) critical thinking, understood as the ability to reflectively evaluate information and resist manipulation, is essential. The literature on cognitive security emphasises that contemporary warfare aims to influence perceptions and decision-making processes by exploiting cognitive vulnerabilities, while "cognitive agility" is seen as the ability to adapt flexibly to dynamic information environments, essential for protecting "cognitive frontiers". In the curricula analysis, this dimension will be quantified by analysing courses that focus on methods and tools for critical analysis and argumentation. Secondly, (b) media and information literacy, which involves the ability to navigate and evaluate the contemporary digital ecosystem. Cognitive warfare uses disinformation and narrative manipulation to fragment social cohesion. Discussions on European resilience highlight media literacy and digital skills as central defence mechanisms in the cognitive domain. This dimension is operationalised by identifying courses or objectives related to strategic communication, combating disinformation, information security, and digital ecosystem analysis. Moving forward, (c)understanding hybrid threats, i.e., knowledge of informational and psychological influence mechanisms, is based on the concept developed by Moleka in the context of the conflict in Ukraine, more specifically that of *Metawar*, which presents a reality of the new type of warfare. More specifically, the authors discuss the fact that contemporary threats combine informational, psychological, and cyber components. In this context, cognitive resilience requires an understanding of the mechanisms of strategic influence and reflexive control. In the analysis, this dimension is reflected in courses dedicated to hybrid warfare, information security, and psychological operations. The final dimension of analysis is (d) strategic analysis capability, reflecting the ability to anticipate, assess risks, and formulate coherent responses in complex security contexts. The comprehensive security models emphasise the integration of the cognitive dimension into decision-making and national security architecture. This dimension is identified through references to strategic planning, public policy analysis, and risk assessment.

The cases were selected through purposive sampling, including higher education institutions in Romania that offer study programs in the field of security, strategic studies, defence, and public order, within civilian universities as well as within military or non-civilian institutions. The choice of this type of sampling is justified by the objective of the research, which does not seek statistical representativeness, but rather the analytical relevance of the selected cases.

Data collection was carried out through documentary analysis of the main curricular instruments that structure the educational process. Thus, the curricula and subject files related to the courses included in the analysed programs were examined. The curricula were used to identify the structure of the programs, the distribution of subjects, and the weight of courses relevant to the dimensions of cognitive resilience. The subject files allowed for a detailed analysis of educational objectives, targeted skills, thematic content, and assessment methods. The analysis focused on explicit formulations regarding the skills developed (e.g., critical thinking, strategic analysis, information assessment), as well as on thematic content associated with hybrid threats, information security, or strategic communication. The use of these official documents ensures access to the formal curriculum

of the programs and allows for a systematic and comparable assessment of how cognitive resilience is integrated at the institutional level.

3. The ecosystem of higher education institutions in Romania

The higher education system in Romania is characterised by significant institutional diversity, structured according to the academic profile and educational mission of each category of institution. This structure reflects both the historical university tradition and the transformations that have taken place since 1990 in the context of educational reforms and alignment with European standards.

Multidisciplinary universities are at the core of the Romanian university system. These institutions have a long academic tradition and a major national impact, offering study programs in a wide range of fields, from social sciences and humanities to exact and technical sciences. They function as centers of advanced research and attract a significant number of students, constituting central landmarks in the national academic architecture. Technical and polytechnical universities specialised in engineering and applied sciences, play an essential role in training specialists in infrastructure development and management, information technology, and industrial systems. In the context of digital transformation and the growing importance of cybersecurity, these institutions also contribute indirectly to strengthening national technological security capabilities. Medical, pharmaceutical, and veterinary universities are centers of training and research in the field of health, integrating teaching with professional practice and biomedical research. Their role is essential for strengthening the national health infrastructure and developing professional expertise in strategic areas. Universities of arts, music, and sports have a specialised profile, focusing on creative and performing arts. Although more limited in terms of disciplinary scope, they contribute to strengthening cultural identity and the symbolic dimension of social cohesion, which are relevant elements in discussions on societal resilience.

A distinct category is represented by institutions focused on governance and public policy, which offer programs in public administration, economics, or political science. These have a narrower profile, but play an important role in training decision-makers and specialists in the public sector.

Private universities, developed mainly after 1990, have contributed to expanding access to higher education and diversifying academic offerings. Although the level of quality varies, they have stimulated institutional competition and are present in many university centers, offering programs in law, management, and finance in particular.

Finally, military higher education institutions occupy a distinct position in the system, being responsible for training personnel in the fields of defence, public order, and national security. Each academy covers a specific operational area, contributing directly to the development of strategic culture and national security architecture. The field of security is approached from both an operational and strategic perspective, integrating components such as information analysis, cybersecurity, and risk assessment.

4. Institutionalisation of Security Studies in Romania: From Militarised to Civilian Models

The evolution of security studies in Romania reflects the broader political and institutional transformations of the Romanian state over the past decades. During the communist period, one could hardly speak of security studies as an autonomous academic field in the Western sense. Security-related knowledge production was highly centralised, ideologised, and institutionally fragmented, with the Department of State Security (*Securitate*) playing the dominant role in the intelligence and internal security domain, while the Ministry of National Defence primarily managed the military dimension.

In the immediate post-1989 period, the dissolution of the *Securitate* and the creation of new intelligence structures (notably the Romanian Intelligence Service) opened the way for the gradual institutionalisation of security and intelligence studies. Early academic efforts in this field were

largely developed within institutions affiliated with the newly created intelligence community, such as the High Institute of Intelligence (1992) and later The Mihai Viteazul National Intelligence Academy (ANIMV), before the progressive expansion of civilian academic programs in the 2000s.

The process of Euro-Atlantic integration has generated significant pressure for conceptual and institutional reform in the field of security. Romania's accession to NATO in 2004 and to the European Union in 2007 required alignment with Western standards on democratic control of the security sector, transparency, and professionalisation of public administration. In this context, it became clear that training was needed not only for military personnel, but also for civilian specialists in fields such as international relations, security policy, defence studies, and strategic analysis. Thus, the first civilian security studies programs appeared at universities such as Babeș-Bolyai University, the University of Bucharest, and the National School of Political and Administrative Studies (SNSPA). The Mihai Viteazul National Intelligence Academy (ANIMV), coordinated by the Romanian Intelligence Service, played a particular role at this stage. Although integrated into an institutional structure specific to the security sector, ANIMV developed programs accredited in the national higher education system, representing a bridge between the traditional militarised model and the emerging academic model.

After joining the European Union, security studies in Romania have gradually gained ground in civilian academia. The topics covered have diversified to include national security, international security studies, cybersecurity, energy security, and societal security.

Universities have become relevant actors in the production of expertise and strategic analysis, and the involvement of civil society and the academic community in the public debate on security has increased significantly. At the same time, the interdisciplinary dimension of the programs has been emphasised by integrating perspectives from political science, law, economics, sociology, and communication sciences. Internationalisation has been another defining feature of this phase, through participation in programmes such as Erasmus and projects funded by the European Union. These processes have contributed to the consolidation of democratic values and the strengthening of the principle of civilian control over the security sector, considered an essential standard of democratic governance.

Overall, the institutionalisation of security studies in Romania highlights a transition from a model focused on operational and doctrinal training to an academic, interdisciplinary model oriented toward critical analysis and integration into the Euro-Atlantic knowledge space.

5. Dimensions of cognitive resilience in the curriculum of security programs in Romania

Security studies programs are offered by a diverse number of higher education institutions in Romania, both public and private, distributed relatively evenly across the country. From an institutional perspective, most programs are hosted by large public universities with a multidisciplinary profile and a strong academic tradition. Relevant examples include Babeș-Bolyai University in Cluj-Napoca, the University of Bucharest, and the West University of Timișoara. These institutions are major university centers with extensive research capacity and a large number of students, which provide security programs with a stable and interdisciplinary academic framework. Alongside these, there are also medium-sised public universities, such as Lucian Blaga University in Sibiu or the University of Oradea, which integrate security studies into faculty structures with a socio-human profile.

Geographically, the programs are distributed across the country's main university centres: Cluj-Napoca (Transylvania), Bucharest (southern region), Timișoara and Arad (west), Sibiu (center), Oradea (northwest), as well as other university cities. This dispersion indicates a relative regional balance in the academic offer in the field of security, avoiding exclusive concentration in the capital. At the same time, the presence of a program in a private university (the "Vasile Goldiș" Western University of Arad) reflects the expansion of the field into the non-public sector.

In terms of institutional framework at faculty level, security studies programs are predominantly placed in faculties specialising in political science, governance sciences, international relations, social sciences and humanities. For example, at Babeș-Bolyai University, the program is integrated into both

the Faculty of History and Philosophy and structures associated with political and administrative sciences. At the University of Bucharest, security studies are associated with the Faculty of Political Sciences, while at other universities they are integrated into faculties of social sciences or governance sciences. This positioning confirms the predominantly civil and analytical nature of the programs, with an emphasis on the political, strategic, and societal dimensions of security.

At the same time, there are also military or non-civilian institutions (such as the *Carol I National Defence University* or the *Mihai Viteazul National Intelligence Academy*) that offer bachelor's degree programs in security or intelligence. However, these operate within a distinct institutional framework, geared towards professional training specific to the defence and security sector.

The broad geographical distribution of security studies programs, their integration into multidisciplinary civilian universities, and their predominant placement in political science and social sciences departments are directly important for strengthening cognitive resilience at the societal level. Firstly, placing these programs in civilian academic environments promotes the development of critical thinking, normative reflection, and democratic debate, which are essential elements for resistance to information manipulation and hostile influence. Second, the interdisciplinary nature of the faculties in which they are integrated, which connects security with political science, communication, sociology, or law, allows hybrid threats to be addressed in a complex, not exclusively operational, manner. Last but not least, the regional distribution of programs helps to avoid the concentration of expertise in the capital alone and supports the formation of a culture of security that extends nationwide. In this sense, the civil-academic institutionalisation of security studies is not only a structural evolution of the university system, but also an indirect mechanism for strengthening cognitive resilience in society.

Critical thinking

Data analysis indicates that critical thinking is one of the most consistent dimensions present in bachelor's degree programs in the field of security studies. It is present in almost all the institutions and programs analysed. The presence of this dimension is not accidental. Within the national quality assurance standards formulated by Romanian Agency for Quality Assurance in Higher Education (ARACIS)[1], the development of critical analysis, argumentation, and information evaluation skills is a central criterion for the accreditation of programs in the field of political science and security studies. The evaluation standards emphasise the need to train graduates who are able to critically interpret political and strategic realities, use appropriate theoretical concepts, and formulate reasoned judgments. Thus, critical thinking is not only a pedagogical objective but also a formal indicator of academic quality.

From the perspective of cognitive resilience, the importance of this dimension is fundamental. The literature shows that cognitive warfare and hybrid threats target precisely the vulnerabilities of perception and decision-making processes, exploiting cognitive biases and analytical deficits. The development of critical thinking contributes to an individual's ability to evaluate information sources, identify narrative manipulation, and distinguish between facts, interpretations, and propaganda. In this sense, the skills cultivated in university programs, comparative analysis, logical argumentation, and reflection on the decision-making process become mechanisms of protection against information distortions. One limitation of this is that critical thinking is often approached in a general manner, without a direct connection to the specific issues of information manipulation, cognitive warfare, or strategic influence. From the perspective of cognitive resilience, the simple development of analytical skills is not sufficient; their explicit contextualisation in relation to contemporary information vulnerabilities is necessary.

Therefore, the systematic inclusion of critical thinking in the curriculum of security studies programs is not only a compliance with ARACIS standards, but also a direct contribution to strengthening cognitive resilience at the individual and societal levels. Training graduates who are able to rigorously analyse the security environment and critically evaluate information is becoming

[1] Romanian Agency for Quality Assurance in Higher Education is an independent Institution who carries out the quality external evaluation of education provided by higher education institutions which operates in Romania.

essential for maintaining decision-making coherence and democratic stability in an increasingly complex information context.

Media literacy

The second dimension analysed, media and information literacy, understood as the ability to critically evaluate digital sources, understand the mechanisms of information propagation, and identify manipulation techniques, appears in our analysis in a significantly less consolidated form than critical thinking, although the literature considers it one of the most important components of cognitive resilience in the current context of information warfare and hybrid threats.

In some universities, this dimension is explicitly present, through disciplines such as "Disinformation and Propaganda", "Communication and Public Relations", "Transparency and Security in the Digital Society", or courses focusing on intercultural communication and digital environment analysis. For example, Babeș-Bolyai University makes direct references to disinformation and strategic communication, while the University of Bucharest includes topics related to security in the digital society. These examples indicate a certain institutional sensitivity to the issues of the contemporary information environment.

In contrast, at other universities, such as the University of Oradea or Lucian Blaga University in Sibiu, media literacy is taught more indirectly, through general courses on communication or public policy, without an explicit focus on disinformation, algorithmic manipulation, or the digital ecosystem. In these cases, the media dimension does not appear as an autonomous curricular pillar, but as a marginal element integrated into broader disciplines.

This variability suggests that media literacy is not yet a consolidated curricular dimension at the national level in the field of security studies. Unlike critical thinking, media literacy does not enjoy the same normative visibility or clear operationalisation in quality criteria. It is often subsumed under general communication or analysis skills, without being treated as a distinct field. This situation is problematic from the perspective of cognitive resilience. The literature on cognitive security emphasises that the digital information environment is the main space for influence operations, disinformation, and narrative manipulation. Cognitive vulnerabilities are amplified by algorithms, online polarisation, and information overload. In this context, media literacy becomes an essential infrastructure for democratic security.

Compared to critical thinking, media literacy is less developed and less systematically integrated into the curricula of the programs analysed. This discrepancy indicates a potential structural vulnerability: universities develop general analytical skills, but do not always anchor them sufficiently in the reality of the contemporary digital information environment. Therefore, strengthening media literacy should be a strategic priority for security studies programs. The integration of courses dedicated to disinformation, information security, analysis of digital ecosystems, and the impact of emerging technologies would significantly contribute to strengthening cognitive resilience, both at the individual and societal levels. Without such reinforcement, there is a risk that security training will remain partially disconnected from one of the most pressing dimensions of contemporary threats.

Hybrid threats

The third dimension analysed, understanding hybrid threats, is relatively well represented in bachelor's degree programs in the field of security studies, but with significant differences in depth and structure between universities.

In several institutions, this dimension is integrated through dedicated disciplines or clear thematic modules. For example, at Babeș-Bolyai University, there are courses such as "Fundamental Problems of the Contemporary World" or "Analysis of Unconventional Risks to Security". The University of Bucharest includes topics such as "Analysis and Resolution of International Conflicts", while other universities offer courses on "Conflict Management" or "Introduction to Security

Studies". These provide a conceptual framework for understanding the interaction between the military, political, economic, and informational dimensions of contemporary conflicts.

In medium-sised universities (e.g., Oradea, Sibiu), hybrid threats are addressed mainly through general security or public policy courses, without necessarily having courses explicitly dedicated to the concept of "hybrid warfare" or "cognitive warfare". In these cases, the analysis remains predominantly theoretical and less anchored in the concrete instruments of strategic influence or information manipulation.

Militarised institutions or those with a national security profile tend to approach this dimension in a more operational manner, with an emphasis on risk assessment, strategic analysis, and applied national security. In contrast, civilian universities favor an analytical and interdisciplinary approach, focused on international relations, security policies, and conflict dynamics.

From the perspective of ARACIS quality standards, addressing contemporary security issues and developing the ability to analyse the international environment are essential skills for specialisations in this field. However, data analysis suggests that the term "hybrid threats" is not always used explicitly, often being subsumed under more general formulations regarding international security or global conflicts.

This dimension plays a major role in strengthening cognitive resilience. The literature emphasises that hybrid threats combine military, informational, economic, and psychological tools, aiming to influence society's perceptions and decisions. Understanding the mechanisms by which state and non-state actors use disinformation, economic pressure, social polarisation, or cyber tools contributes to the development of critical awareness of the security environment.

However, the analysis reveals an important limitation: in many programs, hybrid threats are addressed primarily from a geopolitical or strategic perspective, without sufficient integration of the cognitive dimension, i.e., the impact on perceptions, public opinion, and democratic processes. Thus, although the topic is present at the conceptual level, the direct connection with cognitive resilience is not always explicit.

As a preliminary conclusion, the dimension of hybrid threats is relatively well represented in the curriculum, but there are differences in depth and articulation between universities. Strengthening this component through more integrated approaches, connecting strategic analysis with the informational and psychological dimensions, could significantly amplify the contribution of security studies programs to the development of cognitive resilience at the societal level.

Strategic analysis capacity

The last dimension analysed, strategic analysis capacity, is one of the most consistently represented components in bachelor's degree programs in the field of security studies. It appears both in dedicated disciplines, such as "Strategic Analysis", "Introduction to Security Studies", "Public Policy", or "Decision-Making Processes", and in courses that develop risk assessment and public policy option formulation skills.

At large universities, such as Babeș-Bolyai University or the University of Bucharest, strategic analysis is integrated into a solid theoretical framework, associated with international security studies and comparative public policy. Courses such as "Comparative Public Policy" or "Decision-Making Processes" contribute to the formation of a structural understanding of how national and international strategies are developed and implemented. At the West University of Timișoara and other regional universities, strategic analysis is present in disciplines focused on governance, conflict management, and strategic planning.

Military and national security institutions tend to approach this dimension in a more applied and operational manner, with an emphasis on strategic planning, doctrine, and risk assessment. In contrast, civilian universities favor conceptual analysis, comparison between policy models, and reflection on decision-making processes in democratic contexts.

In relation to cognitive resilience, this dimension has structural relevance. If critical thinking protects individuals against manipulation and media literacy helps them navigate the information environment, strategic analysis contributes to the ability to understand the systemic dynamics of threats and formulate coherent responses. It develops the ability to anticipate, evaluate scenarios, and integrate multiple pieces of information into a strategic perspective, reducing the risk of impulsive or fragmented responses to crises.

However, data analysis suggests that, in some programs, strategic analysis is approached predominantly at a theoretical level, without sufficient practical exercises (such as simulations, in-depth case studies, or prospective scenarios). In the absence of a robust practical component, there is a risk that this dimension will remain at a conceptual level, without fully developing the adaptive response capacity needed in a volatile security environment.

In conclusion, strategic analysis skills are one of the best-integrated dimensions in the security studies programs analysed. However, strengthening the applied components and connecting them more explicitly to the cognitive dimension of security could significantly amplify their contribution to the development of cognitive resilience at the individual and societal levels.

6. Limitations of the research. Future research directions

This research has a number of methodological and conceptual limitations that must be taken into account when interpreting the results. First, the analysis was based exclusively on formal curriculum documents (curriculum plans and subject descriptions). This approach captures the stated curriculum, but does not allow for an assessment of the implemented curriculum or actual teaching practices. It is possible that certain competencies associated with cognitive resilience are developed informally, through teaching methods or extracurricular activities, without being explicitly reflected in the documents analysed. Secondly, the research did not assess the actual impact of the programs on students. The presence of a subject or skill in the course description does not guarantee the effective internalisation of critical analysis, media literacy, or strategic evaluation skills. The lack of empirical tools (questionnaires, interviews, competency tests) limits the ability to measure training outcomes in terms of effective cognitive resilience.

Based on these limitations, future research could adopt a mixed methodological design, combining documentary analysis with empirical methods. The use of questionnaires or interviews with students and teachers would allow for the assessment of perceptions of the skills developed and how they effectively contribute to cognitive resilience. Another relevant direction would be to conduct an international comparative analysis to assess the extent to which Romanian programs align with best practices in the Euro-Atlantic area. A comparison of curricula with universities in NATO or EU member states could highlight gaps or innovative models for integrating media literacy and the cognitive dimension of security.

Conclusions

The analysis carried out in this research must be placed in relation to recent theoretical developments that define cognitive resilience as an essential component of national and societal security. The literature highlights the fact that the contemporary security environment has expanded beyond the traditional military dimension to include the cognitive domain as a space for strategic competition. Conceptualisations of cognitive warfare, hybrid threats, and information security emphasise that current vulnerabilities target not only physical or digital infrastructures, but also the processes of perception, interpretation, and decision-making of individuals and communities. In this theoretical framework, cognitive resilience is understood as the set of skills that enable the identification of manipulation, the critical evaluation of information, and the formulation of coherent strategic responses.

Based on this conceptual framework, the research analysed the extent to which Romanian university programs in the field of security integrate dimensions associated with cognitive resilience. The results indicate the existence of solid foundations, particularly in terms of critical thinking and strategic analysis, but also relevant gaps, especially in the field of media literacy and the explicit articulation of the cognitive dimension of hybrid threats. Thus, the conclusions must be interpreted in light of the theoretical framework that asserts that university education is one of the essential infrastructures for strengthening democratic security in an increasingly complex information environment.

An analysis of the four dimensions - critical thinking, media and information literacy, understanding hybrid threats, and strategic analysis - indicates that bachelor's degree programs in security studies in Romania integrate elements relevant to the development of cognitive resilience, but in an uneven manner and, in some cases, implicitly rather than explicitly.

Critical thinking and strategic analysis are the best represented dimensions, supported both by the disciplinary tradition of political science and security studies, and by the formal requirements of ARACIS standards regarding analytical and argumentative skills. However, in many cases, these competences are formulated in generic terms, without a detailed methodological clarification of how they are cultivated and assessed. There is a risk of declarative formalisation, in which objectives are assumed at the curricular level but not always supported by appropriate pedagogical practices.

Understanding hybrid threats is relatively consistent, particularly in the fields of international security, conflict studies, and public policy. However, the concept of "hybridity" and the cognitive dimension of threats are not always explicitly addressed. Analysis often remains at the geopolitical or general strategic level, without sufficiently integrating the impact on perceptions, decision-making processes, and societal cohesion.

The most vulnerable dimension is media and information literacy, which, although essential for cognitive resilience in the digital age, is poorly structured and insufficiently institutionalised in many of the programs analysed. It appears fragmentarily, through communication courses or references to disinformation, but is rarely treated as an autonomous curricular pillar. This gap is significant, given that the information environment is the main arena for contemporary cognitive warfare.

Overall, it can be said that undergraduate security studies in Romania contain important foundations for the development of cognitive resilience, but this is not formulated as a coherent and integrated curricular objective. The dimensions analysed exist, but they are scattered and not articulated within a unified conceptual framework. The explicit consolidation of cognitive resilience as a cross-cutting educational objective, through the clearer integration of media literacy, the cognitive dimension of hybrid threats, and applied pedagogical methods, could transform these programs from mere spaces for analytical training into veritable academic infrastructures for societal security.

In order to strengthen the contribution of security studies programs to the development of cognitive resilience, it is necessary, first of all, to explicitly formulate it as a cross-curricular objective. This would require the coherent integration of the four dimensions analysed into a unified conceptual framework, rather than merely mentioning them fragmentarily in the course descriptions. The introduction of courses dedicated to media literacy and combating disinformation, the development of applied modules on cognitive warfare and hybrid threats, as well as the use of interactive methods (simulations, wargaming exercises, case studies on manipulation and information) would contribute to the transition from a predominantly theoretical model to a formative and adaptive one. In this regard, updating ARACIS standards could include clearer references to digital skills and the cognitive dimension of contemporary security.

BIBLIOGRAPHY:

Ask, T., S. Sütterlin, L. Müller, and R. Lugo. "Cognitive Security: The Study and Practice of Protecting the Human Mind and Other Cognitive Assets from Cognitive Threats." PsyArXiv preprint, 2025. https://osf.io/preprints/psyarxiv/2ftqc_v1

Brassett, J., et al. "Security and the Performative Politics of Resilience: Critical Infrastructure Protection and Humanitarian Emergency Preparedness." *Security Dialogue* (2015). https://doi.org/10.1177/0967010614555943.

Daskalov, D. "Hybrid Warfare and the Challenge It Poses to the Psychological Resilience Training in the Bulgarian Military." *Information & Security: An International Journal* (2018). https://doi.org/10.11610/ISIJ.3917.

Ducourneau, J. "Un Design Lab. pour la Sécurité Cognitive." *Ingénierie Cognitique*, 2024. https://doi.org/10.21494/iste.op.2024.1094.

Grahn, S., et al. "Cognitive Security in a Changing World: Citizen Perceptions During Finland's NATO Joining Process." *Proceedings of the European Conference on Information Warfare and Security*, 2024. https://doi.org/10.34190/eccws.23.1.2158.

Hardy, M. "(War)gaming: Les Questions Pédagogiques comme Enjeu de Résilience Cognitive." *Ingénierie Cognitique*, 2024. https://doi.org/10.21494/iste.op.2024.1093.

Houck, S. "Building Psychological Resilience to Defend Sovereignty: Theoretical Insights for Mongolia." *Frontiers in Social Psychology* 2 (2024). https://doi.org/10.3389/ frsps.2024.1409730.

Hyvönen, A., et al. "From 'Spiritual Defence' to Robust Resilience in the Finnish Comprehensive Security Model." In *Nordic Societal Security: Convergence and Divergence*, edited by Sebastian Larsson and Mark Rhinard, 154-178. London: Routledge, 2020. https://doi.org/10.4324/9781003045533-11.

Karpenko, O., S. Boniar, T. Semenchuk, Y. Osypova, N. Pakhota, and N. Reznik. "A Decision-Making Model to Ensure National Resilience in the Context of Hybrid Threats." In *The Future of Work: How Technology Is Transforming Jobs and Skills*, edited by R. El Khoury, Studies in Systems, Decision and Control, vol. 291. Cham: Springer, 2025. https://doi.org/10.1007/978-3-031-87372-0_39.

Keinonen, K. "The Concept of Comprehensive Security as a Tool for Cyber Deterrence." In *Proceedings of the 22nd European Conference on Cyber Warfare and Security*, vol. 22, no. 1, 2023. https://doi.org/10.34190/eccws.22.1.1254.

Lesenciuc, A., D. Nagy, and S. Lesenciuc. "Building Resilience in the European Union in Times of Polycrisis and Challenges in the Cognitive Domain." In *Redefining Community in Intercultural Context*, vol. 10, no. 1, 2023.

Moleka, P. "Metawar and the Future of Cognitive Sovereignty: Rethinking National Security Beyond Cyberspace." *Preprints*, 2025. https://doi.org/10.20944/preprints202506.2053.v1.

Reczkowski, R., and A. Lis. "Cognitive Warfare: What Is Our Actual Knowledge and How to Build State Resilience?" *Bezpieczeństwo. Teoria i Praktyka* 48, no. 3 (2022): 51–61. https://doi.org/10.48269/2451-0718-btip-2022-3-003.

Sencar, M. "The Cognitive Aspects of Europe's Security and Defence Challenges." *Communications and Mobile Computing*, 2021. https://doi.org/10.33179/BSV.99.SVI.11.CMC.23.3.1.

Taranenko, A. "Cognitive Security as a Dimension of Russia-Ukraine War." *Politology Bulletin*, no. 92 (2024): 371-382.

Tsikhelashvili, N. "Cognitive Warfare through Reflexive Control Strategy in Georgia." *The Defence Horizon Journal*, 2023. https://doi.org/10.5281/zenodo.8374123.

Wibisono, S., et al. "Psychological Dimensions of Sishanta for Societal Resilience and National Unity in the Digital Defense Era." *Formosa Journal of Multidisciplinary Research* 4, no. 8 (2025): 3733–3750. https://doi.org/10.55927/fjmr.v4i8.353.

Zakharov, M. Y., I. E. Starovoitova, and A. V. Shishkova. "Cognitive Security in the Digital Age: Types, Levels, Functions." In *Socio-economic Systems: Paradigms for the Future*, edited by E. G. Popkova, V. N. Ostrovskaya, and A. V. Bogoviz, Studies in Systems, Decision and Control, vol. 314. Cham: Springer, 2021. https://doi.org/10.1007/978-3-030-56433-9_93.

Zarghooni-Hoffmann, J., et al. "Societal Security as a System-of-Systems: Customs Agencies' Cross-Sectoral Contributions." In *Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)*, Southampton, UK, September 3-8, 2023. https://doi.org/10.3850/978-981-18-8071-1_p381-cd.

SECTION II
STATE AND NONSTATE ACTORS IN POWER RELATIONS

DOI: 10.53477/3045-2309-26-07

MANUFACTURING THREAT AND FRIENDSHIP: NORTH KOREAN STATE MEDIA AND THE EMERGENCE OF A STRATEGIC PARTNERSHIP WITH RUSSIA

Jana CHAMROVA,
PhD Candidate, Faculty of Arts, History and Culture of Asian Countries, Charles University,
Consultant at the Korea-Europe Network, Prague, Czech Republic.
E-mail address: jana.chamrova@ff.cuni.cz

Abstract*: This paper examines how North Korean state media has reflected and discursively constructed the deepening relationship between the Democratic People's Republic of Korea (DPRK) and the Russian Federation in the context of Russia's war in Ukraine. While public debate often emphasises material cooperation, this study argues that DPRK media provides evidence of a gradual, strategic alignment, built through narrative cues, historical analogies and ideological framing that present Russia as a principled partner confronting the West. Using a constructed four-week sample of Korean-language articles from 2015 and 2025, this research combines qualitative content analysis with critical discourse and narrative analysis to trace how Russia's function in DPRK discourse shifts from relatively routinized "friendship" to a more central role as legitimating authority, moral ally and counter-hegemonic pole. The findings suggest that North Korean media is not merely reporting cooperation but actively stabilising a worldview in which DPRK–Russia partnership belongs to a polarised international order.*

Keywords*: North Korea; Russia; state media; strategic partnership; polarization; security discourse.*

Introduction

Russia's war against Ukraine has had global repercussions well beyond the European security environment. For North Korea, the conflict has provided not only an opportunity for diplomatic positioning but also a discursive resource through which the regime articulates its vision of the international order in the context of DPRK-Russia relations (Armstrong 2013; Cha 2012; Toloraya 2025). This paper explores how North Korean state media represents the evolving relationship between Pyongyang and Moscow, arguing that media narratives reveal the gradual emergence of a strategic partnership rather than a temporary alignment of convenience. In doing so, the study sheds light on the ideological framing behind Pyongyang's portrayal of Russia as both a trusted friend and a fellow antagonist of the West. North Korean media, long used to manufacture a sense of external threat and embattled solidarity, appears to be "manufacturing friendship" with Russia as a natural counterpart to those threats.

The focus on 2015 versus 2025 provides a baseline and a contrast at the same time. In 2015, DPRK–Russia ties were cordial and commemorative, however Russia was not consistently positioned as an indispensable strategic "co-protagonist" in DPRK worldmaking. By 2025, after years of intensified confrontation between Russia and the West, DPRK media increasingly frames Russia as a morally aligned partner whose struggle mirrors North Korea's own confrontation with "hostile forces". In this sense, the DPRK press appears to be doing two things at once: manufacturing threat (by reiterating an embattled worldview) and manufacturing friendship (by narratively stabilising Russia as a principled ally).

This paper contributes to security-oriented media research by treating DPRK news not only as propaganda, but also as political storytelling: a genre in which states become characters with narrative roles. Rather than measuring "bias" as deviation from factual reporting, the analysis examines how Russia is made meaningful through repeated discursive functions, narrative roles and storytelling strategies.

1. Framing Alliance and Threat in North Korean State Media

North Korean state media has historically played a central role in constructing external threat perceptions and legitimising foreign policy choices. By examining these narratives, this study contributes to understanding how North Korea interprets global polarisation and positions itself within an emerging multipolar or bipolar order. Prior scholarship has documented North Korea's adept use of propaganda to justify its policy and isolate domestic audiences from alternative viewpoints (Armstrong 2013; Lankov 2014). However, less attention has been paid to how allies are framed in DPRK discourse. The DPRK's relations with Russia have fluctuated since the Cold War, from the patron-client dynamics of the Soviet era to estrangement in the 1990s and cautious engagement in the 2000s (Wishnick 2003).

Recent developments point to a qualitative deepening of DPRK–Russia relations that goes beyond diplomatic symbolism. Since the outbreak of Russia's full-scale war in Ukraine, Pyongyang and Moscow have not only aligned positions on major international issues and intensified high-level exchanges, but have also been widely reported to engage in material cooperation linked to the conflict, including the supply of munitions and the deployment of North Korean personnel in support roles. These developments have led a growing number of analysts to describe the relationship as an emerging quasi-alliance, reviving patterns of bloc-based alignment reminiscent of the Cold War. As Toloraya (2025) notes, under conditions of sustained rivalry with the United States and its allies, the DPRK–Russia relationship increasingly appears "built to last".

Against this backdrop, this paper situates its inquiry at the intersection of media studies and international security. Rather than assessing the operational or military effectiveness of DPRK–Russia cooperation, it examines how Pyongyang's official media discursively constructs this partnership and embeds it within a broader narrative of global polarisation. State-controlled media in the DPRK serves as the primary conduit for these narratives. Previous studies on North Korean propaganda (e.g., Myers 2010 on racialised nationalist narratives) show that portrayals of foreign countries can reveal Pyongyang's strategic intentions. For instance, media depiction of China tends to emphasise fraternal ties but carefully avoids suggesting North Korean dependence, reflecting a concern for equal footing. How, then, is Russia depicted when it shifts from being a secondary partner to a potential "comrade-in-arms"?

Research Design Research Design and Analytical Framework

The corpus consists of Korean-language state media texts collected via a constructed-week sampling strategy, designed to capture routine patterns while avoiding overrepresentation of single events. The study analyses four constructed weeks: two from 2015 (H1 and H2) drawn from Rodong Sinmun, the Korea Workers' Party daily; and two from 2025 (H3 and H4) drawn from the Korea Central News Agency, the DPRK's official news agency, comprising approximately 850 news items.[1] The 2015 weeks serve as a baseline for the intensity and function of Russia references prior to the major post-2022 geopolitical shift; the 2025 weeks capture discourse under conditions of heightened polarisation and wartime alignment.

The analysis follows the discourse-analytical tradition that treats media texts as sites of ideological encoding (Fairclough 1995; van Dijk 2008). Articles were examined through close qualitative reading using a multi-layered coding framework developed iteratively after an initial pilot reading of the corpus. Drawing on Critical Discourse Analysis (CDA) and narrative theory, particularly Propp's concept of narrative roles (Propp 1968), the framework captures not only the presence of Russia in DPRK media but the functions, roles and meanings assigned to it. Combining CDA with narrative analysis allows the study to conceptualise Russia not merely as an external actor,

[1] KCNA was used for the 2025 constructed weeks due to archival availability. KCNA functions as the primary distributor of official DPRK news and substantially overlaps with Rodong Sinmun in political and foreign-policy reporting. This choice follows the design of a wider doctoral project and does not affect the study's focus on discursive patterns.

but as a discursive construct, i.e. a character within North Korea's political storytelling about the international order.

The analysis operates across three analytical layers. First, it identifies the *discursive functions* Russia serves in the text, such as external legitimation, moral alignment, or counter-hegemonic positioning. Second, it examines the *narrative roles* attributed to Russia, treating foreign actors as characters within North Korea's political storytelling (e.g., helper, comrade-in-arms or symbolic supporter). Third, it analyses *storytelling strategies* through which these portrayals are stabilised, including temporal compression (linking past, present, and future), personalisation and silencing or omission of contradictory information.

Rather than assigning each article to a single category, the analysis identifies dominant patterns across the corpus and illustrates them through recurring lexical cues and formulations. All translations from Korean belong to the author. Quoted expressions represent recurrent discursive patterns observed across the constructed-week samples rather than isolated verbatim statements. This approach allows the study to trace shifts in the meaning and function of Russia in DPRK media discourse over time, while remaining sensitive to the highly ritualised and formulaic nature of North Korean state reporting.[2]

2. Findings and Analysis: From "Friend" to "Comrade" – Evolving Portrayals of Russia (2015 vs 2025)

In 2015, North Korean media references to Russia were cordial and ceremonial, stressing *traditional friendship* and cooperation, but typically in a muted, routinised fashion. Russia was one of several friendly nations mentioned and often appeared in contexts like cultural exchanges, messages on anniversaries or foreign news commentary about U.S. actions. By 2025, the tone and intensity of Russia's portrayal had transformed. Russia is now depicted as a central strategic partner, morally aligned with North Korea against common adversaries. The frequency and prominence of Russia-related stories increased and the language grew more ideological (anti-imperialist) and fraternal. In what follows, we dissect these changes through the layers of discursive functions, narrative roles and storytelling strategies, using illustrative examples from the corpus.

2.1. Discursive Functions: What Russia does in DPRK discourse

This section maps what Russia *does* in DPRK discourse, tracing a shift from largely routinised mention in 2015 to more explicit strategic meaning-making in 2025.

2.1.1. External Legitimation

In both 2015 and 2025, Russia functions as a source of external validation for the North Korean regime, but the visibility and intensity of this legitimation change markedly over time. In 2015, such validation was largely implicit. DPRK media highlighted favorable coverage by Russian outlets such as TASS or Pravda of Kim Jong-un's activities, suggesting that international recognition, especially from Russia, conferred prestige and legitimacy. Occasional reports of formal greetings from Russian political figures, including leaders of the Russian Communist Party and the LDPR, further signaled recognition, though the language remained restrained and procedural rather than overtly propagandistic.

By 2025, external legitimation becomes explicit and celebrated. DPRK media prominently reports Russian endorsement of North Korean positions in international forums, including opposition to UN resolutions and affirmation of Pyongyang's right to self-defence. Such instances are framed as Russia validating North Korea's stance as just and strategically sound. This elevation is reflected in

[2] Given the qualitative, discourse-analytic focus of the study and the instability of DPRK media archives, individual articles are not cited separately in the analysis. Instead, examples are attributed to the relevant corpus year (2015 or 2025), which is sufficient for analytical distinction and replication within the constructed-week framework.

official language: a 2025 KCNA report quoting Foreign Minister Choe Son-hui describes relations with Russia as a "powerful strategic element" for regional security, explicitly positioning Russia as a legitimating authority. Leader-to-leader exchanges further reinforce this role. Kim Jong-un's congratulatory messages to Vladimir Putin and reciprocal praise from Russian leaders are quoted to underline that bilateral ties have reached the level of a "strategic partnership". DPRK media frequently employs evaluative verbs such as "highly appraise" and "extol" to characterise Russian statements, foregrounding Russia's approval of Kim's leadership and policy line.

Overall, external legitimation shifts from indirect and symbolic in 2015 to overt and politically instrumental in 2025, reflecting Pyongyang's increased reliance on Russian endorsement under conditions of heightened global polarisation.

2.1.2. Moral Alliance

Perhaps the most striking shift from 2015 to 2025 lies in the portrayal of Russia as a moral and ideological ally. In 2015, DPRK media described relations with Russia in polite, commemorative terms, emphasising historical friendship and cooperation rooted in the Soviet role in Korea's liberation. Coverage of events such as the "DPRK-Russia Friendship Year" stressed "traditional friendly relations" developing "ever better day by day", with references to friendship and cooperation largely confined to cultural exchanges and ceremonial goodwill. Importantly, Russia was not yet positioned as sharing a common enemy with North Korea; even critical references to U.S. policy appeared as general international commentary rather than expressions of DPRK–Russia solidarity.

By 2025, this framing shifts decisively. Russia is cast as a strategic moral ally, firmly placed on the "us" side of an ideological us-versus-them divide. DPRK media increasingly employs fraternal language, referring to Russia as a comradely or brotherly ally and emphasising a shared "common struggle" against imperialism. Articles invoke morally charged concepts such as justice, sovereignty and dignity, framing Russia and North Korea as jointly defending these values against Western hostility. In this discourse, Russia is no longer simply friendly but is bound to the DPRK through principles described as timeless and sacralised, often reinforced through war-time analogies referencing World War II and the Korean War. The transformation is clear: where Russia was a *friend* in 2015, it becomes a *comrade* by 2025.

This moralisation is especially significant when viewed against earlier alliance narratives. Notably, DPRK media begins to apply historical analogies previously reserved for China – particularly the Korean War-era trope of righteous solidarity against imperial aggression – to Russia. By invoking this lineage, contemporary cooperation with Russia is framed as analogous to China's intervention in the 1950s, effectively elevating Russia to the status of an ideological comrade following in China's historic footsteps. Through this discursive move, DPRK media "manufactures friendship" by embedding Russia within the same moral universe that legitimises North Korea's own revolutionary identity.

2.1.3. Militarisation Normalisation

North Korean media has long justified its militarisation by reference to external threats or historical sacrifices. In this regard, Russia's role in the narrative adds a comparative and justificatory element. In 2015, direct references to Russia in a military context were relatively rare, since at that time Russia was not directly engaged in any widely acknowledged conflict (Crimea/Donbass were ongoing but DPRK media touched them lightly). One notable example from 2015 was an article about U.S. missile defence, where the DPRK paper described "Russia countering U.S. military pressure". This piece, while ostensibly foreign news, implicitly drew a parallel: just as Russia must enhance its defences due to U.S. encirclement, so must North Korea. The article detailed Russia's military upgrades (new ICBM tests, anti-missile systems) in sympathetic tones, clearly suggesting that Russia's militarisation is a rational response to Western threats – an analogy not lost on a North Korean reader. Therefore, even in 2015, Russia was used to *normalise the idea of military build-up*:

if a great power like Russia is doing it in face of U.S. hostility, it validates North Korea doing the same. However, this was somewhat indirect.

By 2025, Russia's war in Ukraine and confrontation with NATO provided a much more explicit template for normalising militaristic themes. North Korean media openly sided with Russia's narrative of the war. Although they often avoided naming "Ukraine" directly (a silence that we will discuss later), they echoed Russian justifications. For example, articles spoke of Russia "fulfilling its international duty to oppose fascism in Ukraine" – a portrayal that glorifies Russia's military actions as heroic and necessary, thus implicitly casting North Korea's own military posture (nuclear tests, missile launches) as likewise part of a noble anti-fascist, anti-imperialist cause.

News stories about Russian Victory Day commemorations were given significant space, emphasising "sacred sacrifice" and "heroic struggle" of the Russian army. By repeatedly highlighting Russian veterans, war anniversaries and Putin's invocation of the Great Patriotic War (i.e. World War II in Russian political discourse), DPRK media reinforces its own militarised worldview. While North Korea does maintain an anti-fascist narrative rooted in its anti-Japanese resistance against colonial rule, it lacks a mass, society-wide anti-fascist war memory comparable to the Soviet experience. Russia's Great Patriotic War thus provides a more expansive and morally universal framework, which DPRK media appropriates to normalise contemporary militarisation and frame present conflicts as historically justified resistance. North Korea often analogises its situation to the 1940s or 1950s; now Russia's contemporary fight is analogised to those struggles also. The outcome is a discursive synergy: Russia's current militarism *normalises* North Korea's perpetual military mobilisation. One KCNA commentary in late 2025 even argued that *just as Russia stands firm against NATO, North Korea must bolster its deterrence against the U.S.–ROK*[3] *alliance*, directly linking the two situations. In sum, Russia's portrayal in 2025 strongly serves to rationalise and elevate North Korea's Songun (military-first) policy as part of a wider legitimate resistance. This is a significant evolution from 2015, when Russia was not actively used as such a prominent mirror for DPRK's own military justification.

2.1.4. Implicit Polarisation

A core discursive function that becomes prominent by 2025 is Russia as an *external pole in an implicitly polarised narrative*. North Korean propaganda has always relied on dichotomies (e.g. imperialists vs independent peoples). In 2015, Russia occasionally figured into this schema but carefully. For instance, an article might criticise U.S. actions by citing Russian critiques – effectively using Russia to voice condemnation of the West, which the DPRK narrator can then amplify. In the aforementioned 2015 piece regarding the U.S. missile defence, the writer notes that "Russia refuted that the U.S. missile defense is clearly aimed at it and causes rising tensions". Here, Russia is the one calling out the hostile (American) force, implying a world divided into a U.S.-led bloc and those resisting it. Yet in 2015, DPRK media still did not explicitly say "Russia and we are together against the West".

By 2025, the polarisation is explicit in sentiment if not always in naming. North Korean media frequently invokes a global divide between anti-imperialist forces and a hostile Western bloc. However, rather than crudely saying "new Cold War blocs", they often imply it. Russia is consistently on the "good" side of this implication. For example, KCNA articles would mention "external threats" and "hostile forces" in the same breath as praising Russia. The enemy is often unnamed – possibly "imperialists" or "hegemonic forces" in general – but contextually it is clear that means the U.S., NATO, Japan, etc. By not naming the U.S. every time, the media uses what Fowler calls meaning through absence (Fowler 1991). Readers fill in the blank: if Russia and DPRK are celebrating a partnership of justice and sovereignty, the adversary must be the unjust imperialists (everyone knows who they are).

A concrete instance of this came with North Korean coverage of the expansion of trilateral U.S-ROK-Japan cooperation in 2025. One DPRK commentary noted that "our relations with Russia will prove a powerful strategic factor if the U.S. and its puppets persist in aggression", without detailing what that means. The phrase signals: North Korea and Russia stand aligned ("strategic

[3] ROK denotes the Republic of Korea (South Korea).

factor") against the U.S. bloc. Thus, the polarisation function is fully realised – Russia is depicted as the counter-hegemonic pole balancing the U.S. and by extension as part of North Korea's own camp. This is a notable change from 2015, where China was often given more weight as a partner against the U.S. while Russia was secondary. By 2025, the media places Russia in parallel with China as pillars of a friendly camp. In fact, North Korean outlets sometimes mention Russia and China together (e.g. referencing support from both at the UN). The ideological message is that the world is now divided and North Korea is not alone: Russia is on its side.

2.2. Narrative Roles: What Russia is as a "character" in the story

Beyond abstract functions, the DPRK media also "casts" Russia in certain narrative roles within its storytelling. Using Proppian narrative analysis as a heuristic, we identify roles like *Helper/Donor, Witness, Brother-in-Arms* and *Gatekeeper* that Russia fulfills. These roles are present in both periods but with different frequencies and emphasis[4].

2.2.1. Helper/Donor: From symbolic gestures to more strategic support cues

In 2015, Russia often appears in the narrative as a symbolic supporter, present through messages, formal gestures or acknowledgements timed to politically meaningful occasions. The recurring cue "at a meaningful time" is important: it frames support as providential and appropriate, reinforcing the idea that Russia "shows up" when the DPRK's storyline requires external recognition.

In 2025, the helper role is narratively amplified. Even where concrete material cooperation is not described in detail, the rhetorical structure implies that Russia's presence and stance provide the DPRK with strategic reinforcement. The "helper" framing therefore functions as a bridge between domestic legitimacy and foreign alignment: Russia appears as a benefactor-like partner without casting the DPRK as dependent.

2.2.2. Brother-in-arms / Comrade: The key narrative upgrade in 2025

The most consequential narrative shift is the emergence of Russia as a co-fighter rather than a peripheral friend. In 2015, this role was marginal and largely historical or implicit. By 2025, it becomes central: the language of *shared struggle* and *moral alignment* recasts Russia as a peer actor within the DPRK's conflictual worldview. Where such cues appear, Russia is no longer merely friendly; it becomes a co-protagonist in an anti-imperialist struggle, providing ideological justification for strategic alignment.

By 2025, the comrade-in-arms trope operates as a present-tense narrative rather than historical reference. DPRK media explicitly depicts Russia as having "formed a common front" with North Korea, frequently collapsing past and present through compressed historical analogies. References to World War II and anti-fascist resistance are repurposed to frame contemporary cooperation as the continuation of a shared historical mission. Russia is thus labeled a "comrade" not only through inherited memory, but through an ongoing "struggle for justice" conducted in parallel in Moscow and Pyongyang.

Russia is never portrayed as a patron or superior power, but as fighting side-by-side with the DPRK. The frequent use of comradely language in leader-level interactions underscores equality, mutual respect and shared sacrifice. In propaganda terms, elevating Russian leaders to the status of "comrade" places them within the DPRK's inner ideological circle, a designation typically reserved for socialist fraternity. In this way, a role only faintly present in 2015 becomes, by 2025, a stabilised narrative of Russia as an active brother-in-arms in the present tense.

[4] For reasons of space the analysis focuses only on selected examples that are most representative of the broader patterns observed.

2.2.3. Gatekeeper to the World

A third role is Russia as a *gatekeeper* enabling controlled access to the outside world under sanctions and isolation. In 2015 this appears sporadically (Russia-hosted events; occasional UN coverage implying Moscow helps make Pyongyang's position heard). By 2025, the framing is clearer: DPRK media credits Russia with shielding North Korea diplomatically and amplifying its positions in international settings, while also narrativising practical connectivity (e.g., Pyongyang–Moscow links) as part of the "strategic partnership." Russia thus functions not only as a bilateral ally but as a curated corridor for external engagement without hostile scrutiny.

2.3. Storytelling Strategies: How the "friendship" story is stabilised

North Korean state media relies on a set of recurring storytelling strategies to stabilise and naturalise the DPRK-Russia partnership. These include *ritualisation* (presenting cooperation as ceremonial and historically inevitable), *personalisation* (anchoring interstate relations in leader-to-leader ties), *temporal compression* (linking past, present and future into a continuous narrative) and *silencing or omission* (excluding dissonant information that could complicate the partnership's moral clarity)[5].

2.3.1. Temporal Compression: "Past–present–future" continuity as an alliance technology

A central strategy in the 2025 discourse is *temporal compression*, i.e. the collapsing of historical memory and future destiny into a single storyline of continuity. Lexical cues such as "inherit/continue", "tradition" formulations and implied permanence present DPRK-Russia alignment as something that transcends tactical convenience. Instead of saying "we cooperate because of circumstances", the narrative says: we cooperate because history and principle demand it.

This matters in security terms because it shifts the partnership from "contingent" to "natural." If the alliance is narrated as historically rooted and forward-moving, it becomes harder, both discursively and politically, to reverse.

2.3.2. Silencing/omission: Ukraine and the costs of alignment structurally absent

A second central storytelling strategy is *silencing*. DPRK media never frames Russia in ways that would complicate the moral clarity of the partnership, most notably by avoiding any portrayal of Russia as an aggressor in Ukraine. Instead, reporting relies on euphemism, abstraction and blame displacement, preserving Russia's image as a morally coherent ally and minimising cognitive dissonance for domestic audiences.

Within the 2025 constructed-week corpus analysed here, North Korean coverage does not refer to Russia's actions as an "invasion" or as a war initiated by Moscow. When Ukraine appears at all, it is filtered through Russian framing, via references to a "special military operation", NATO expansion or vague formulations, such as a "crisis" or "situation" caused by Western forces. Civilian harm, battlefield setbacks, international condemnation and the economic costs of sanctions are entirely absent. Any acknowledgement of difficulty is oblique, expressed through vague phrases such as Russia "facing challenges while continuing to stand firm", without specifying their source.

Silencing also extends to the bilateral relationship itself. DPRK media never acknowledges disagreement, asymmetry or constraint in DPRK–Russia relations, nor does it reference instances where Russian interests might diverge from Pyongyang's. Third-party perspectives that could complicate the narrative are similarly excluded, while only supportive foreign voices are amplified. The result is a tightly controlled discursive environment in which alignment with Russia appears universally endorsed, morally justified and cost-free – an essential condition for sustaining domestic legitimacy in the context of a globally contested war.

[5] Given space constraints, this section focuses on two analytically central strategies that are most consequential for understanding how the partnership is framed as durable and uncontested: temporal compression and silencing. Together, these techniques allow DPRK media to present cooperation with Russia as historically destined, forward-looking and free of contradiction, thereby reinforcing the perception of a stable strategic alliance.

3. Discussion: From Portrayal to Partnership – Media Framing and Alliance Legitimation

This discussion situates the empirical findings within broader debates on alliance formation, securitisation and media framing in authoritarian systems. It examines how North Korean state media not only reflects but actively stabilises strategic alignment with Russia and considers the implications of this discursive shift for understanding partnership durability and flexibility in a polarised international order.

3.1. Strategic Partnerships and Media Framing in a Polarised Order

The findings reveal a clear shift in North Korean state media from portraying Russia as a routine diplomatic partner in 2015 to framing it as a strategic and ideological ally by 2025. This transformation reflects a broader reconfiguration of how Pyongyang narrates its place within an increasingly polarised international system.

Most notably, Russia is presented less as a transactional partner and more as a moral ally. DPRK media emphasises shared values, i.e. anti-imperialism, sovereignty and resistance to external pressure, over material cooperation, thus framing alignment with Russia as principled and long-term rather than opportunistic. Where political legitimacy is closely mediated through official discourse, such shifts help stabilise foreign policy choices by rendering them domestically legitimate. By embedding Russia within narratives of “common struggle” and “comradeship”, state media anchors the partnership within the regime’s ideological universe.

From a security studies perspective, the narrative roles assigned to Russia are equally significant. By depicting Russia as both helper and brother-in-arms, DPRK media mitigates the asymmetry inherent in alliances between weaker and stronger states. Russia is never framed as a patron; instead, the relationship is narrated horizontally, as cooperation between equals. This reflects what Myers identifies as a core feature of North Korean ideology: a strong emphasis on dignity, autonomy and resistance to subordination, even vis-à-vis nominal allies (Myers 2010). Media discourse thus functions as a form of status management, allowing Pyongyang to preserve sovereignty while aligning closely with a major military power.

The analysis also shows how manufactured threat and manufactured friendship operate in tandem. Abstract references to “hostile forces”, rather than explicit naming, sustain a sense of external siege that renders alignment with Russia natural and necessary. This mirrors securitisation dynamics, in which threat construction legitimises extraordinary alignments. Within this framing, the DPRK-Russia partnership appears not as a strategic choice among alternatives, but as the logical outcome of a world divided into opposing camps.

Finally, storytelling strategies such as temporal compression and silencing contribute to portraying the partnership as stable and inevitable. By linking past, present and future through notions of inherited tradition and by omitting costs, controversy or disagreement, DPRK media reduces the perceived risks of alignment while narrowing rhetorical flexibility vis-à-vis the West.

Taken together, these findings suggest that North Korean state media does not merely reflect closer DPRK-Russia ties but actively consolidates a strategic worldview in which alignment with Russia is morally justified, historically grounded and security-enhancing. For scholars of security and alliance politics, this underscores the value of media discourse as an early indicator of strategic orientation in authoritarian systems.

3.2. Future Trajectories and Alliance Flexibility

The elevation of Russia as a moral and strategic ally should be read against North Korea’s post-Hanoi recalibration: after the 2019 DPRK-U.S. summit collapse, sustained dialogue with the United States effectively ended, lowering the diplomatic costs of overt alignment with Russia

compared to 2015. In alliance-theoretical terms, the media framing signals movement from hedging toward clearer alignment under heightened threat.

Yet the durability of this discursive alignment is not guaranteed. Its intensity is tightly tied to wartime polarisation; de-escalation in Ukraine or shifts in Russia's global posture could prompt a more pragmatic recalibration. China remains a key variable: while ties with Beijing are affirmed, China is not consistently framed as unequivocally anti-U.S., making relative Russia-China emphasis sensitive to Sino-U.S. dynamics. Finally, South Korea is framed as part of a hostile U.S.-led bloc, consistent with Pyongyang's recent shift away from inter-Korean unity toward treating the ROK as a separate adversarial state.

Conclusions

This paper has demonstrated that North Korean state media offers critical insight into how Pyongyang interprets and legitimises its evolving relationship with Russia. A comparative analysis of 2015 and 2025 media content reveals a clear narrative shift: Russia is no longer portrayed as a peripheral diplomatic partner, but as a strategic and ideological ally embedded in North Korea's vision of a polarised world order. Media discourse frames DPRK-Russia cooperation not as ad hoc or transactional, but as a principled partnership rooted in shared confrontation with the West.

Three core conclusions emerge. First, the portrayal of Russia has become strongly ideologised. By embedding the partnership in narratives of *moral righteousness*, *historical continuity* and *common struggle*, DPRK media incorporates Russia into the regime's domestic legitimacy framework. This suggests a level of commitment that is rhetorically difficult to reverse. Second, the use of layered narrative strategies, combining discursive functions, character roles and storytelling techniques, demonstrates a deliberate effort to naturalise the partnership as enduring and inevitable. Russia is cast simultaneously as *comrade, validator* and *strategic counterpart*, reinforcing an image of equal and sovereign alignment. Third, the *construction of friendship* operates alongside the *construction of threat*. By portraying the international environment as sharply polarised and hostile, state media presents alignment with Russia as both necessary and justified.

For security and international relations scholarship, these findings underline the value of state media analysis as an indicator of strategic orientation in systems where official discourse plays a central political role. In the DPRK case, discursive shifts toward Russia precede and accompany tangible policy developments, suggesting that propaganda plays a preparatory and stabilising role in alliance formation. Understanding how North Korea narrates its friendships and enemies therefore remains essential for interpreting its strategic behavior and anticipating future alignments.

North Korean state media does not merely reflect the deepening DPRK-Russia relationship; it actively contributes to constructing it as an ideological alliance. In Pyongyang, alliance politics is not only practised through diplomacy and arms, but narrated into existence through state discourse. This underscores the importance of reading North Korean media as a strategic signal, rather than dismissing it as mere propaganda.

BIBLIOGRAPHY:

Armstrong, Charles K. 2013. *Tyranny of the Weak: North Korea and the World, 1950–1992*. Ithaca: Cornell University Press.

Cha, Victor D. 2012. *The Impossible State: North Korea, Past and Future*. New York: HarperCollins.

Fairclough, Norman. 1995. *Media Discourse*. London: Edward Arnold.

Fowler, Roger. 1991. *Language in the News: Discourse and Ideology in the Press*. London: Routledge.

Korean Central News Agency (KCNA). 2025. Selected articles from constructed-week sample. Pyongyang.

Lankov, Andrei. 2014. *The Real North Korea: Life and Politics in the Failed Stalinist Utopia*. Oxford: Oxford University Press.

Myers, B. R. 2010. *The Cleanest Race: How North Koreans See Themselves and Why It Matters.* New York: Melville House.

Propp, Vladimir. 1968. *Morphology of the Folktale*. Austin: University of Texas Press.

Rodong Sinmun. 2015. Selected articles from constructed-week sample. Pyongyang.

Toloraya, Georgy. 2025. "Why the North Korea–Russia Relationship Is Built to Last." NK News, March 6, 2025.

Van Dijk, Teun A. 2008. *Discourse and Power.* New York: Palgrave Macmillan.

Wishnick, Elizabeth A. 2003. "A New Era in Russian-North Korean Relations?" In North Korea and Northeast Asia, edited by Samuel S. Kim, 139-162. Boulder: Rowman & Littlefield.

DOI: 10.53477/3045-2309-26-08

STRATEGIC BALANCING IN TRANSITION: REASSESSING ARMENIA'S FOREIGN AND SECURITY POLICY PARADIGM

Rafik AVETISYAN, PhD,
Associate Professor, Senior Research Fellow, National Defence Research University,
Center for Regional Strategic Studies, of the Ministry of Defence of the Republic of Armenia,
Researcher, Institute for Armenian Studies, Yerevan State University
E-mail address: ravetisyan94@gmail.com

Tigran KOCHARYAN, PhD,
Colonel, Professor, Deputy Commandant of the National Defence and Research University,
Head of the Institute for National Strategic Studies, Republic of Armenia
E-mail address: ttqocharyan@yahoo.com

Abstract*: This article examines the transformation of Armenia's foreign and security policy in the context of the post-2020 regional order in the South Caucasus. It argues that Armenia is transitioning from a model of single-patron security dependence toward a strategy of diversification, driven by the erosion of alliance reliability and growing asymmetric threats. The study demonstrates that this shift represents a structural adaptation rather than an ideological realignment, as Armenia seeks to expand its strategic autonomy without fully abandoning existing institutional ties. Using neorealist balance-of-power theory and small-state behavior literature as its theoretical framework, the article employs qualitative case-study analysis, process tracing, and document analysis covering the period 2020–2025. The findings highlight both the opportunities created by diversified partnerships and the constraints imposed by continued economic dependence and regional isolation. The article's originality lies in conceptualising Armenia's policy change as adaptive balancing under constraint, offering analytical utility for understanding small-state strategies in volatile security environments.*

Keywords*: Armenia; foreign and security policy; strategic diversification; small-state balancing; South Caucasus.*

Introduction

The South Caucasus has entered a period of profound geopolitical transformation marked by the erosion of established security architectures, the resurgence of regional power competition, and the reconfiguration of external influence. The combined impact of the 2020 Nagorno-Karabakh war, Russia-Ukraine war, Azerbaijan's post-war coercive diplomacy, and the collapse of Russia's role as a credible security guarantor has dismantled the foundational assumptions that governed Armenia's foreign and security policy for more than three decades.

Within this context, Armenia is undergoing a paradigmatic shift from a model of single-patron security dependence toward a strategy of diversification, hedging, and limited external balancing. This transition is not the result of ideological realignment or Westernisation but of structural compulsion. Russia's growing alignment with Azerbaijan, its failure to deter or reverse Azerbaijani military coercion against Armenia, and its acquiescence in the 2023 ethnic cleansing of Nagorno-Karabakh have fundamentally undermined the credibility of Armenia's traditional security framework. Simultaneously, Türkiye's expanded regional role and Azerbaijan's revisionist posture have created a hostile security environment in which Armenia must seek new instruments of deterrence, diplomacy, and resilience.

Against this backdrop, Armenia's intensified engagement with the European Union, the United States, France, India, alongside initiatives such as TRIPP (Trump Route for International Peace and Prosperity), and emerging connectivity frameworks, signals the emergence of a new foreign and security policy paradigm. Rather than replacing one alliance with another, Armenia is attempting to widen its strategic space by embedding itself in multiple overlapping diplomatic, economic, and security networks. This strategy reflects a classical small-state response to asymmetric threat environments: maximizing autonomy by diversifying external ties while avoiding irreversible geopolitical commitments.

Yet, this transformation is neither complete nor uncontested. Armenia remains deeply embedded in Russian-centered economic, energy, and institutional structures, while its security environment continues to be shaped by military asymmetries and geographic isolation. The coexistence of military diversification and economic dependence creates structural tension within Armenia's foreign policy, raising fundamental questions about the sustainability, coherence, and limits of its new strategic orientation.

The central research question guiding this study is: How and to what extent is Armenia transitioning from a Russia-centered security dependence model to a diversified balancing strategy, and what are the structural opportunities and constraints shaping this transformation? The study is grounded in the neorealist balance-of-power theory, particularly the concepts of external balancing, hedging, and alliance reliability, as developed by Kenneth Waltz and subsequent scholarship on small-state behaviour. This framework enables a systematic assessment of how shifts in alliance credibility and regional power configurations shape the strategic choices of vulnerable states.

Methodologically, the paper employs a qualitative case-study approach combining process tracing of key geopolitical events from 2020 to 2025, document analysis of Armenian, Russian, EU, and U.S. policy statements and security agreements, and a comparative assessment of Armenia's military, diplomatic, and economic alignments before and after the erosion of the Russian security guarantee. By integrating empirical evidence with theoretical analysis, the study demonstrates that Armenia's foreign policy is not drifting opportunistically between power centers but is undergoing a systemic reconfiguration driven by alliance failure and regional power realignment.

1. The paradigmatic shift in the Armenian foreign and security policy

The increasing instability in the South Caucasus and its neighboring regions has significantly impacted the paradigm of Armenia's foreign and security policy. The 2020 Nagorno-Karabakh war and Russia-Ukraine war established a new status quo in the South Caucasus, resulting in a new balance of power in which Türkiye's role has notably increased. During the 2020 Nagorno-Karabakh war, Türkiye was the primary regional power providing military and political support to Azerbaijan, while the Armenian-Russian allied relations were ineffective in restraining the actions of the Turkish-Azerbaijani alliance. This exposed growing vulnerabilities in Armenia's traditional reliance on Russia for security.

To *de jure* capitalise on its influence in the post-war South Caucasus, Türkiye signed a declaration with Azerbaijan on June 15, 2021, elevating Turkish-Azerbaijani cooperation to unprecedented levels. According to the declaration, Türkiye and Azerbaijan embarked on a new phase of close cooperation in mutual military assistance and defence industry (Press Service of the President of the Republic of Azerbaijan 16 June 2021). This development raises serious concerns for Armenia, as the declaration is practically directed against it. Armenia's Ministry of Foreign Affairs has expressed its apprehension, noting that the declaration is founded neither on the UN Charter nor the OSCE's principle of comprehensive and indivisible security, but on a 'kinship security' approach aimed at unifying the 'Turkic world' (Ministry of Foreign Affairs of the Republic of Armenia 17 June 2021).

The need to shift the paradigm of Armenia's foreign and security policy became particularly evident with the onset of the war in Ukraine and the establishment of alliance relations between Russia and Azerbaijan. As Russia, the state historically guaranteeing Armenia's security, began aligning

more closely with Azerbaijan, this created a fundamental dilemma for Armenia's security strategy. On February 22, 2022, Russia signed a declaration 'On Allied Cooperation' with Azerbaijan (Press Service of the President of the Republic of Azerbaijan 22 February 2022), signaling a further erosion of Armenia's reliance on Russia as its primary security guarantor. This marked a turning point, as Russia's strategic alignment with Azerbaijan raised new questions about the viability of the Armenian-Russian security partnership, especially in light of Azerbaijan's ongoing threats to Armenia's sovereignty.

The need to change the paradigm of Armenia's foreign and security policy became increasingly urgent following Azerbaijan's aggression towards Armenia's sovereign territory. In September 2022, Azerbaijan's military operations in the south-eastern border areas resulted in significant territorial losses for Armenia. Russia and the CSTO failed to fulfill their contractual obligations and did not provide adequate support to Armenia, prompting the country to seek additional mechanisms to preserve its territorial integrity. This contributed to a strategic rebalancing of Armenia's foreign policy, as decision-makers increasingly sought additional mechanisms to ensure territorial integrity while avoiding overdependence on a single security provider.

Armenia's policy pivot became most evident following the statement made in Prague, on October 6, 2022, when Armenia aligned itself more closely with Western agendas. In a significant move, Armenia agreed that the basis for the delimitation of the Armenian-Azerbaijani border would be the Alma-Ata Declaration of 1991, thereby recognising Azerbaijan's territorial integrity (The Office to the Prime Minister of the Republic of Armenia 7 October 2022). This agreement contributed to the political conditions enabling the deployment of a European Union civilian mission on the Armenian side of the border, aimed at balancing Russia's role in the settlement of Armenian-Azerbaijani border issues. This pivot to the West marked a key moment in Armenia's foreign policy, signaling a departure from its traditional alignment with Russia.

In the wake of these developments, Russia's role as a mediator in the Nagorno-Karabakh conflict has further weakened. Even before the Prague statement, Russia had failed to fully adhere to its peacekeeping responsibilities in Nagorno-Karabakh. Following the signing of the Russian-Azerbaijani alliance agreement, Azerbaijani forces occupied strategic positions in Nagorno-Karabakh with Russia's tacit approval. This culminated in Azerbaijan's closure of the Lachin corridor in December 2022, violating the 2020 Ceasefire Agreement and effectively isolating Nagorno-Karabakh. The failure of Russian peacekeepers to prevent Azerbaijan's September 2023 actions, which led to the forced displacement of over 100,000 ethnic Armenians, further undermined Armenia's confidence in Russia as a security guarantor. During this period, Russian peacekeepers did not fulfill their mandated obligations and failed to prevent the ethnic cleansing by expulsion of the Armenian population of Nagorno-Karabakh. Moreover, Russian officials attributed responsibility for these events to the Armenian authorities, arguing that Armenia's recognition of Azerbaijan's territorial integrity contributed to the outcome (TASS 12 January, 2024).

By 2024, the erosion of Russian support, combined with Azerbaijan's anti-Armenian rhetoric and demands for an extraterritorial 'corridor', had fueled growing anti-Russian sentiment in Armenia. Azerbaijan's proposal for a corridor, envisaged to be secured by Russian forces, was perceived in Armenia as a direct threat to its territorial integrity. While expressing readiness to unblock regional transportation routes, Armenia consistently rejected any extraterritorial arrangements that would undermine its sovereignty.

The United States and the European Union supported Armenia in its efforts to preserve its territorial integrity and to unblock transport communications in the region by upholding state sovereignty. Notably, during the Granada meeting, in October 2023, which hosted the leaders of Armenia, France, Germany, and the President of the European Council, the parties reaffirmed their commitment to maintaining Armenia's territorial integrity and the inviolability of its borders (The Office to the Prime Minister of the Republic of Armenia 4 October 2023). Additionally, in April 2024, Armenian Prime Minister Pashinyan met with European Commission President Ursula von der Leyen, U.S. Secretary of

State Antony Blinken, and EU High Representative Josep Borrell. During this meeting, it was agreed that the European Union and the United States would provide more than $300 million in aid for the development of Armenia's economy (An official website of the United States Government 5 April 2024). These developments highlight the deepening cooperation between Armenia and Western institutions, marking a significant balance in its foreign policy orientation. This transformation can be understood as a shift from a single-patron security dependence model to a hedging and diversification strategy, driven by alliance unreliability and systemic power reconfiguration in the South Caucasus.

2. Armenia's balancing act: opportunities and challenges

The security situation in the South Caucasus necessitates that Armenia pursue a carefully calibrated foreign and security policy in order to manage emerging risks and mitigate security threats. According to the Balance of Power Theory, smaller states such as Armenia seek to counter the ambitions of larger regional powers by diversifying their alliances and enhancing resilience. As Kenneth Waltz argues, balancing behavior manifests through internal and external balancing mechanisms (Waltz 1979, 118). Internal balancing involves strengthening a state's economic capacities, developing realistic strategic doctrines, and enhancing military capabilities. External balancing, by contrast, is pursued through the formation of alliances and partnerships with external actors in order to compensate for structural vulnerabilities and ensure security.

For Armenia, this has meant reducing its historical dependence on Russia while engaging new regional and global actors to protect its sovereignty. Since its declaration of independence, Armenia has faced existential threats, necessitating the creation of a combat-ready army to neutralise threats from Azerbaijan. The process of building the Armenian army followed the approaches typical of the Soviet military, resulting in near-total dependence on Russia for ammunition supplies. Before the 2020 Nagorno-Karabakh war, 90% of Armenia's ammunition came from Russia. However, in recent years, Armenia's balancing policy in ammunition procurement has significantly reduced its dependence on Russia to just 10% (First channel news 06 March 2024).

While Armenia remains institutionally tied to Russia through bilateral and multilateral agreements, including its participation in the CSTO, these arrangements have proven unreliable in safeguarding Armenia's territorial integrity. These include the 'Agreement between the Republic of Armenia and the Russian Federation on the Russian Military Base in the Territory of the Republic of Armenia' dated March 16, 1995, the 'Treaty on Friendship, Cooperation, and Mutual Assistance between the Republic of Armenia and the Russian Federation' dated August 29, 1997, and the collective security agreements within the CSTO (Ministry of Foreign Affairs of the Republic of Armenia 2026). The CSTO and Russia's failure to adequately respond to Azerbaijan's aggression has prompted Armenia to freeze its political participation in the organisation (Armenpress 23 February 2024). This highlights a broader challenge facing Armenia's security policy, where options are limited. Armenia must either seek to improve the existing Russia-centered security system, whose shortcomings have become particularly apparent in light of the war in Ukraine, or it must explore alternative balancing strategies to protect its security interests. In response to the changing nature of Russia's interests in the South Caucasus, Armenia was compelled to pursue the second option. It sought new avenues to balance regional powers and enhance its strategic resilience.

2.1. From Complementarity to Diversification

Historically, Armenia's foreign policy was based on complementarity, seeking balanced relations with both Russia and the West. Armenia's 2007 National Security Strategy stated that the country implemented its foreign security strategy based on the principles of 'complementarity' and 'engagement' (Ministry of Foreign Affairs of the Republic of Armenia 2007). Through the policy of complementarity, Armenia aimed to build relations on the basis of partnership, fostering effective relations with all regional actors. The engagement policy underscored Armenia's obligations as part

of the international community. The 2020 National Security Strategy reaffirmed this approach, emphasising the 'principle of developing mutually beneficial and equal relations with all states' as the foundation of Armenia's foreign policy (The Government of Armenia 2020). This principle was maintained in the 2021 Government Programme of Armenia, which highlighted 'enterprising and effective involvement in all directions' as the main principle of Armenia's foreign policy (The Government of Armenia 2021).

Armenia's turn toward diversification reflects not merely a tactical adjustment but a structural response to the erosion of its traditional security framework. Russia's deepening alignment with Azerbaijan, coupled with its inability to uphold security commitments toward Armenia, exposed the limitations of Armenia's long-standing reliance on a single external guarantor. This deterioration accelerated after 2020 and became unmistakable after 2022, prompting Yerevan to reassess the sustainability of its security dependence.

Within this context, diversification has emerged as the central organising principle of Armenia's foreign policy. Rather than constituting a full strategic realignment or alliance substitution, diversification represents a form of external balancing under constraint, aimed at expanding Armenia's diplomatic, political, and institutional options while avoiding abrupt ruptures with existing security arrangements. This approach underscores Armenia's recognition that disengagement from its traditional security system is neither immediate nor cost-free, necessitating a gradual and calibrated transition.

Engagement with the European Union occupies a pivotal place in this strategy. The Comprehensive and Enhanced Partnership Agreement (CEPA) institutionalised Armenia–EU relations by providing a legal and normative framework that enhanced Armenia's international visibility, governance capacity, and reform credibility. While CEPA does not offer hard security guarantees, it strengthens Armenia's strategic autonomy indirectly by embedding the country within EU regulatory, political, and economic networks. In this sense, EU engagement functions as a soft security multiplier, reinforcing state resilience, legitimacy, and bargaining power rather than substituting for military deterrence.

The adoption of the new Strategic Agenda for the EU-Armenia Partnership marks a qualitative deepening of this relationship. By replacing the 2017 Partnership Priorities with a more ambitious and comprehensive framework, the Strategic Agenda reflects both Armenia's evolving security perceptions and the EU's growing willingness to engage more substantively. Its inclusion of cooperation on connectivity, energy security, trade diversification, and - critically - security and defence signals a gradual expansion of the EU's role in Armenia's broader security environment. Although these dimensions remain limited in scope, they contribute to a layered security approach that complements Armenia's diversification strategy.

From a theoretical perspective, Armenia's evolving foreign policy aligns with limited external balancing and hedging behaviour, characteristic of small states operating under asymmetric power constraints. Rather than seeking immediate alliance replacement, Armenia leverages EU engagement to mitigate overdependence, reduce strategic vulnerability, and enhance policy flexibility. This incremental approach reflects an awareness of regional power asymmetries and the risks associated with rapid geopolitical reorientation.

Nevertheless, the EU track also faces structural limitations. The absence of binding security guarantees, the EU's cautious approach to hard security in the South Caucasus, and Armenia's ongoing exposure to military pressure constrain the transformative potential of EU engagement. As a result, diversification remains an adaptive strategy rather than a definitive solution, aimed at widening Armenia's strategic margin rather than resolving its security dilemma.

2.2. Opportunities in Geopolitical Engagement

The displacement of Armenians from Nagorno-Karabakh in 2023 and the withdrawal of Russian peacekeepers have accelerated Armenia's rapprochement with the West, offering new opportunities to

balance Russian influence. Armenia's growing alignment with the European Union, demonstrated by the deepening of diplomatic ties and the Prime Minister's call for closer cooperation (European Parliament 17 October 2023), reflects its strategic pivot toward the West. In addition to relations with the EU, Armenia has restored diplomatic ties with Hungary, initiated strategic dialogues with the United States and United Kingdom, and signed a strategic partnership agreement with Georgia.

In the process of defending Armenia's territorial integrity, establishing a strategic partnership with the Trump administration has played a particularly important role. U.S. President Donald Trump, by supporting the Armenia - Azerbaijan peace process, initiated the unblocking of regional communication and transit routes, creating opportunities for Armenia to position itself as a regional transit and cooperation hub. This recalibration has intersected with emerging geopolitical and connectivity initiatives, most notably the Trump Route for International Peace and Prosperity (TRIPP). Within Armenia's strategic discourse, TRIPP is increasingly viewed not as a formal military alliance but as a geo-economic and connectivity framework capable of enhancing Armenia's role as a transit and cooperation node linking Europe, the South Caucasus, and broader regional trade corridors. By emphasising infrastructure, trade, and regional connectivity, TRIPP complements Armenia's broader diversification strategy and reinforces the country's efforts to strengthen its security and autonomy through external engagement.

In the defence sector, Armenia's partnership with France has been particularly significant. The agreements signed between Armenia and France in 2024 have introduced much-needed military reforms and equipment supplies (RFI 23 February 2024), further reducing Armenia's reliance on Russia. These defence partnerships allow Armenia to strengthen its military capabilities through external support, thus maintaining a degree of autonomy and resilience in a region dominated by larger powers.

The balancing of Armenia's foreign and security policy is not limited to cooperation with Western countries. In recent years, Armenia has also intensified its cooperation with Arab states. Historically, Armenia has always maintained good relations with Arab nations and has been an observer state of the Arab League since 2004. A significant event for Armenia was the establishment of diplomatic relations with the Kingdom of Saudi Arabia on November 25, 2023 (Ministry of Foreign Affairs of the Republic of Armenia 12 May 2023). This development may contribute to the diversification of Armenia's foreign and security policy, as Saudi Arabia is not only a major regional power in the Middle East but also a leading state in the Organization of Islamic Cooperation and a member of the G20 (Alrmizan 2020, 19). In recent years, Armenia has also been towards strengthening its relations with Egypt. In March 2024, the Prime Minister of Armenia visited Egypt and signed agreements with the President of Egypt to deepen cooperation in various fields. In addition to expressing its support for the cessation of the war in Gaza, Armenia sent humanitarian aid to Gaza's residents. Armenia has officially recognized a Palestinian state and explicitly supports the application of the "two states" principle in the Israeli-Palestinian conflict (The Office to the Prime Minister of the Republic of Armenia 05 March 2024).

Following the 2020 Karabakh war, Armenia significantly recalibrated its engagement with the United Arab Emirates (UAE), elevating bilateral relations from a largely secondary partnership to an increasingly important component of its diversification strategy between 2020 and 2025. This shift was reflected in intensified high-level political dialogue, with Armenia conducting eight official visits to the UAE at the presidential and foreign ministerial levels during this period (Ministry of Foreign Affairs of the Republic of Armenia, 7 February 2024). These interactions resulted in the signing of a series of agreements aimed at expanding cooperation across multiple sectors. With this strengthening of relations, Armenia-UAE cooperation especially in the trade and economic sectors has notably expanded. In 2023, the UAE became Armenia's second largest trade partner. Within a year, Armenia's trade with the UAE increased nearly fourfold, amounting to approximately $2.3 billion, or 11.1% of Armenia's foreign trade (ArmStat 2024).

With the strengthening of bilateral relations, Armenia–UAE cooperation - particularly in the trade and economic spheres - expanded markedly. In 2023, the UAE emerged as Armenia's second-

largest trade partner, with bilateral trade increasing nearly fourfold within a single year to approximately USD 2.3 billion, accounting for 11.1 percent of Armenia's total foreign trade turnover (ArmStat, 2024). This surge was driven largely by the UAE's role as a key destination for the re-export of gold and diamonds. Despite a broader moderation in Armenia's foreign trade dynamics thereafter, the UAE retained its position as Armenia's second-largest trading partner in 2025. Between January and August 2025, Armenia exported goods worth USD 1.26 billion to the UAE while importing USD 0.25 billion, resulting in a substantial trade surplus (Council of the European Union 2025). These figures underscore the sustained importance of the UAE within Armenia's external economic diversification strategy, even as the composition and intensity of trade evolved beyond the peak levels observed in 2023.

For the purpose of diversifying Armenia's foreign and security policy, deepening the military-political cooperation with India is also crucial. Following the 2020 Karabakh war, the strengthening of Türkiye-Azerbaijan-Pakistan strategic cooperation, Azerbaijan's ambitions to control Armenian sovereign territory, and changes in the geopolitics of transport communications in Eastern Europe and the Middle East have created a new impetus for increasing India's influence in the South Caucasus. It must be noted that before the war in Ukraine, India was able to export its goods to European markets through Russia, which became impossible after the war began. Consequently, India is seeking to fill this gap by cooperating with the South Caucasian countries, particularly through the 'Persian Gulf-Black Sea' multimodal route. In this context, India supports establishing stability in the region and is contributing to Armenia's efforts to achieve a military balance. India condemned Azerbaijan's aggression against Armenia during the UN Security Council meetings on September 15, 2022 (UN Meetings Coverage and Press Releases 15 September 2022). In 2023, Armenia and India signed contracts for the supply of Indian military equipment, including rocket artillery systems.

These relationships not only diversify Armenia's military capabilities, such as its acquisition of Indian military equipment, but also enhance its strategic position in the broader geopolitical landscape. Armenia's engagement with India, particularly in military cooperation, aligns with the principles of external balancing, helping Armenia counterbalance the influence of Türkiye and Azerbaijan in the region.

2.3. Challenges in Economic Diversification

While Armenia has made progress in diversifying its military and diplomatic relations, economic diversification remains a significant challenge. The 2021 Government Programme of Armenia emphasises the importance of diversifying export markets as a key aspect of its foreign economic policy (The Government of Armenia 2021). This means reducing dependence on a single center by diversifying export and import markets and expanding investments and economic partnerships. Armenia also places great importance on energy security, particularly the diversification of imports of gas, oil and petroleum products. Additionally, Armenia emphasises the significance of participating in emerging international transport programs in the region.

In recent years, Armenia has not only failed to reduce its dependence on the Russian market, but Russia's influence on Armenia's economic development has further intensified, shaped in large part by Western sanctions on Russia and Armenia's continued engagement within the Eurasian Economic Union (EEU). According to the Armenian National Statistical Committee and external trade analyses, Armenia's foreign trade turnover experienced robust growth in 2024, reaching over $26 billion in the first ten months of the year, with Russia remaining the country's largest trade partner and accounting for more than 40 % of total trade; bilateral trade turnover with Russia exceeded $10.8 billion, underpinned by a sharp increase in imports from Russia even as Armenian exports to Russia declined modestly (Business media 6 December 2025).

Despite this high level of trade with Russia in 2024, the trend in 2025 shows a contraction in Armenia's overall foreign trade turnover, which fell by roughly 39 % in the first nine months of the year compared to 2024, with Russia still ranking among the top sources of imports (ARKA 6 November 2025). These dynamics underscore that Armenia's recent economic performance remains

closely tied to trade flows tied to Russia and the broader post-sanctions Eurasian market, with much of the export growth linked to re-exports and integration within the EEU rather than diversification toward Western markets. Consequently, it can be concluded that Armenia's recent economic growth and external trade orientation continue to reflect the structural effects of Western sanctions on Russia and Armenia's economic orientation within the Eurasian Economic Union rather than a successful reduction of its economic dependence on Moscow.

The increase in Armenia's economic dependence on Russia and the failures in its economic diversification efforts are primarily attributable to the isolation policy implemented by Türkiye and Azerbaijan. Since the 1990s, Armenia's eastern and western land borders have remained closed. The southern border, connecting Armenia to Iran, offers no opportunities for completely free economic activity due to the economic sanctions against Iran. Furthermore, access to European markets via Georgia's Black Sea ports has been significantly restricted because of the war in Ukraine.

While Armenia has successfully diversified its defence partnerships, its economic dependence on Russia limits its ability to fully execute a balanced foreign policy. Armenia's foreign and security policy reflects both successes and challenges in its pursuit of a balanced approach to managing regional threats. The expansion of military and diplomatic partnerships with Western and regional powers has allowed Armenia to reduce its political and military dependence on Russia. However, Armenia's economic dependence on Russia continues to pose significant challenges to its diversification efforts. To enhance its sovereignty and resilience, Armenia must continue to pursue a balanced foreign policy, leveraging its new partnerships while addressing the economic limitations imposed by its reliance on Russia. If these dynamics persist, the likelihood increases that, upon the resolution of the Ukrainian conflict, Russia may leverage its growing economic influence to exert renewed political pressure on Armenia's foreign policy decisions. By capitalising on its economic leverage, Russia could seek to reassert control over Armenia's geopolitical orientation, particularly as Armenia attempts to diversify its external partnerships. This potential shift underscores the delicate balance Armenia faces in navigating its foreign policy, as it seeks to reduce dependence on traditional alliances while maintaining sovereignty in a complex and evolving regional environment.

However, Armenia does not seek a radical change in its foreign policy. Maintaining stable relations with Russia remains a key element of its diplomatic agenda. The country does not aim to replace dependence on Russia with reliance on another state. Instead, Armenia pursues a balanced approach, navigating competing geopolitical pressures while protecting its national interests and strategic autonomy.

Conclusions

Armenia's foreign and security policy is undergoing a structural transformation driven not by ideological realignment but by the erosion of its traditional security architecture and the reconfiguration of power relations in the South Caucasus. The collapse of Russia's credibility as a security guarantor - exposed by its failure to deter Azerbaijani coercion against Armenia, and its inability or unwillingness to prevent the 2023 ethnic cleansing of Nagorno-Karabakh - has fundamentally altered the strategic assumptions that underpinned Armenia's post-independence security paradigm. In response, Armenia has moved away from a model of single-patron dependence and adopted a strategy of diversification, hedging, and limited external balancing. This shift is consistent with neorealist expectations of small-state behavior under conditions of alliance unreliability and asymmetric threat environments.

The analysis demonstrates that this shift does not constitute a wholesale geopolitical reorientation or alliance substitution. Rather, Armenia is pursuing a calibrated and incremental strategy aimed at widening its strategic space while avoiding abrupt ruptures with existing institutional and economic ties. Engagement with the European Union, the United States, France, UAE, India has enhanced Armenia's diplomatic visibility, military resilience, and international

embeddedness, while initiatives such as EU monitoring missions, defence cooperation with France and India, and geo-economic frameworks like TRIPP function as complementary layers of soft and hard security. From a theoretical perspective, Armenia's behaviour aligns with hedging and limited external balancing, whereby diversification serves to mitigate vulnerability and increase autonomy rather than to decisively shift the balance of power.

At the same time, the study highlights the structural constraints that limit the depth and sustainability of this transformation. Armenia's continued economic dependence on Russia, reinforced by geography, closed borders, and integration within the Eurasian Economic Union, creates a persistent asymmetry between military-political diversification and economic reliance. This imbalance generates internal tension within Armenia's foreign policy and leaves open the possibility of renewed Russian leverage in the future, particularly in a post-Ukraine war environment. Consequently, Armenia's emerging foreign and security policy paradigm should be understood as adaptive rather than resolved: a pragmatic effort to navigate a hostile regional environment by maximising flexibility, resilience, and autonomy under severe structural constraints. The durability of this strategy will ultimately depend on Armenia's ability to deepen economic diversification, consolidate new partnerships, and translate external engagement into sustainable deterrence and long-term strategic stability.

BIBLIOGRAPHY:

Alrmizan, Mohammed. 2020. Armenia and Saudi Arabia: Potential Diplomacy in Complex International Relations, Riyadh, King Faisal Center for Research and Islamic Studies.

ARKA. "Armenia's foreign trade turnover decreased by 39.3% in the first nine months, amounting to $14.6 billion. Russia surpasses China and the UAE in the top three". 6 November, 2025. Accessed January 10, 2026. https://www.arka.am/en/news/economy/armenia-s-foreign-trade-turnover-decreased-by-39-3-in-the-first-nine-months-amounting-to-14-6-billio/?utm

Armenpress. "Armenia Freezes Participation in CSTO." Armenpress Armenian News Agency, February 23, 2024. Accessed January 9, 2026. https://armenpress.am/en/article/1130942

ArmStat. External trade database. 2024. Accessed January 8, 2026. https://armstat.am/en/?nid=160

Business media, Armenia's Foreign Trade Surge: Turnover Exceeds $26 Billion, 6 December, 2025, Accessed January 8, 2026. https://bm.ge/en/news/armenias-foreign-trade-surge-turnover-exceeds-26-billion?utm

Council of the European Union. Partnership Implementation Report on Armenia (SWD 2025) 401 final), Document 16174/25. Brussels, 28 November 2025. Accessed January 7, 2026. https://data.consilium.europa.eu/doc/document/ST-16174-2025-INIT/en/pdf

European Parliament. "Verbatim Report of Proceedings – Formal Sitting: Address by Nikol Pashinyan, Prime Minister of the Republic of Armenia", October 17, 2023. Accessed January 10, 2026. https://www.europarl.europa.eu/doceo/document/CRE-9-2023-10-17-ITM-005_EN.htm

Grigoryan, Armen. "Acquisition of Military Equipment from Russia Dropped from 96 Percent to Less than 10 Percent: Secretary of Security Council." First channel news, March 6, 2024. Accessed December 24, 2025. https://www.1lurer.am/en/2024/03/06/Acquisition-of-military-equipment-from-Russia-dropped-from-96-percent-to-less-than-10-percent-Secre/1089073

Ministry of Foreign Affairs of the Republic of Armenia. "The Comment of the Foreign Ministry of Armenia on the Declaration Signed by the Presidents of Turkey and Azerbaijan.", June 17, 2021. Accessed January 6, 2026. https://www.mfa.am/en/interviews-articles-and-comments/2021/06/17/mfa_ statement_on_the_decl/10995.

Ministry of Foreign Affairs of the Republic of Armenia, National Security Strategy of the Republic of Armenia, 2007. Accessed January 9, 2026. https://www.mfa.am/filemanager/Statics/ Doctrinearm.pdf

Ministry of Foreign Affairs of the Republic of Armenia. "Bilateral Relations: Russia." Accessed January 9, 2026. https://www.mfa.am/en/bilateral-relations/ru

Ministry of Foreign Affairs of the Republic of Armenia. Bilateral Relations, Saudi Arabia, 12 May 2023. Accessed January 11, 2026. https://www.mfa.am/en/bilateral-relations/sa

Ministry of Foreign Affairs of the Republic of Armenia. Bilateral Relations, United Arab Emirates. 07 February 2024. Accessed January 8, 2026. https://www.mfa.am/en/bilateral-relations/ae

Office to the Prime Minister of the Republic of Armenia. "Press Release: Granada Meeting with European Leaders", October 4, 2023. Accessed January 7, 2026. https://www.gov.am/en/news/calendar/2023/10/04/

Office to the Prime Minister of the Republic of Armenia. "Press Release on the Joint Armenia–EU–US High Level Meeting in Brussels in Support of Armenia's Resilience." April 5, 2024. Accessed January 7, 2026. https://www.primeminister.am/en/press-release/item/2024/04/05/Nikol-Pashinyan-Press-Release

Office to the Prime Minister of the Republic of Armenia. "Statement Following Quadrilateral Meeting between President Aliyev, Prime Minister Pashinyan, President Macron and President Michel", October 7, 2022. Accessed January 7, 2026. https://www.primeminister.am/en/press-release/item/2022/10/07/Nikol-Pashinyan-Announcement/

Press Service of the President of the Republic of Azerbaijan. "Declaration on Allied Interaction between the Republic of Azerbaijan and the Russian Federation", February 22, 2022. Accessed January 6, 2026. https://president.az/en/articles/view/55498

Press Service of the President of the Republic of Azerbaijan. "Joint Declaration of Allied Relations Between the Republic of Azerbaijan and the Republic of Turkey", June 15, 2021. Accessed January 5, 2026. https://president.az/en/articles/view/52122.

RFI. Armenia signs arms contract with France amid boost in military ties, 23 February 2024. Accessed January 11, 2026. https://www.rfi.fr/en/international/20240223-armenia-signs-arms-contract-with-france-amid-boost-in-military-ties

TASS. "МИД РФ считает обвинения Армении в адрес миротворцев в Карабахе деструктивными [Russian MFA Considers Armenia's Accusations Against Peacekeepers in Karabakh Destructive]", January 12, 2024. Accessed January 8, 2026. https://tass.ru/politika/ 19715639

The Government of Armenia, Programme of the government, 2021. Accessed January 9, 2026. https://www.gov.am/en/gov-program/

The Government of Armenia. National Security Strategy of the Republic of Armenia, 2020. Accessed January 10, 2026. https://www.mfa.am/filemanager/security%20and%20defense/Armenia%202020%20National%20Security%20Strategy.pdf

The Office to the Prime Minister of the Republic of Armenia. Press releases, Nikol Pashinyan and Abdel Fattah el-Sisi make statements. 05 March 2024. Accessed January 11, 2026. https://www.primeminister.am/en/press-release/item/2024/03/05/Nikol-Pashinyan-Statement/

UN Meetings Coverage and Press Releases. 15 September 2022. Amid Fighting between Armenia, Azerbaijan, Assistant Secretary-General Urges Both Parties Commit to Lasting Peace Treaty, in Security Council Briefing, 9132ND MEETING (AM), SC/15031. Accessed January 8, 2026. https://press.un.org/en/2022/sc15031.doc.htm

Waltz, Kenneth. 1979. *Theory of International Politics*. Reading, MA: Addison-Wesley.

DOI: 10.53477/3045-2309-26-09

THE BLACK SEA REGION IN THE CONTEXT OF FOUR YEARS OF WAR IN UKRAINE. THE GAME OF CHESS BETWEEN NATO, EU, RUSSIA, AND OTHER RELEVANT ACTORS

Daniela LICĂ, PhD,
Researcher, Centre for Defence and Security Strategic Studies,
"Carol I" National Defence University, Bucharest, Romania.
E-mail: lica.daniela@unap.ro

Ana-Maria FLOREA,
PhD Candidate, National School of Political and Administrative Studies, Bucharest, Romania.
E-mail: ana.m.florea8@gmail.com

Abstract: *The paper examines aspects related to the Black Sea Region (BSR) security environment in the context of four years of ongoing conflict in Ukraine, including most recent advances up to March 2026. The region is seen as a strategic chessboard shaped by intensifying great-power rivalry, divergent dynamics within the Alliance and the EU and the expanding use of hybrid threats.*
The paper aims to discuss the posture of concerned actors on the chessboard as it results from strategic documents and position statements that make up StratCom; the relation among them is also approached in the light of recent developments as a result of the regime change in the USA, for instance. And last but not least, narrative coherence is approached, bringing into attention issues such as coordination and synchronisation. All these are seen as key indicators of diplomacy during wartime.
Using offensive Realism and alliance theories, as well as qualitative analysis of strategic documents, defence procurement data, and mass-media articles presenting key StratCom messages, the study argues that NATO and the EU operate as complementary but asymmetrical players whose sometimes divergent strategies determine the operational landscape and regional balance of power.
Particular attention is given to the role of Romania, positioned as a frontier country for NATO's Eastern Flank. Written from the perspective of a NATO and EU member, the paper concludes that a resolution of the conflict and the achievement of effective stability require coherent multi-domain responses, alongside enhanced cooperation and aligned Euro-Atlantic strategic planning and actions.

Keywords: *Black Sea Region (BSR); diplomacy during wartime; defence strategy; hybrid warfare; NATO-EU strategic cooperation; strategic engagement.*

Introduction

With Russia's actions in the last two decades (invasion of Georgia in 2008, occupation of Ukrainian territory of Crimea in 2014 and subsequent invasion of the country in 2022), reflecting its grand strategy that translates in regional hegemonic ambitions and the will to regain the status of a great world power, the Black Sea Region (BSR) has become the security centre of gravity for Europe (Gaber 2024, 1-2). In other words, the BSR can be seen as a pivotal strategic chessboard on which regional and extra-regional powers manoeuvre for influence, positional advantage and deterrence dominance. Renewed great-power rivalry, NATO's reinforced posture, and the European Union's growing concern with hybrid coercion have collectively transformed the region into a multi-domain battlespace in which military action, diplomacy and economic leverage converge. Russia's hybrid strategies have fundamentally altered the equilibrium, compelling NATO and the EU to rethink how

they counter multi-vector threats that span information, cyber, and energy domains beside classical ones (land, air, maritime, and space).

The BSR is seen as a chessboard, similarly to Brzezinski's use of the expression in his book *The Grand Chessboard* (Brzezinski 2016). State and supranational actors are seen as autonomous players, some having a larger manoeuvre of action than others, depending on their power resources, position and implication in the ongoing regional events, dominated by the war in Ukraine. In using the metaphor of chess, there was taken into account that it is a game of strategy built on anticipation, patience, and cumulative advantage. Victory rarely comes through a single dramatic move; rather, it emerges from sustained positional pressure and the gradual restriction of the opponent's options. As Sun Tzu observed, "The supreme art of war is to subdue the enemy without fighting" (Tzu 2005). In this sense, both chess and strategic competition in the BSR illustrate that decisive outcomes are often prepared long before the final move. Checkmate, as like strategic victory, is achieved not through impulse but through disciplined coordination, foresight, and the careful sequencing of power.

Against this backdrop, the paper argues that diplomacy during wartime is a form of strategic engagement whereby states coordinate diplomatic and military instruments, including Cognitive Warfare with its information component, as well as economic instruments to shape the adversary's behaviour, impose costs upon them and protect own strategic positions without further escalating the full-scale conflict. Framed through the metaphor of chess, war diplomacy is treated as a sequential, cumulative contest in which states employ strategic moves, anticipate counter-moves, seeking positional superiority.

The analysis draws on offensive Realism and alliance theory, combined with qualitative examination of strategic documents and defence procurement trends, as well as mass-media articles presenting key StratCom messages.

1. Hybrid Warfare as Irregular Strategic Play. Strategic Terrain and Operational Realities in the BSR

Dominated by the current attrition war in Ukraine, now in its fifth year, the Wider Black Sea Region has become an area where national and supranational actors struggle to find ways to cope with the effects of this hybrid war, impacting countries and people in multiple ways. Against this backdrop, manifestations of power projection by the actors located in the region or with interests in this area, such as the USA, result in shifts, increasing already existent challenges and rising volatility of the security environment.

The section provides a synthetic *X-ray* type of analysis related to the current security environment in the BSR, on the background of the war in Ukraine, highlighting several aspects considered important, including most recent developments[1], also providing explanations and illustrations.

A first aspect to consider is that *the war, with its hybrid components, goes beyond the two belligerent countries*, extending to Ukraine's supporting partners (NATO, the EU and their members, and the USA with its own large contributions), *entailing costs and consequences for those states and organisations.*

The EU and the North Atlantic Alliance have made a pledge on granting longstanding support to Ukraine (NATO 2026), in the name of defending democracy and the international law. Based on political will and consensus, huge aid was provided to Ukraine in funding, weapons and support equipment, training and know-how for the military and for the central administration, economic sanctions imposed on Russia, and humanitarian aid, for instance. Another direction of the aid envisages efforts to counter the Russian disinformation (EU n.d.), this aspect being also of constant internal concern for NATO and the EU.

The continuous and multidimensional aid provided to Kyiv for the past four years involved considerable economic resources (EEAS 2025), (Gutterman, Foltynova and Sijamija 2025), (Statista

[1] The analysis, elaborated in the first months of 2026, includes developments up to the beginning of March.

n.d.), (Kiel Institut 2025), (Ardelean 2025), impacting on the economies of the donor states. These expenses are publicly shown as being cost-effective actions and even resulting in economic benefits, being "significantly cheaper than the potential costs of deterring Russia in the event of its victory" (Chouet 2025), (McCusker 2024). A recent study elaborated by Corisk and the Norwegian Institute of International Affairs argues that "a Russian military victory in Ukraine would cost Europe twice as much as a Ukrainian victory" (Bjørtvedt 2025) apud (Olteanu 2025). However, in our opinion, this can also be seen as StratCom advocating for maintaining public opinion's support for the aids, despite economic negative effects felt in the daily life even since the early stages of the war. These translate in rising inflation (Smit 2022), (Afunts, Cato and Schmidt 2024), reduced levels of consumption, and also increase of the VAT and of taxation, and even lower incomes in the public sector, as observed, for instance, in Romania.

Additionally, it should be considered that supporting Ukraine in the war may generate or enhance the risk of vulnerability to Moscow's threat, especially for the countries located in its proximity that make up NATO's Eastern Flank. Thus, there were several reports of Russian drones incursions and drones or parts of drones fallen in Romania and in Poland (Starinac and Bostenaru 2025), (Drilea 2023), Romanian authorities reaction evolving throughout the war developments (Euronews 2025), (Dima 2025). It should be kept in mind that a state supporting Kyiv becomes an adversary of Kremlin and, consequently, a target of its information warfare. One example of the Russian aggressive rhetoric is the nuclear bomb threat (Reuters 2024). The threat narrative has also been present in the past years, with NATO SecGen and member countries senior military warnings of such a possible outcome, for instance in Germany (Gardner and Wong 2025) and in Romania (Observator 2024). The NATO SecGen's declaration in December 2025 that «members of the Alliance could be "Russia's next target"» (CNN 2025) in the following years serves as a compelling argument "for a rapid rise in defense spending to prevent a war similar to those seen by past generations" (CNN 2025). The timeframe for such a possible attack, announced since early 2024, varies between three, five or eight years, extending up to a decade (Financial Times 2024) (Daily Mail 2024).

However, the media also reflected contrasting instances of StratCom, reassuring the public that such a threat does not exist. Illustrations come from the former NATO SecGen's statement at the end of January 2024 that no direct or imminent threat against an ally was perceived (NATO SG 2024) and, similarly, from the former Romanian Prime Minister, stating, in an electoral year, that there is no threat of an attack against the country, contrary to the declaration of the Chief of the General Staff (Observator 2024). These divergent public communication messages, occuring within a short period of time (January-February 2024), indicate a lack of coordination both at the Alliance level and between political and military authorities at the national level, in some European states[2]. The situation generates a negative cognitive and emotional impact on the public opinion in NATO member countries and at the same time makes them vulnerable to Russia, which exploits such aspects and causes them to backfire in the form of disinformation/hostile narratives.

As seen, *the war, with its hybrid components, goes beyond the two belligerent countries*, as it extends to the supporting partners as well, with negative consequences spanning across their populations. Referring to the cognitive dimension, following media monitorisation throughout the conflict development, it can be stated that *all parties involved use information as a weapon* in various ways, aiming to maximise the chances of victory. This translates, for instance, in contrasting narratives and reciprocal accusations of disinformation and propaganda[3]. Contrasting narratives regarding the dead and casualty tolls of Russia and Ukraine, for example, may produce several effects: they generate confusion for the adversary, represent an element of power projection in relation to the adversary when displaying a larger number of victims and have a positive impact upon the morale of

[2] For more details, see Daniela Lică, "Dezinformarea în contextul a doi ani de război în Ucraina" in *Colocviu strategic* nr. 2/2024 (Lică 2024).
[3] *Ibidem*.

one's own military and population when lower numbers are made public. As for reciprocal accusations, while Ukraine and the West repeatedly assert that Russia employs cognitive warfare against them (EEAS n.d.), the Kremlin accuses Ukraine, the EU, and NATO of lying (WION 2025). Consequently, *a continuous information chaos results*, on an infodemic[4] background, whose *effects* (of a cognitive nature – psychological and emotional), *push the war* beyond the military sphere, *into daily life*. Moreover, the disinformation process is developed progressively with the application of the latest technological developments, including Artificial Intelligence (AI), Machine Learning (ML), and brain-machine interfaces (BMI).

Another important characteristic factor not only for this area, but for the global security environment as well is the *very high dynamics and volatility also reflected in bilateral and multilateral relations*. This aspect is of major concern in the current war context, which is already challenging, in multiple ways. An illustration is the major shift in the USA foreign policy with President Trump's second term-in-office, showing a pragmatic nationalist view, based on transactional relations. The President's declarations and actions place the EU, NATO, and their member countries in challenging positions, making them wonder whether the alliance and strategic partnership are still valid.

The promise to «make America great again» translated in MAGA policies included the intention to impose additional trade fees to foreign actors such as the EU, generating great economic costs. Brussels responded in a similar way, and diplomatic talks were ongoing for months (Le Monde with AFP 2025), until a deal was finally agreed at the end of July last year (Commission 2025). Former close diplomatic ties have come under scrutiny, especially with the USA ambition to acquire Greenland from Denmark, an Allied country (Belin 2025). Subsequently, the EU provided a prudent diplomatic response, in order to prevent worsening of relations in a challenging security context. Some analysts considered this a "cacophony [showing] weakness at home and abroad" (Balfour 2026), with a chance to be turned into strategic ambiguity, should the anti-coercion instrument (ACI) be applied. The ACI allows the EU to take deterrence and retaliatory measures if established that a foreign actor makes use of economic coercion to undermine Brussels (Balfour 2026).

Regarding USA-NATO relations, the American leader adopted an ambiguous StratCom, casting doubt upon allies at key moments on the commitment to Article 5 (Lunday, Traylor and Kayali 2025), (Liptak 2025), while emphasising that their contribution is the largest and asking the Allies at The Hague 2025 Summit to bolster defence spending from 2% to 5% over the following decade (Liptak 2025).

With these challenges, the division among EU member states (some of which are also NATO members) comes as an additional problem in handling the transatlantic relation. Europe is still dependent on the USA for granting its security, both economically and cognitively (as a reflection of a post-communist educated diplomatic mindset) (Balfour 2026). A blunt piece of StratCom in this respect is that of NATO SecGen stating that Europe does not have a chance to defend itself without USA support unless defence spending were increased to 10% to create a nuclear capability (Danaher 2026), which is quite unrealistic, having in mind the current economic situation.

As observed, the recently released American strategic documents do not prioritise Europe, and do not even mention the Black Sea. When presenting issues of concern for Europe, the 2025 National Security Strategy (NSS) points to "insufficient military spending and economic stagnation" (The White House 2025, 25), as well as "migration policies […] transforming the continent and creating strife, censorship of free speech and suppression of political opposition" (The White House 2025, 25). Additionally, the EU is described as undermining "political liberty and sovereignty" (The White House 2025, 25). As for the 2026 National Defense Strategy (NDS), it stipulates increasing the burden sharing with Allies and Partners and putting an end to their dependency, also pointing that they must take the lead against threats that are more severe for Europe than for the USA (Department of War 2026, 4).

[4] *Infodemy* refers to a massive amount of widely and rapidly circulating information about a particular crisis or controversial issue, consisting of a confusing combination of fact, falsehood, rumour, and opinion (Dictionary.com 2024).

Additionally, there is the *issue of strategic and vital resources*, primarily energy, and the challenges for ensuring it lead to a continuum of competition that can either result in cooperation or in confrontation. An important aspect with impact on security regards the European dependency on Russian oil, gas and nuclear energy imports, allowing Kremlin to use it as a weapon, as "hydrocarbons are not simply a market commodity but a key element of the hybrid toolkit to advance its strategic interests" (Gaber 2024). Since the beginning of the war in Ukraine, the EU has committed itself to gradually reduce and ultimately put an end to this dependency through the REPowerEU strategy. Thus, EU reliance on Russian gas has decreased from about half of overall imports, namely 45% in early 2022 to 12% in 2025, while oil imports diminished from 27% at the beginning of 2022 to only 2%, at present having two EU countries importing Russian oil (Hungary and Slovakia). At the end of January 2026, the EU adopted a regulation (EURLex 2026) aiming to gradually and permanently put a ban on Russian oil imports by no later than 2027, with the overall goal of strengthening Europe's energy security and independence (European Commission 2026).

The last aspect to be mentioned is related to the *uncertainty and lack of perspective for a cease of fire*, as peace talks between Russia and the Ukraine, going on since mid-May 2025, have been difficult and led to no concrete results. More concretely, peace negotiations have been characterised by conflicting attitudes, each of the belligerent parties claiming to desire peace while accusing the opposing side of not wanting it. A very recent survey conducted by the Kyiv International Institute of Sociology (KMIS), has shown that about 70% of Ukrainian people do not believe in a positive outcome of the negotiations (Charter 97 2026). Following media monitoring throughout the period, a continuous tendency to condemn and even demonise the adversary can be noticed, as well as a lack of willingness for conciliation, with each side conditioning the adversary, territorial claims being the unsurpassable aspect of negociations (Ehl 2025). As a result, peace negotiations have paradoxically turned in a war of statements and, what is more, escalations of the conflict can be seen on the ground (Lederer 2026) (Kakissis and Fadel 2025). At present, there is no agreed scenario on what the outcome of the war could be and how Ukraine will look like in terms of frontier with the Russian Federation (Global Times 2026), including access to the Black Sea. The USA has been putting pressure to resolve the conflict, hopefully by summer (Lederer 2026). Moreover, by engaging, together with Israel, in a new conflict in Iran, which has been expanding across the Middle East, the USA is facing additional security challenges, and President Trump's actions have been largely criticised (Walldorf 2026). Although happening at a distance from Europe and the region under current focus, concrete effects have been felt in this area as well, for instance regarding repeated increase in fuel prices in Romania (Grigorescu 2026).

Summing up, the key aspects addressed dwell on the following: the war, with its hybrid components, extends beyond the two belligerent countries, entailing costs and various consequences for the states and organisations supporting Ukraine; all parties involved use information as a weapon on the background of the conflict, resulting in a continuous information chaos pushing the war into daily life; the very high dynamics and volatility reflected in bilateral and multilateral relations, with reference to the relations between the USA and NATO and especially with the EU; European dependency on the USA for granting its security; the issue of strategic and vital resources, primarily energy, with the European dependency of the Russian oil; and last, but not least, the uncertainty and lack of perspective for a ceasefire.

For the near future, there needs to be taken into account that no matter what the result will be, Ukraine will further need consistent and multidimensional support to recover from the war. From a national point of view, Romania has to be a part of the process, as Ukraine is its neighbour (Colibășanu 2026). Also, we consider that cooperation among regional actors, the EU and NATO included, will be of the highest importance, and USA support, as a major world power would also be beneficial, especially from a financial point of view.

2. Strategic Indicators of Diplomacy During Wartime

The wider Black Sea Region has evolved into a multidomain theatre defined by structural rivalry, hybrid confrontation, and institutional balancing. The war in Ukraine has fundamentally

transformed the regional security architecture, producing a condition of continuous strategic contestation rather than episodic crises. In order to better understand the positioning of Russia, NATO, the EU, and Romania on the BSR chessboard, doctrinal documents are going to be analysed, providing essential aspects from these, as key indicators of war diplomacy actions.

2.1. Doctrinal Posture and Escalation Logic

Strategic documents provide codified expressions of threat perception and escalation logic, therefore, analysing doctrine is indispensable for understanding the way of thinking that lies at the foundation of an actor's narratives and actions that constitute diplomacy, especially in a war context (Echevarria 2017, 88-104), (Gray 1999).

Russian hybrid activities in NATO and EU countries, such as cyber attacks and influence activities – operating below the threshold of declared war – illustrate limited coercion designed to establish *faits accomplis* while avoiding full-scale escalation. These dynamics align with broader understandings of grey-zone competition (Rid 2012). Official Russian documents frame such measures within narratives of sovereignty protection and resistance to external interference (President of the Russian Federation 2021).

Thus, the Russian Federation's National Security Strategy explicitly identifies NATO expansion and Western military infrastructure near Russian borders as primary threats, perceiving the Alliance's activity as destabilising and emphasising Russia's sovereignty and territorial integrity (President of the Russian Federation 2021).

The Maritime Doctrine of the Russian Federation designates the Black Sea as a priority region for safeguarding sovereignty and projecting naval power, reinforcing the importance of fleet modernisation and maritime sovereignty in the Black Sea (President of the Russian Federation 2022).

These documents articulate a Russian posture centred on layered defence, maritime dominance, and resistance to perceived encirclement, which generates structural insecurity for NATO's Eastern Flank states, particularly Romania and Bulgaria.

NATO's Strategic Concept characterises Russia as "the most significant and direct threat" (NATO 2022, 4) to Allied security and commits to strengthened forward defence and deterrence-by-denial, multidomain integration, and high-readiness forces (NATO 2022, 4).

Alliance responses reflect balance-of-threat dynamics, whereby states align against perceived aggressive intent rather than power alone (S. Walt 1987, 17-33), (Snyder 1997, 180-192), (S. M. Walt 2010), (Niemi 2026), or in other words, threat perception plays a determinant role (Cohen 1978). Enhanced forward presence, rotational deployments, and increased defence expenditure documented in NATO's Defence Expenditure Report for the period 2014–2023 illustrate institutionalised balancing (NATO 2023).

NATO doctrinal documents, as well as other public statements – both illustrations of StratCom – signal preparedness, reinforcing collective defence commitments, and emphasising integrated conventional and nuclear deterrence. These communications serve as a proof of the credibility of its posture, a few illustrative examples including the NATO Strategic Concept (NATO 2022) and Summits Declarations, most recently at The Hague in June 2025 (NATO 2025).

The European Union regulatory and resilience-oriented instruments complement NATO's military posture. Thus, the EU Strategic Compass prioritises resilience and hybrid threat response through a comprehensive Hybrid Toolbox, encompassing cyber defence, critical infrastructure protection, including maritime infrastructure, and countering foreign information manipulation and interference (FIMI) (EU 2022). Additionally, the EU Cybersecurity Strategy further emphasises institutional resilience against state-sponsored malicious cyber activities (European Commission 2020).

The Joint EU-NATO Declaration in 2023 highlights "the importance of the transatlantic bond" (NATO 2023) while acknowledging that the context requires for an even closer cooperation. Thus, the two organisations commit to further mobilizing the "combined set of instruments […], be they political, economic or military […], strengthening cooperation in existing areas" (NATO 2023), and

increasing it in the following fields: "growing geostrategic competition, resilience […], protection of critical infrastructures, emerging and disruptive technologies, space, security implications of climate change, as well as FIMI" (NATO 2023). This discursive alignment reduces fragmentation and strengthens institutional credibility.

From a national point of view, Romania's National Defence Strategy for the period 2025–2030 aligns national priorities with NATO and EU frameworks, identifying the BRS as a highly important strategic area and emphasising the need to develop national capabilities of defence and resilience and interoperability with the allies and partners (Romanian Presidency 2025, Ch. 5, para. 103). The Military Strategy of Romania from 2021, still in force, envisaged as national military objective (for the period up to 2024) an increase of the presence of Allied and partner forces in the region, while facilitating mobility, collocation and deployment (Ministry of National Defence of Romania 2021, 12); nevertheless, it should be taken into account that the cited document precedes the outburst of the war in Ukraine, an updated version being currently in final stages of elaboration.

As a preliminary conclusion, we consider that narrative convergence across national and supranational levels (for instance NATO), referring to doctrine and various position statements, constitutes a core indicator of war diplomacy in practice.

2.2. Diplomacy during wartime and Strategic Competition in the BSR

Diplomacy during wartime translates in the coordinated use of military posture, economic instruments, and diplomatic signalling. This approach builds upon the Clausewitzian understanding of war as a continuation of politics (Clausewitz 1976) and on coercive diplomacy frameworks emphasising the manipulation of adversary expectations through credible signalling (Schelling 1966, 1-34; 69-91), (George 1991, 4-11). Deterrence seeks to prevent adversarial action by raising anticipated costs (Huth 1988, 20-35), (Jervis 1989, 1-28), while compellence attempts to induce behavioural change through sustained pressure (Byman and Waxman 2002, 30-45), (Pape 1996, 12-18).

As observed, strategic manoeuvre unfolds cumulatively across the Black Sea Region chessboard. NATO's reinforcement measures, EU sanctions regimes, and national defence modernisation interact sequentially, shaping adversary cost-benefit calculations over time. Such incremental positioning reflects a strategic logic of gradual environment-shaping rather than decisive confrontation (Gray 1999, 121-128), (Mazarr 2015, 9-28). From a structural perspective, the regional strategic behaviour can be interpreted through the logic of power maximisation under anarchy (Waltz 1979, 102-128), (J. J. Mearsheimer 2014, 30-36).

In the current security context, deterrence-by-denial through forward defence operates in the BSR alongside economic sanctions and diplomatic coordination. To sum up, it can be stated that the regional security environment is shaped by a layered strategic interaction, in which military deterrence, economic sanctions, regulatory coordination, and narrative competition operate simultaneously.

2.3. Strategic Narratives as Diplomatic Tool and the Importance of Coordination

Strategic narratives, by shaping perceptions, attitudes and behaviours, impact on political decisions and military actions legitimacy, and also upon national cohesion and cohesion within supranational entities such as NATO and the EU, and, not least, upon escalation thresholds.

In this context, NATO's official documents and communications, for instance, show a defensive posture grounded in collective security commitments (NATO 2022), while the Russian ones portray NATO expansion as a threat to its sovereignty and stability (President of the Russian Federation 2021) and use this as a legitimisation for the ongoing war in Ukraine (President of the Russian Federation 2022). Simultaneously, Russian naval modernisation, as articulated in the maritime doctrine, underscores sustained regional ambition and capacity for sea denial (President of the Russian Federation 2022).

Romania's strategic narratives reflected in documents and official discourse situate national defence within the broader Euro-Atlantic framework, reinforcing alignment with the two organisations and strategic coherence (Romanian Presidency 2025, 4-6).

Discursive synchronisation and coordination among NATO and EU members, and also between the two organisations, enhance credibility and reduce opportunities for adversaries to exploit internal divergences. Accordingly, it can be stated that strategic narratives are a valuable diplomatic tool.

3. Romania's Strategic Posture on NATO's Eastern Flank

Romania's strategic posture on NATO's Eastern Flank can be best understood through the combined lenses of offensive realism, alliance theory, and theories of cooperation under anarchy (Waltz 1979, 102-128), (J. J. Mearsheimer 2014, 30-36), (S. Walt 1987, 17-33), (Snyder 1997, 180-192), (Keohane 1984, 49-64). Together, these approaches illuminate how a medium power positioned in a contested geopolitical space seeks to maximise security, manage asymmetries relative to great powers, and reduce vulnerability in an environment characterised by constant change, hybrid threats, and persistent revisionism (Axelrod 1984, 12-20), (Hoffman 2009, 34-36), (Lanoszka 2016, 175-182). Diplomacy during wartime thus emerges not as a departure from realist logic but as its contemporary operationalisation under conditions of sub-threshold conflict, where coercion, signalling, and selective cooperation coexist as instruments of strategic competition (Schelling 1966, 12-20), (NATO 2022), (Romanian Presidency 2025).

3.1. Deterrence and Resilience through the Lens of Offensive Realism

From the perspective of offensive Realism, the Black Sea Region represents a classic arena of power competition in which states operate under conditions of anarchy and uncertainty regarding the intentions of others (J. J. Mearsheimer 2014, 29-36). Russia's military build-up, anti-access/area-denial (A2/AD) posture, and use of hybrid instruments confirm the realist assumption that great powers seek to maximise relative power and shape regional order in their favour.

Romania's emphasis on deterrence and resilience reflects a rational response to the structural constraints imposed by its position on NATO's Eastern Flank and proximity to a revisionist power in the Black Sea. From an offensive realist perspective, states exposed to heightened threats prioritise survival through capability enhancement rather than power maximisation or normative restraint (Waltz 1979, 126), (J. J. Mearsheimer 2014, 29-36).

While trying to balance its inequities with strategic alliances, Romania has therefore focused on deterrence by denial, investing in territorial defence, host-nation support, and critical infrastructure resilience while embedding these efforts within NATO's collective defence framework (S. Walt 1987, 17-18), (NATO 2022).

Within this context, diplomacy during wartime deepens limited national power by linking military preparedness with diplomatic signalling and alliance credibility. Strategic Communication and participation in multinational exercises reinforces perceptions of determination among allies and shapes adversary expectations, making deterrence a relational process grounded in alliance politics rather than material capabilities alone (Snyder 1997, 43-45; 180-192).

3.2. Alliance Politics and Strategic Partnerships – Insights from Alliance Theory

Alliance theory provides further explanatory leverage for understanding Romania's strategic behaviour. Classical alliance theorists emphasise that states align not out of ideological affinity, but in response to threats (S. Walt 1987, 17-18). Romania's deepening strategic partnerships with the United States, the United Kingdom, and France can be interpreted as a form of external balancing against perceived Russian revisionism in the Black Sea.

At the same time, alliance theory highlights the twin risks of abandonment and entrapment (Snyder 1997, 43-45; 180-192). Romania's security strategy seeks to minimise abandonment by

demonstrating commitment, interoperability, and burden-sharing within NATO. Forward presence, defence spending increases, and procurement aligned with Allied standards are signals designed to reassure major Allies of Romania's reliability and at the same time of its strategic value in the region.

These dynamics underscore that Romania's partnerships are not merely bilateral security arrangements, but instruments through which alliance credibility and deterrence are co-produced.

While Realism traditionally privileges competition, contemporary theories of cooperation under anarchy demonstrate that states may engage in limited, functional cooperation when interests converge and institutions reduce uncertainty (Keohane 1984, 12-20), (Axelrod 1984, 124-141). Romania's trilateral cooperation with Türkiye and Bulgaria, reflected in the Mine Countermeasures Black Sea Task Group (MCM BSTG) reveals such logic. From a diplomatic perspective, trilateral formats act as confidence-building mechanisms that stabilise interaction without diluting deterrence.

Defence procurement decisions are central to Romania's strategic alignment and reflect core realist assumptions about power and security. Offensive realism emphasises that military capabilities underpin credibility, while alliance theory highlights interoperability as a key determinant of alliance effectiveness (J. Mearsheimer 2001, 31; 55-57), (Snyder 1997, 43-45; 180-192).

Romania's acquisition of U.S. and European systems – particularly in air defence, naval platforms, and command-and-control – serves multiple strategic functions: enhancing national deterrence, embedding Romania within NATO's operational ecosystem, and signalling long-term commitment to alliance priorities in the Black Sea (NATO 2022), (Ministry of National Defence of Romania 2021).

In this sense, it can be stated that defence procurement functions as a sort of conclusive diplomacy, in the sense that it is costly, durable, and politically binding, thus linking military modernisation with alliance cohesion. Diplomacy during wartime thus operates at the intersection of defence economics and strategic alignment, reinforcing deterrence and reducing the risks of alliance abandonment (Snyder 1997, 43-45; 180-192).

Conclusions

The paper provided an analysis of the Black Sea Region security environment, where the region is envisaged as a strategic chessboard dominated by the war in Ukraine, entered in its fifth year. Following other Russian actions in the region in last two decades, expressing its longing to regain former status of a great world power and regional hegemon, this war turned once again the area in the security centre of gravity for Europe.

As observed, the war's multiple effects are dominating regional security, characterised by intensifying great-power rivalry, divergent dynamics within NATO and the EU and the expanding use of hybrid threats. Specific aspects of diplomacy during wartime are revealed, having as protagonists both regional and international actors, seen as chess players. Also, major impacts of the war for the countries supporting Ukraine are discussed. Thus, apart from challenges of military nature, such as drones incursions and parts of drones fallen on NATO's Eastern Flank countries, other challenges, such as economic and even societal ones have emerged or deepened on the background of the war.

Power projection manifestations by actors either located in the region (Russia, Türkiye, Romania), operating herein (NATO, the EU), or having strategic interests in the area (the USA), result in shifts, increasing already existent challenges and rising volatility of the security environment. Another aspect worth mentioning is that capability development reinforces the competitive structure of the region.

The current span of hybrid threats compels NATO and the EU to rethink their ways and means to counter such challenges. A key conclusion is that the two actors operate as complementary players, whose strategies and actions determine the regional balance of power. However, it should be noticed that they are not symmetrical players – primarily, the EU is not a military-focused entity; additionally, the two organisations sometimes have divergent strategies and position statements, which impact the operational landscape. Nevertheless, this asymmetry does not undermine their effectiveness, but it produces a layered structure, where military deterrence, combined with economic instruments,

institutional coordination, and ultimately Strategic Communication interact in a complex way, reinforcing deterrence credibility, while revealing the weak points in the Euro-Atlantic strategic partnership, also reflected in the security framework. Thus, NATO and the EU should assume which of the two takes on the leader and respectively the supporter role, on a case by case issue. Also, Europeans need to assume their own security without depending so much on US contribution, having in mind the American engagement other parts of the world, namely in the Middle East and the focus on China. Moreover, European strategic autonomy that has become a buzz word in the past years should be put in practice. In this respect, the paper argues that restoring security and safeguarding stability on the BSR chessboard requires synchronised Euro-Atlantic approaches, enhanced cooperation and greater integration of military and diplomatic tools within coherent multi-domain responses.

In our opinion, war diplomacy in the BSR operates through narrative coordination and synchronisation, including doctrine, and also through capability development, to include procurement. Another important regional characteristic translates in a continuous competition below the threshold of open conflict. Together, these elements shape the regional balance of power, and at the same time they define the operational landscape.

For coherence and credibility issues, we consider that there needs to be a convergence between strategic documents, public declarations and position statements, especially in the context of ongoing conflict developments. Otherwise, impredictibility, contradictory declarations and/or contradictions between words and actions may lead to additional challenges for other actors while they make efforts to cope with the impacts of the conflict.

In terms of perspective, regardless of the war's outcome, it is important needs to take into account that Ukraine will further need consistent and multidimensional support to recover. Speaking from a national point of view, as a neighbouring state, Romania will most probably be a part of the process. Cooperation among regional actors, the EU and NATO included, will be of high importance, as well as US support.

In the light of the aspects developed in the paper, two open questions arise for further reflection, addressed to any potential reader: in the current war context, in terms of threat perception, where can a line be drawn between an adversarial actor's proactive measures, deterrence and escalation of conflict? And the second question – in an age where the power of words is acknowledged, why is defence diplomacy not put to work in positive terms, to resolve the conflict, but in negative ones, maintaining and further fuelling it?

All in all, diplomacy nevertheless will need to provide a viable solution to the current war destabilising the region and consuming resources, while affecting lots of humans, both directly and indirectly. Thus, political will, cooperation, and compromise seem the only way towards maintaining an equilibrium, as everything is interconnected in geopolitics.

BIBLIOGRAPHY:

Afunts, Geghetsik, Misina Cato, and Tobias Schmidt. 2024. "Inflation expectations in the wake of the war in Ukraine". *Journal of Behavioral and Experimental Economics.* doi:https://doi.org/10.1016/j.socec.2024.102303.

Ardelean, Adrian. 2025. *Consiliul Fiscal: România a sprijinit Ucraina cu 1,5 miliarde de euro, echivalentul a 10% din dobânzile plătite de statul român.* 03 September. https://romania.europalibera.org/a/consiliul-fiscal-romania-a-sprijinit-ucraina-cu-1-5-miliarde-de-euro-de-la-inceputul-razboiului/33520491.html.

Axelrod, Robert. 1984. *The evolution of cooperation.* New York: Basic Books.

Balfour, Rosa. 2026. "The EU finally used an economic threat against Trump. But the markets forced his climbdown". *The Guardian.* Accessed February 6, 2026. https://www.theguardian.com/commentisfree/2026/jan/24/eu-economic-threat-donald-trump-greenland.

Belin, Celia. 2025. “MAGA goes global: Trump’s plan for Europe”. (European Council on Foreign Relations (ECFR)). Accessed February 05, 2026. https://ecfr.eu/publication/maga-goes-global-trumps-plan-for-europe/.

Bjørtvedt, Erlend et al. 2025. *Europe's choice. Military and economic scenarios for the War in Ukraine*. CORISK & NUPI (Norwegian Institute of International Affairs). Accessed February 4, 2026. doi:10.13140/RG.2.2.29662.70725.

Brzezinski, Zbigniew. 2016. *The Grand Chessboard*. Basic Books. https://books.google.ro/books/about/The_Grand_Chessboard.html?id=pFhxDAAAQBAJ&redir_esc=y.

Byman, Daniel, and Matthew Waxman. 2002. *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might*. Cambridge: Cambridge University Press.

Charter 97. 2026. “Ukrainians Do Not Believe In Peace Through Negotiations, Nor In Putin's Voiced Goal Of War. Survey”. *Charter 97*. https://charter97.org/en/news/2026/1/16/670176/.

Chouet, Armand. 2025. *Economic Benefits of Continuing Military Aid to Ukraine*. Robert Lansing Institute. 13 January. Accessed February 4, 2026. https://lansinginstitute.org/2025/01/13/economic-benefits-of-continuing-military-aid-to-ukraine/.

Clausewitz, Carl von. 1976. *On War*. Edited by Michael Howard and Peter Paret. Princeton University Press.

CNN. 2025. Edited by Issy Ronald. *CNN*. Accessed January 28 2026. https://edition.cnn.com/2025/12/11/europe/mark-rutte-nato-chief-russia-europe-intl.

Cohen, Raymond. 1978. “Threat Perception in International Crisis 93”, no. 1. *Political Science Quarterly*, 93-107. https://www.jstor.org/stable/2149052.

Colibășanu, Antonia, interview by Cristina Cileacu. 2026. *Cum poate Europa să arate forță în era Trump. Antonia Colibășanu: A vorbit pe limba lui și a rezultat un tratament de la egal la egal* Digi24, (30 January). https://www.digi24.ro/stiri/externe/ue/...

Commission, European. 2025. “Joint Statement on a United States-European Union framework on an agreement on reciprocal, fair and balanced trade”. 21 August. Accessed February 6, 2026. https://policy.trade.ec.europa.eu/news/joint-statement-united-states-european-union-framework-agreement-reciprocal-fair-and-balanced-trade-2025-08-21_en.

Daily Mail. 2024. “Germany is preparing for Putin attack against NATO in 2025: Leaked secret plans reveal step-by-step how Russia will escalate conflict to all-out war in 18 months.” 15 January. https://www.dailymail.co.uk/news/article-12964575/Germany-preparing-Putin-attack-against-NATO-2025-Leaked-secret-plans-reveal-step-step-Russia-escalate-conflict-war-18-months.html.

Danaher, Caitlin. 2026. “NATO chief says Europe should ‘keep on dreaming’ if it thinks it can defend itself without the US.” *CNN*. Accessed February 6, 2026. https://edition.cnn.com/2026/01/26/europe/nato-chief-rutte-european-defense-us-intl.

Department of War. 2026. *National Defence Strategy (2026 NDS)*. https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF.

Dictionary.com. 2024. *Infodemic*. Random house. https://www.dictionary.com/browse/infodemic.

Dima, Maria. 2025. “Armata şi aliaţii NATO pot doborî drone în spaţiul aerian. Echipamente suplimentare pentru România”. https://evz.ro/armata-si-aliatii-nato-pot-dobori-drone-in-spatiul-aerian-echipamente-suplimentare-pentru-romania.html.

Drilea, Andreea. 2023. “S-a dublat numărul localităţilor care primesc mesaje Ro-Alert cu privire la pericolul de cădere a unor bucăţi de drone”. *Radio Romania, Iasi*. https://www.radioiasi.ro/stiri/national/s-a-dublat-numarul-localitatilor-care-primesc-mesaje-ro-alert-cu-privire-la-pericolul-de-cadere-a-unor-bucati-de-drone/.

Echevarria, Antulio J. 2017. *Military Strategy: A Very Short Introduction*. II. Oxford University Press.

EEAS. 2025. *EU Assistance to Ukraine (in U.S. Dollars)*. 11 December. Accessed January 28, 2026. https://www.eeas.europa.eu/delegations/united-states-america/eu-assistance-ukraine-us-dollars_en?s=253.

_____. n.d. *EUvsDisinfo*. https://euvsdisinfo.eu/articles/.

Ehl, David. 2025. “Ukraine: Which territorial concessions are under debate?” *DW*. https://www.dw.com/en/russia-ukraine-war-which-possible-territorial-concessions-are-under-debate/a-73630386.

EU. 2022. *A Strategic Compass for Security and Defence*. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

EU Council. 2022. *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*. 2 March. Accessed March 20, 2024. https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/.

EU. n.d. *EU support for Ukraine*. Accessed January 28, 2026. https://european-union.europa.eu/priorities-and-actions/eu-support-ukraine_en.

EURLex. 2026. “Regulation (EU) 2026/261 of the EP and of the Council of 26 January 2026 on phasing out Russian natural gas imports and preparing the phase-out of Russian oil imports, improving monitoring of potential energy dependencies and amending Reg. (EU) 2017/1938.” *EURLex*. 26 January. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202600261.

Euronews. 2025. “Oficial ucrainean: România mi-a cerut să tac în legătură cu dronele care ajung la ei”. *Euronews*. https://www.euronews.ro/articole/oficial-ucrainean-romania-mi-a-cerut-sa-tac-despre-dronele-care-ajung-la-ei.

European Commission. 2026. *REPowerEU – phase out of Russian energy imports*. Directorate-General for Energy. February. https://energy.ec.europa.eu/strategy/repowereu-phase-out-russian-energy-imports_en.

_____. 2020. “The EU’s Cybersecurity Strategy for the Digital Decade”. https://digital-strategy.ec. europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

Financial Times. 2024. *Russia could attack a Nato country within 3 to 5 years, Denmark warns*. Edited by Richard Milne. 9 February. https://www.ft.com/content/b3101099-9516-4b0b-92c6-179997d7e4cf.

France24. 2025. *Banned Russian media sites 'still accessible' across EU: report*. Edited by AFP. 05 08. https://www.france24.com/en/live-news/20250805-banned-russian-media-sites-still-accessible-across-eu-report.

Gaber, Yevgeniya. 2024. “A New Security Reality. Strategic Approaches for the Wider Black Sea Region”. *The Clock Tower Security Series* (George C. Marshall European Center for Security Studies (GCMC)). https://www.marshallcenter.org/en/publications/clock-tower-series/new-security-reality-strategic-approaches-wider-black-sea-region/new-security-reality-strategic-approaches-wider.

Gardner, Frank, and Tessa Wong. 2025. “Russia may attack Nato in next four years, German defence chief warns.” *BBC*. https://www.bbc.com/news/articles/c62v63gl8rvo.

George, Alexander L. 1991. *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*. Washington, DC: United States Institute of Peace Press.

Global Times. 2026. “Zelensky says US wants a Russia-Ukraine peace deal 'by June'; hasty pressure is not beneficial for talks as territory remains main obstacle: Chinese expert.” *Global Times China*. Accessed February 8, 2026. https://www.globaltimes.cn/page/202602/1355006.shtml.

Gray, Colin S. 1999. *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*. London: Routledge.

Grigorescu, Alexandru. 2026. “Motorina standard, tot mai aproape de pragul de 9,5 lei după a zecea scumpire de la începerea războiului.” https://economedia.ro/motorina-standard-tot-mai-aproape-de-pragul-de-95-lei-dupa-a-zecea-scumpire-de-la-inceperea-razboiului-creste-si-pretul-benzinei-standard.html.

Gutterman, Ivan, Kristyna Foltynova, and Mahir Sijamija. 2025. “Who Spends More on Ukraine Aid: The US or EU?” *Radio Free Europe, Radio Liberty (RFE/RL)*, 05 March. Accessed February 2, 2026. https://www.rferl.org/a/ukraine-us-russia-aid/33337524.html.

Hoffman, F.G. 2009. “Hybrid Warfare and Challenges.” *Joint Force Quarterly*.

Hung, Tzu-Chieh, and Tzu-Wei Hung. 2022. "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars." *Journal of Global Security Studies* 7 (4): Figure no. 1. doi:10.1093/jogss/ogac016.

Hutchinson, Andrew. 2022. "Russia's Invasion of Ukraine Represents a New, Key Stage in the Battle Against Online Misinformation." *Social Media Today*. 06 March. https://www.socialmediatoday.com/news/russias-invasion-of-ukraine-represents-a-new-key-stage-in-the-battle-agai/619899/.

Huth, Paul K. 1988. "Extended Deterrence and the Outbreak of War." *American Political Science Review* (Cambridge University Press) 82 (2). https://ideas.repec.org/a/cup/apsrev/v82y1988i02p423-443_08.html.

Jervis, Robert. 1989. *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*. Ithaca: Cornell University Press.

_____.. 1989. *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*. Ithaca: Cornell University Press.

Kakissis, Joanna, and Leila Fadel. 2025. "Russia accuses Ukraine of attempted drone strike, threatens to harden peace stance." *NPR*. https://www.npr.org/2025/12/30/nx-s1-5660691/russia-accuses-ukraine-of-attempted-drone-strike-threatens-to-harden-peace-stance.

Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton University Press.

Kiel Institut. 2025. *Ukraine support after 3 years of war: Aid flows remain low but steady - Shift towards weapons procurement*. 14 February. Accessed February 2, 2026. https://www.kielinstitut.de/publications/news/ukraine-support-after-3-years-of-war-aid-flows-remain-low-but-steady-shift-towards-weapons-procurement/.

Lanoszka, Alexander. 2016. "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe 1944-) 92, no. 1 (2016): 175-95." *International Affairs*, 175-195. http://www.jstor.org/stable/24757841.

Le Monde with AFP. 2025. "EU approves €93 billion in counter-tariffs on US goods." *Le Monde*. Accessed February 6, 2026. https://www.lemonde.fr/en/europe/article/2025/07/24/eu-approves-93-billion-in-counter-tariffs-on-us-goods_6743677_143.html#.

Lederer, Edith M. 2026. "US accuses Russia of 'dangerous and inexplicable escalation' of war in Ukraine as Trump seeks peace". https://www.aol.com/articles/us-accuses-russia-dangerous-inexplicable-001621207.html.

Lică, Daniela. 2024. „Dezinformarea în contextul a doi ani de război în Ucraina." *Colocviu strategic*, martie: 20-26. https://cssas.unap.ro/ro/pdf_publicatii/cs02-24.pdf.

Liptak, Kevin. 2025. "Trump gets a big win on NATO — but key questions over the alliance remain." *CNN*. Accessed February 6, 2026. https://edition.cnn.com/2025/06/25/politics/nato-meeting-trump-defense-spending.

Lunday, Chris, Jake Traylor, and Laura Kayali. 2025. "Trump casts doubt on Article 5 commitment en route to NATO summit." *Politico*. Accessed February 6, 2026. https://www.politico.eu/article/donald-trump-nato-summit-sidesteps-article-5-mark-rutte-eu-defense-budget-russia-vladimir-putin-iran-israel-strikes-qatar/.

Mazarr, Michael J. 2015. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. United States Army War College Press.

McCusker, Elaine. 2024. "The Price of Russian Victory." *Foreign Affairs*. Accessed February 4, 2026. https://www.foreignaffairs.com/ukraine/ukraine-aid-price-russian-victory-putin-elaine-mccusker.

Mearsheimer, John J. 2014. *The Tragedy of Great Power Politics*. Updated edition. New York: W. W. Norton & Company.

Mearsheimer, John. 2001. *The Tragedy of Great Power Politics*. W.W. Norton & Company.

Ministry of National Defence of Romania. 2021. *Military Strategy of Romania*. https://www.mapn.ro/legislatie/documente/STRATEGIA-MILITARA-A-ROMANIEI-ENG.pdf.

NATO. 2023. *Defence Expenditure of NATO Countries (2014-2023)*. https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2024/3/pdf/240314-def-exp-2023-en.pdf.

NATO. 2012. *Deterrence and Defence Posture Review*. 20 May. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2012/05/20/deterrence-and-defence-posture-review.

_____.. 2023. "Joint Declaration on EU-NATO Cooperation." 10 January. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/01/10/joint-declaration-on-eu-nato-cooperation.

—. 2026. *NATO's support for Ukraine*. Accessed January 28, 2026. https://www.nato.int/en/what-we-do/partnerships-and-cooperation/natos-support-for-ukraine.

NATO SG. 2024. *Remarks by NATO Secretary General Jens Stoltenberg and the General Manager of the NATO Support and Procurement Agency, Stacy Cummings at the signing ceremony for a major new investment in artillery ammunition*. 23 January. https://www.nato.int/cps/en/natohq/opinions_222003.htm.

NATO. 2022. *Strategic Concept*. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf.

NATO. 2025. *The Hague Summit Declaration*. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration.

Niemi, Seppo. 2026. *IR Theory / Alliance formation / Responding to threats*. https://greatpowerrelations.com/ir-theory-and-great-powers/alliance-formation/responding-to-threats/.

Observator. 2024. "'"Populaţia României trebuie să se îngrijoreze". Avertismentul şefului Statului Major care dă fiori: cât de pregătită e Armata pentru un eventual atac rusesc." Accessed February 5, 2026. https://observatornews.ro/eveniment/populatia-romaniei-trebuie-sa-se-ingrijoreze-avertismentul-sefului-statului-major-care-da-fiori-cat-de-pregatita-e-armata-pentru-un-eventual-atac-rusesc-561113.html.

Olteanu, Irina. 2025. "Russian victory would cost Europe twice as much as supporting Ukraine, study finds". Accessed February 4, 2026. https://spotmedia.ro/en/news/news/russian-victory-would-cost-europe-twice-as-much-as-supporting-ukraine-study-finds.

Pape, Robert A. 1996. *Bombing to Win: Air Power and Coercion in War*. Ithaca: Cornell University Press.

Pocheptsov, Georgii. 2018. "Cognitive Attacks in Russian Hybrid Warfare." *Information & Security: An International Journal*, 37-43. https://it4sec.org/system/files/4103_pocheptsov_cognitive_attacks.pdf.

President of the Russian Federation. 2022. *Maritime Doctrine of the Russian Federation*. http://en.kremlin.ru/events/president/news/69084.

President of the Russian Federation. 2021. "Strategy of the National Security of the Russian Federation". *Rusmilsec*. https://rusmilsec.blog/wp-content/uploads/2021/08/nss_rf_2021_eng_.pdf.

Reuters. 2024. "Putin issues nuclear warning to the West over strikes on Russia from Ukraine." *CNN*. https://edition.cnn.com/2024/09/25/europe/putin-nuclear-warns-west-missile-strikes-ukraine-intl-latam/.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." 35 (1): 5–32. doi:10.1080/01402390.2011.608939.

Romanian Presidency. 2025. *Strategia Națională de Apărare a Țării pentru Perioada 2025-2030*. 26 November. https://www.presidency.ro/ro/media/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2025-2030.

Schelling, Thomas C. 1966. *Arms and Influence*. New Haven: Yale University Press.

Smit, Sven et al. 2022. *War in Ukraine: Lives and livelihoods, lost and disrupted*. McKinsey & Company. Accessed February 4, 2026. https://www.mckinsey.com/~/media/mckinsey/business%20functions/strategy%20and%20corporate%20finance/our%20insights/war%20in%20ukraine%20lives%20and%20livelihoods%20lost%20and%20disrupted/war-in-ukraine-lives-and-livelihoods-lost-and-disrupted_vf.pdf...

Snyder, Glenn Herald. 1997. *Alliance politics*. Cornell University Press.

Starinac, Milica, and Alexandra Bostenaru. 2025. *Russian Drone Incursions in Poland and Romania*. Bloomsbury Intelligence & Security Institute. 18 September. https://bisi.org.uk/reports/russian-drone-incursions-in-poland-and-romania.

Statista. n.d. *Aid to Ukraine.* Accessed February 3, 2026. https://www.statista.com/search/?q=aid+to+ukraine&Search=&p=1.

The White House. 2025. *National Security Strategy of the United States of America*. November. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.

Tzu, Sun. 2005. *The Art of War.* 2005 by Harper Press.

Walldorf, Charles. 2026. "Trump's war against Iran is uniquely unpopular among US military actions of the past century." *The Conversation*. https://theconversation.com/trumps-war-against-iran-is-uniquely-unpopular-among-us-military-actions-of-the-past-century-277586.

Walt, Stephen M. 2010. *Balancing Threat: The United States and the Middle East* https://www.yalejournal.org/publications/balancing-threat-the-united-states-and-the-middle-east.

Walt, Stephen. 1987. *The Origins of Alliances*. Cornell University Press.

Waltz, Kenneth N. 1979. *Theory of International Politics*. Addison-Wesley Publishing Company .

WION. 2025. *Lie, pure nonsense': Putin slams NATO chief's 'prepare for a war' remark, says Russia is not threat for Europe.* Edited by Gulshan Parveen. New Delhi, 17 December. Accessed January 28, 2026. https://www.wionews.com/world/-lie-pure-nonsense-putin-slams-nato-chief-s-prepare-for-a-war-remarks-says-russia-is-not-threat-for-europe-1765985005838.

DOI: 10.53477/3045-2309-26-10

ROMANIA'S NATIONAL SECURITY BETWEEN THE STRATEGIC PARTNERSHIP WITH THE USA AND THE EU STRATEGIC AGENDA

Sînziana IANCU, PhD,
Major, Expert, Euro-Atlantic Resilience Centre (E-ARC), Bucharest, Romania
E-mail address: iancu_sanziana@yahoo.com

Abstract*: The paper analyses how Romania's national security is influenced by the Strategic Partnership with the United States of America and the European Union's Strategic Agenda for the 2024-2029 period. In an international context marked by insecurity and accelerated geopolitical shifts, Romania holds a key position on the eastern border of the Euro-Atlantic space. The study explores the main directions of bilateral and multilateral cooperation, the points of convergence and divergence between the two strategic frameworks, as well as the future courses of action for the Romanian state. The conclusion highlights the need for a coherent strategy capable of leveraging the complementarity of these two main pillars of national security.*

Keywords*: conflict; Ukraine; Russian Federation; EU Agenda; U.S. Strategic Partnership.*

Introduction

National security represents a fundamental concept for the existence and sovereignty of any state, defining its capacity to protect essential values, institutions, population, and territory against internal and external threats. For Romania, positioned at the intersection of major geostrategic interests in the Black Sea region, national security acquires complex dimensions, being influenced by both internal developments and international dynamics.

In this context, the Strategic Partnership with the United States of America and membership in the European Union represent two essential pillars of Romania's foreign and security policy. This paper examines the interaction between these two dimensions during the 2024-2029 period, highlighting the points of convergence as well as the challenges of maintaining an effective strategic balance.

The strategic relevance of Romania within the Euro-Atlantic and European frameworks has grown significantly in recent years. The consolidation of the Strategic Partnership with the United States - formally established in 1997 and reinforced through continued military, political, and technological cooperation - has positioned Romania as a frontline NATO member and a regional pillar of stability. American military presence on Romanian soil, including key assets, such as the Aegis Ashore missile defence system at Deveselu and the Mihail Kogălniceanu Air Base, reflects the critical role Romania plays in ensuring security along NATO's eastern flank. Beyond defence, the U.S.-Romanian partnership extends to cybersecurity, justice, energy diversification, and joint efforts in combating organised and transnational crime.

Simultaneously, Romania's 2007 integration into the European Union continues to shape its security and strategic outlook. The EU's Strategic Agenda for 2024-2029 outlines an ambitious vision for a more resilient, autonomous, and capable Europe, structured around three key priorities: a free and democratic Europe, a strong and secure Europe, and a prosperous and competitive Europe. Romania's active involvement in EU defence initiatives – such as SAFE, PESCO, the European Defense Fund, and CSDP operations - highlights its commitment to a common European security

framework. At the same time, EU policies on societal resilience, digital sovereignty, green transition, and strategic autonomy offer Romania both challenges and valuable opportunities to adapt its internal structures and policies.

While the United States and the European Union share many strategic objectives, their priorities and methods sometimes diverge, particularly in areas such as global competition with China, energy policies, and approaches to conflict resolution. For Romania, this dual alignment presents both a strategic challenge and a diplomatic balancing opportunity. Navigating between transatlantic commitments and European integration requires a flexible, proactive, and coherent foreign policy capable of harmonising overlapping but occasionally competing agendas.

In a global context marked by rising instability, the war in Ukraine, evolving threats in cyberspace, and intensifying geopolitical competition, Romania must consolidate its strategic posture. This includes strengthening its national defence, modernising its military and technological capacities, reinforcing internal societal resilience, and contributing constructively to both NATO and EU efforts in regional and global security. Positioned as both a beneficiary and a potential provider of stability in the Black Sea region, Romania's ability to effectively leverage its strategic partnerships will be a determining factor in safeguarding its national security throughout the 2024–2029 period and beyond.

1. The strategic partnership between Romania and the U.S.

The Strategic Partnership between Romania and the United States, officially launched on July 11, 1997, during the visit of U.S. President William (Bill) J. Clinton to Bucharest, has significantly strengthened over the past decades, becoming a central element of Romania's foreign and national security policy. It focuses on cooperation in key areas such as defence, cybersecurity, energy, and the rule of law (U.S. Department of State, 2025). Romania builds its security strategy on the premise that its main security guarantees stem from its NATO membership and the privileged relationship it holds with the United States - a partner that shares its perception of the threat level along the eastern flank of the Alliance (MFA, 2025).

According to Romania's National Defense Strategy for the 2025-2030 period, the Strategic Partnership with the United States continues to represent a core pillar of Romania's foreign and security policy, underpinning its role within NATO and complementing its engagement in the European Union.

A fundamental pillar of this partnership is the military component. The presence of U.S. troops on Romanian territory, the development of facilities at the Mihail Kogălniceanu Air Base, and the deployment of the U.S. ballistic missile defence system, "Aegis Ashore", at the Deveselu Military Base[1] underscore Romania's strategic importance in the security architecture of NATO's eastern flank. The Aegis Ashore site in Romania achieved operational certification in May 2016 (US Congress, 2025). Romania's constant participation in joint NATO military exercises fosters interoperability and enhances rapid response capabilities in the face of potential conventional or hybrid threats. Furthermore, the signing of the "Access Agreement" (MFA, 2025) regarding United States armed forces activities stationed on Romanian territory, on December 6, 2005 (which entered into force on July 21, 2006), as well as Romania's military involvement in theaters of operations in Afghanistan and Iraq in support of the United States-led international coalition against terrorism, have constituted major coordinates in the bilateral relations established between Romania and the United States. In addition, Romania's role within United States Operation ***Atlantic Resolve*** has further consolidated the military dimension of the Strategic Partnership. Launched in 2014 in response to the deteriorating security environment in Eastern Europe, *Atlantic Resolve* aims to demonstrate sustained the United States commitment to NATO's collective defence and to enhance deterrence on the Alliance's Eastern flank. Through rotational deployments of United States' forces, pre-positioning of

[1] The signing, on September 13, 2011, of the "Agreement between Romania and the United States of America on the Deployment of the United States Ballistic Missile Defense System in Romania".

equipment and an intensified tempo of joint training and exercises hosted on Romanian territory, the operation has significantly contributed to strengthening allied interoperability, readiness and forward defence posture in the Black Sea region. Romania's consistent participation in and support for *Atlantic Resolve* initiatives underscores its status as a key security provider and a reliable ally in the Euro-Atlantic security architecture.

Beyond the military dimension, bilateral cooperation also includes areas such as economic security, collaboration in internal affairs and justice, energy security (projects on diversifying energy sources, including small modular reactors), combating cyber threats, and promoting good governance in the spirit of shared security and prosperity[2]. The United States has supported Romania's efforts to strengthen digital resilience and protect critical infrastructure.

Additionally, cooperation in intelligence sharing and coordination between law enforcement institutions contributes to combating terrorism, human trafficking and other forms of transnational crime. Recent provisions outlined in the United States National Security Strategy 2025 reaffirm Europe's centrality to the United States strategic interests, emphasising deterrence, forward defence and the strengthening of allied burden-sharing in response to persistent Russian revisionism. While the document signals a growing expectation that European allies assume greater responsibility for their own security, it does not indicate a strategic disengagement from the continent. Nevertheless, a hypothetical total withdrawal of the United States' forces from Romanian territory would represent a major strategic rupture, significantly weakening deterrence on NATO's southeastern flank, increasing Romania's exposure to conventional and hybrid threats in the Black Sea region and placing substantial additional pressure on both national defence capabilities and the European pillar of NATO. Such a scenario would fundamentally alter Romania's security calculus and underscore the irreplaceable role of the United States' military presence in the current regional balance of power.

2. The EU Strategic Agenda 2024-2029

The European Union's Strategic Agenda for the 2024-2029 period reflects the commitment of the 27 member states to strengthen the Union's resilience in an international context marked by instability, geopolitical competition, climate crises, and accelerated technological advancement. Adopted at a time of major geopolitical shifts - including the ongoing war in Ukraine, the rise of authoritarian regimes, and the challenges posed by emerging technologies - the Agenda is structured around three key pillars: *A Free and Democratic Europe, A Strong and Secure Europe, and A Prosperous and Competitive Europe*. These encompass priorities such as protecting citizens and European values, developing a competitive European economy, achieving the green and digital transitions, and promoting the EU's interests and values on the global stage (European Council, EU Council, 2024).

A Free and Democratic Europe sets the following objectives (European Council, EU Council, 2024): * promoting and protecting the rule of law[3]; * safeguarding online debates; * strengthening resilience and democratic discourse; * combating foreign interference and destabilisation efforts; * supporting the UN Charter and a global framework for peace, justice, and security.

A Strong and Secure Europe outlines priorities such as (European Council, EU Council, 2024): * continuing support for Ukraine, including in its reconstruction efforts and in securing a just and lasting peace; * preparing the EU for defence through increased defence spending and investment; * Maintaining strong relationships with transatlantic partners and NATO; * Taking necessary measures

[2] Aspects stipulated within The National Defense Strategy for the 2020–2024 period, which was approved by Decision No. 22 of the Joint Session of the Senate and the Chamber of Deputies on June 30, 2020 and was published in the Official Gazette, Part I, No. 574 of July 1, 2020 (Administrația prezidențială / The Romanian presidential administration, 2025).
[3] Within the EU, the rule of law, just as in Romania's Strategic Partnership with the United States, plays an essential role. It derives from the treaties signed by the member states, which include both the objectives and priorities of the EU and the activities of EU institutions that have the authority to create legislation, which the member states are then required to implement.

for prevention, response, and resilience in the face of crises, natural or man-made disasters, or health emergencies; * Combating organised crime, radicalisation, terrorism, and violent extremism; * managing borders and migration; * supporting the continuation of EU enlargement alongside internal reforms.

A Prosperous and Competitive Europe prioritises actions such as (European Council, EU Council, 2024): * collective investments from both public and private sectors, including through the European Investment Bank; * investments in skills, training, and education; * an integrated single market for energy, finance, and telecommunications; * development of key technologies such as artificial intelligence, net-zero emission technologies, and semiconductors; * reducing harmful dependencies and strengthening supply chains; * advancing the green and digital transitions; * reforming the agricultural system; * enhancing cooperation in public health at both European and international levels.

In the field of security, the European Union aims to become a more capable and autonomous actor, especially through the strengthening of the Common Security and Defense Policy (CSDP). Initiatives such as PESCO (Permanent Structured Cooperation), BUS (Brussels-based Union Security), and the European Defense Fund are intended to stimulate defence cooperation among member states and reduce fragmentation in the European defence market (European External Action Service, 2024). Strategic autonomy does not imply a break from NATO, but rather an enhancement of Europe's capacity to act independently in its immediate neighborhood or in support of the transatlantic alliance.

For Romania, active participation in these structures represents both an opportunity to modernise its armed forces and national defence industry, and a political tool to influence the shaping of European security policies. As an active member involved in PESCO projects, Romania participates in initiatives concerning military mobility, the development of cyber defence and the training of military personnel. Furthermore, Romania benefits from financial support through the European Defense Fund to modernise its defence industry and to increase its own capabilities (European Defence Cooperation, 2025). In addition, Romania's engagement with initiatives developed under the SAFE (Security Action for Europe) framework further supports its efforts to strengthen defence capabilities by facilitating joint procurement, enhancing defence-industrial cooperation and improving access to financing for priority capability gaps. Participation in SAFE-related projects complements Romania's involvement in PESCO and the European Defense Fund, reinforcing military mobility, resilience and the sustainability of national and allied force structures within the broader European security architecture.

Beyond strictly military aspects, the EU Strategic Agenda for 2024-2029 emphasises the importance of broad societal resilience across European communities. This includes strengthening energy security, combating disinformation, protecting critical infrastructure, and developing digital autonomy. In all these areas, Romania benefits from financial and technological support but also bears the responsibility to adapt its domestic policies in order to fully leverage these resources. Thus, the EU is shaping up not only as a source of economic and regulatory security but also as an increasingly active player in defence and collective security. As a member state, Romania must integrate effectively into this effort, balancing its interests between the transatlantic orientation and the building of a more strategically capable Europe.

3. Points of Convergence and Divergence

Romania's relations with the United States of America and the European Union in the field of security are not conflicting, but rather complementary. According to the scientific military literature, *The European Union is a unique and essential partner for NATO, shares the same values, and plays complementary, coherent, and mutually reinforcing roles in supporting international peace and security. NATO and the EU will enhance the strategic partnership, strengthen political consultations and increase cooperation on issues of common interest, including the military field. Developing coherent and mutually reinforcing capabilities, while avoiding unnecessary duplications, are the key to joint efforts to make the*

Euro-Atlantic area safer. - NATO Strategic Concept, June 29, 2022, pp. 1, 10 (CERNAT, 2011 p. 128). However, differences in approach, pace, or priorities may arise between the two strategic frameworks, making the management of this balance essential for Bucharest. Currently, the Trump administration's vision is shifting toward a conditional stance, namely: either ending the conflict between Ukraine and the Russian Federation, or distancing the United States from the conflict in all aspects - diplomatic, logistical, etc. This approach stems from the fact that one of the new president's key objectives within his first 100 days in office is to end the Russia–Ukraine war, under the diplomatic direction of the U.S. administration. If this objective were to fail, it could signal the end of the era in which the United States positioned itself as the guarantor of international security. In such a scenario, Romania would find itself caught between the Strategic Partnership with the U.S. and the EU's foreign policy goals, which include continued support for Ukraine - aimed at securing a peace aligned with Ukraine's current national interests, including the preservation of its full territory (namely, Kherson, Zaporizhzhia, Donetsk, Luhansk, and Crimea).

3.1. Convergences

Both the U.S. and the EU regard the stability of the Black Sea region as a strategic objective. In this regard, Romania benefits from direct military support from the United States through the presence of U.S. troops and NATO infrastructure, while the EU invests in economic development, civil infrastructure, and regional resilience. Both entities support the modernisation of the Romanian army, the fight against hybrid threats, the protection of critical infrastructure, and the development of a national defence industry.

In the fields of cybersecurity and countering disinformation, Romania collaborates with the U.S. through bilateral and multilateral initiatives (e.g., within NATO), and also participates in EU rapid alert and response mechanisms in the event of cyberattacks or hostile influence campaigns. Romania also benefits from European expertise and funding to enhance its digital infrastructure and response capacities.

Another point of convergence is the shared support for Ukraine and the efforts to curb Russian influence in the region. Romania serves as a bridge between these two agendas, actively contributing humanitarian, economic, and military assistance to Kyiv.

3.2. Divergences

Nonetheless, divergences may emerge between the U.S. and the EU in terms of how strategic crises or priorities are addressed. For instance, while the U.S. maintains a global strategy focused on strategic competition with China and preserving its influence in the Indo-Pacific, the EU places greater emphasis on internal resilience, technological sovereignty, and strategic autonomy from all external actors, including, in certain respects, from the U.S. itself.

In this context, Romania may feel the pressure of aligning its defence and security policies with two centers of power that, although allied, do not always share the same priorities. For example, in military procurement or technological standardisation, Romania must navigate between American and European requirements.

Furthermore, European projects regarding green taxonomy, the energy transition, and digital regulations may sometimes clash with the more flexible U.S. approach in these areas. Here, Romania must adopt a pragmatic stance, capitalising on economic support from both directions without jeopardising its strategic relationships.

Managing these points of convergence and divergence requires an active, well-calibrated, and coherent foreign policy. Romania must strengthen its capacity to act as a mediator and integrator of Western interests in the region while maintaining a clear strategic vision of its own national interests.

4. Analysis and Perspectives for Romania

Between 2024 and 2029, Romania stands at a geopolitical turning point, where national security depends directly on the country's ability to simultaneously capitalise on transatlantic support and European integration. In recent years, Romania has emerged as a critical component of NATO's defence strategy in Eastern Europe, reflecting the shifting dynamics of global security and regional geopolitics (China CEE, 2024). Amid intensifying global strategic competition and emerging threats, ranging from conventional and hybrid warfare to cyberattacks and regional instability, Romania must adopt a coherent, proactive, and adaptable strategic approach.

Romania's geostrategic position presents both advantages and vulnerabilities. Located on the eastern border of NATO and the EU, Romania is both a frontier state of Western democracy and a security bastion for the entire Black Sea region. This position provides strategic benefits - such as access to vital resources and Western military and economic support - but also exposes the country to direct risks from the East. Therefore, Romania must continue investing in defence infrastructure, cybersecurity, and border protection.

Against the backdrop of the war in Ukraine and instability in the Republic of Moldova and the Western Balkans, Romania has the opportunity to become a regional security actor, promoting stability, democracy, and regional cooperation. Active involvement in Ukraine's reconstruction, support for the European path of the Republic of Moldova, and strengthening trilateral cooperation between Romania, Poland, and Ukraine can contribute to this strategic positioning.

Romania is also expected to consolidate its role within European integration and strategic partnerships - both with the United States and other European allies - by pursuing objectives such as: updating its National Defense Strategy to reflect post-2024 realities and aligning it with the new NATO and EU strategies; increasing investments in defence and military innovation in line with NATO commitments; strengthening internal resilience through integrated public policies on security education, countering disinformation, and protecting critical infrastructure; and continuously promoting a balanced and coherent diplomacy, capable of mediating and harmonising transatlantic and European interests.

Conclusions

Between 2024 and 2029, Romania's national security will increasingly be defined by the state's ability to efficiently navigate between the two poles of Western strategic support: the Strategic Partnership with the United States of America and the European Union's Strategic Agenda. For now, these two frameworks are not antagonistic, but complementary - each providing essential tools, resources, and mechanisms for defending national interests.

The strategic partnership with the United States remains the fundamental military security guarantee, offering vital operational, technological and political support for the defence of national territory and the projection of stability in the Black Sea region. At the same time, active membership in the European Union and integration into common defence and security policies open new opportunities for the modernisation of the armed forces, the development of the defence industry and the strengthening of internal resilience.

In this context, Romania's participation in the SAFE program represents a pragmatic mechanism for partially compensating structural capability gaps through joint procurement, industrial cooperation, and improved access to European financing, thereby strengthening national and allied defence readiness. However, a potential downsizing of the United States forces along NATO's Eastern European border, particularly within the framework of Operation Atlantic Resolve, would have significant strategic implications. Such a development would place increased pressure on European-led defence initiatives and national force generation, while amplifying Romania's responsibility to accelerate defence modernisation, enhance resilience and deepen its role as a security provider in the

Black Sea region. In this evolving strategic landscape, SAFE-type instruments can mitigate, but not fully substitute the deterrent and reassurance effect generated by the United States' military presence.

Romania must leverage this dual strategic anchoring through a balanced foreign policy, by consolidating its national defence capabilities and actively participating in regional and global initiatives aimed at ensuring stability and peace. The balance between transatlantic and European commitments does not mean choosing between two options, but rather synergistically utilising the advantages offered by both.

In conclusion, Romania's national security in the coming years will depend on the strategic coherence of internal and external political action, commitment to Western democratic values and the ability to build durable alliances in a profoundly uncertain international environment. Through a clear and strategic approach, Romania can become not only a beneficiary, but also a provider of security in the Euro-Atlantic space.

BIBLIOGRAPHY:

Administrația Prezidențială/The Romanian Presidential Administration. 2020. „Strategia Naţională de Apărare a Țării pentru perioada 2020-2024" available at https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf. Accessed: May 1, 2025.

Cernat R. 2011. "Considerations on the EU and NATO security responsibilities", p. 128, în Revista "Romanian Military Thinking" (Journal of Military Science and Security Studies published by the Defence Staff) available at https://en-gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20reviste/RMT/2022/3/RMT_3__2022.pdf. Accessed: April 28, 2025.

China CEE. October, 2024. „Romania Political Briefing: Romania's Strategic Role in European Security, Romania's Strategic Role in European Security: Historical Foundations and Contemporary Relevance" available at https://china-cee.eu/2024/12/31/romania-political-briefing-romanias-strategic-role-in-european-security-historical-foundations-and-contemporary-relevance/. Accessed: April 28, 2025.

Consiliul European, Consiliul UE/European Council, EU Council. 2024. "Agenda Strategică 2024–2029", available at https://www.consilium.europa.eu/ro/european-council/strategic-agenda-2024-2029/ and https://www.consilium.europa.eu/ro/european-council/strategic-agenda-2024-2029/#democratic. Accessed: May 1, 2025.

European Defence Cooperation. 2025. "Permanent Structured Cooperation (PESCO)", available at https://eda.europa.eu/what-we-do/EU-defence-initiatives/permanent-structured-cooperation-(PESCO). Accessed: April 29, 2025.

European External Action Service. The Diplomatic Service of the European Union. 2024. "A Strategic Compass for Security and Defence", available at https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en. Accessed: April 30, 2025.

MAE / MFA. January 2025. "Parteneriatul strategic România – SUA" available at https://www.mae.ro/node/4944. Accessed: May 1, 2025.

US Congress. March 28, 2025. "Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress", available at https://www.congress.gov/crs-product/RL33745. Accessed: May 1, 2025.

US Department of State. January 20, 2025. "U.S. Security Cooperation with Romania" available at https://www.state.gov/u-s-security-cooperation-with-romania/. Accessed: May 1, 2025.

DOI: 10.53477/3045-2309-26-11

VOLUNTARY RESERVE AS AN INSTRUMENT FOR SOCIAL COHESION AND EXTENDED NATIONAL RESILIENCE IN THE BLACK SEA REGION

Elena-Adriana BRUMARU,
PhD Student, Military Academy "Alexandru cel Bun", Chișinău, Republica Moldova.
E-mail address: brumaru_adriana@yahoo.com

Abstract*: In the contemporary security environment of the Black Sea region, characterised by extreme volatility, hybrid warfare and the persistent threat of a high-intensity conflict, the traditional paradigms of national defence are undergoing a fundamental transformation. As the Euro-Atlantic community navigates the complex geopolitical landscape of 2026, the concept of resilience has gone beyond military reinforcement to adopt a comprehensive "Whole-of-Society" approach. This article provides an exhaustive analysis of the voluntary reserve as an essential tool for promoting social cohesion and improving Extended National Resilience capabilities. Anchored in the legislative progress of Law no. 5/2026 of Romania and aligned with the strategic imperatives of NATO's policy MC 0441/3 and the European Union Strategy for Preparedness, the research argues that a modernised voluntary reserve serves as a critical link between the armed forces and the civilian population. Through a multidimensional examination of threat vectors - from cognitive subversion to critical infrastructure sabotage - and a comparative analysis of reserve models in Ukraine, Turkey, and Bulgaria, this report demonstrates that voluntary reserve is not just a force multiplier for combat operations, but a strategic necessity for democratic stability. By transforming citizens from passive consumers of security into active producers of defence, the voluntary reserve mitigates the vulnerabilities of societal polarisation and infrastructural fragility, thereby strengthening the "Extended National Resilience" (also known in NATO terminology as "multi-layered resilience") needed to withstand the systemic shocks of the 21st century.*

Keywords*: Voluntary Reserve; Social cohesion; Civil Defence; Black Sea Security; Resilience; Law 5/2026; Hybrid Warfare; The whole society; NATO MC 0441/3.*

Introduction

The geopolitical architecture of the Black Sea region has evolved into a strategic melting pot, serving as the main fault line between Euro-Atlantic stability and revisionist aggression. As we move into 2026, the security environment is defined not only by the threat of a conventional confrontation, but also by a pervasive conflict, in several areas, in the "grey zone", which targets the cognitive, economic and infrastructural fabric of democratic societies.

Lessons identified from the protracted conflict in Ukraine and growing hybrid threats along the Pontic coastline have catalysed a doctrinal renaissance within NATO and the EU. It is important to note that a lesson is considered "learned" only when it is implemented into doctrine or operationalised into a specific capability. This renaissance recognises that national security can no longer be the exclusive remit of permanent professional armies. The magnitude of modern threats calls for a radical expansion of the defence paradigm toward "Extended National Resilience". The research methodology employed in this article involves the evaluation of available databases and information, followed by a multidimensional analysis of legislative influence on political and military

mentalities. A limitation of this research is the reliance on early-stage implementation data for Law 5/2026, which may evolve as the program matures.

In this context, the voluntary reserve becomes an indispensable strategic asset.

Reimagined as the essential bridge between the military establishment and civil society, the voluntary reserve provides surge capacity for national defence while acting as a mechanism for social cohesion. By integrating citizens with diverse expertise, the state effectively "deputizes" the resilience of the private sector to counter hybrid warfare. This analysis explores how these instruments operationalise the voluntary reserve as a pillar of Extended National Resilience in the 21st century.

1. Geostrategic imperative: Black Sea security environment in 2026

To understand the need for a robust voluntary reserve, we must first look at the threat landscape of 2026. The distinction between peace and war has eroded, as adversaries use all instruments of national power, including conventional and unconventional methods of struggle. Intelligence assessments from 2024-2025 indicate a four-fold increase in sabotage incidents targeting logistics hubs and energy networks across Europe.

The most insidious vector is information. Opponents use cognitive warfare to target the population's "will to resist". In this environment, an isolated army in the barracks is structurally disadvantaged. The voluntary reserve, composed of trusted community members, serves as a credible intermediary capable of dismantling disinformation at the local level. Furthermore, modern defence depends on privately owned infrastructure. NATO documents show that 90% of military transport depends on commercial assets. Protecting distributed assets, such as port facilities in Constanța, requires a ubiquitous security presence (CCDCOE 2025).

Regarding maritime insecurity and the "grey zone", the maritime domain remains disputed. Floating sea mines and electronic warfare continue to pose lethal threats to navigation and economic stability. A reserve with specialised maritime capabilities is essential for expanding maritime awareness without diverting high-value ships from deterrence missions. Euro-Atlantic doctrine has shifted to "Extended National Resilience", a proactive ability to anticipate and absorb shocks. This is aligned with NATO's Article 3 and the EU's "Preparedness Union". The voluntary reserve is the structural embodiment of this permeability, transforming resilience from rhetoric into a deployable capability.

2. Theoretical frameworks: social cohesion and civil-military relations

The voluntary reserve force is not just a ***labour*** buffer, but a sociological tool that renegotiates the social contract. In defining social cohesion in a security context, it is critical to recognise that social cohesion - trust and solidarity within a community - is a critical variable of national power. Research indicates that participation in collective action increases social trust (Journal of International Affairs 2025). Voluntary military service amplifies this; a voluntary reserve unit that brings together diverse professionals creates a microcosm of national unity ("emerging social cohesion") that transcends class divisions and strengthens resistance to subversion (Royal Society 2024).

The perspective of the reservist as "twice the citizen", a concept famously attributed to Winston Churchill, highlights their dual identity (Leatherneck 1968). Occupying a liminal space between military discipline and civilian expertise, the reservist acts as a binder between these worlds. This liaison function is vital for bridging the "civil-military gap", making defence visible in everyday life and reinforcing the principle that citizens are the ultimate guardians of freedom.

Acting as a *"whole-of-society"* interface, the voluntary reserve allows the military to access the *"cognitive surplus"* of the civilian sector - expertise in cyber, logistics, or the medical field - without the prohibitive costs of permanent retention (CIMIC COE 2024). This permeability ensures that the defence establishment can quickly integrate private sector innovations.

3. NATO and EU political landscape: The strategic engine

The revitalisation of reserves is driven by coordinated supranational frameworks that increase collective deterrence. NATO's new reserve policy (MC 0441/3), approved at the end of 2024, MC 0441/3 represents a paradigm shift, recognising reserves as a critical component of combat capability. Key principles include: Deterrence and Defence - Reserves provide the strategic depth needed for Article 5 operations; Social value - Explicitly links reserves to strengthening the military-population bond and Total Force Concept - Requires the seamless integration of active and spare components into the planning.

In the context of the Union Strategy for EU Preparedness, the EU strategy converges with NATO's Seven Core Requirements for National Resilience, particularly in managing casualties and ensuring resilient transport. Voluntary reserve units are uniquely positioned to respond locally to these requirements, ensuring that populations can sustain themselves for at least 72 hours during crises (European Commission 2025).

4. Legislative evolution in Romania: The impact of Law 5/2026

Apart from the existing Law No. 270/2015 for the Voluntary Reserve Corps, Romania has put these concepts into practice through Law No. 5/2026. Through the "Soldier/Volunteer Rank in Term" Program, the basic innovation is the newly established program in peacetime (Art. 13^1), targeting citizens aged 18 to 35.

- Structure: A fixed period of basic military training of up to four months, designed to minimise career disruption.
- Incentives: A completion bonus of three average national gross salaries acting as a strong economic "pull factor".
- Result: Graduates are automatically enrolled in the Operational Reserve, creating a young and dynamic group of trained citizens.

Furthermore, regarding mobilisation protocols and the diaspora, Law 5/2026 affirms extraterritorial influence. Article 8^1 provides that volunteer reservists temporarily abroad must report within 15 calendar days from notification during mobilisation. Although a logistical challenge, this reinforces the universality of the obligation to defend.

By redefining the reserve structure, the law divides the reserve into the Operational Reserve (highly trained volunteers) and the General Reserve (for mass mobilisation). This structure allows for scalable responses without the political cost of general mobilisation.

5. Voluntary reserve as a social instrument

The social impact of the voluntary reserve depends on its operational culture.

The social impact depends on operational culture. The "Volunteer Reservist Guide" adopts a modular training approach (Module 1 - Basic knowledge; Module 2 - Preparation and conduct of actions). This efficiency allows for the recognition of civilian abilities, maximising the usefulness of the "Whole-of-Society" approach. Volunteer reservists act as ambassadors, normalising military presence. By applying job protection (Art. 46 of Law 5/2026), the state aligns private sector interests with national security.

6. Regional benchmarking

Models of reserve forces in the Black Sea region (see Table no. 1) provide key lessons for operationalisation.

Table no. 1: Comparative analysis of reserve force models in the Black Sea region
Source: Adapted from comparative regional data (2026).

Feature	Ukraine (TDF)	Turkey (Yedek Subay)	Bulgaria (mixed)	Romania (Law 5/2026)
Structure	Regional Brigades; decentralised ordering.	Centralised; The "Reserve Officer" route for graduates.	Mixed volunteer/mobilisation; demographic difficulties.	Hybrid: "Soldier/Volunteer Rank in term" (4 months) + Contracted Reserve.
Recruitment	A high volunteering driven by existential threats.	On a recruitment basis; High social prestige.	Reduced number of volunteers; weak stimulant.	Incentive-based (3 salaries); targets young people (18-35).
Integration	Total: Units defend their own communities.	Disaster Response Integration (AFAD).	Limited; separate from civil society.	Increasing the synergy of the "whole-of-society" through a new law.
Key lesson	Location: The house defence is a force multiplier.	Scale: Mass is essential for disaster response.	Adaptability: Rigid systems fail; flexibility is key.	Stimulation: Economic realism is necessary in peacetime.

7. Operational scenarios: Reserve forces in action

To visualise the usefulness of the reserve forces in 2026, we analyse three scenarios:

- Hybrid infrastructure sabotage: Specialised IT reservists assist in restoring the system while operational units secure physical stations.
- Mass casualty response: Medical and logistics reservists manage triage within a military command framework (NATO Basic Requirement 5).
- Support for host nations: Reservists secure transit routes for the NATO Response Force, ensuring Allied mobility while minimising friction with the local population.

Conclusions

The trajectory of the Black Sea region indicates that challenges will be defined by ambiguity and hybridity. In this context, the voluntary reserve is a structural necessity. The introduction of Law 5/2026 marks a significant evolution over the previous Law 270/2015 on the Status of Voluntary Reservists, which faced limitations in attractiveness and mass mobilisation capacity. Law 5/2026 addresses these gaps by providing robust financial incentives and a younger, more agile Operational Reserve pool.

Critical conclusions include: Legislative agility - Incentives demonstrate that patriotism must be backed by economic reality; Social cohesion - Reserves are the engine of the "Whole-of-Society" approach, immunising society against cognitive warfare; Regional synchronisation - Resilience depends on interoperability and common training standards.

The voluntary reserve remains proof of the enduring power of the citizen-soldier, ensuring that society remains united and resilient in the face of all challenges.

BIBLIOGRAPHY:

Ioniță, Crăișor-Constantin and Elena-Adriana Brumaru. 2025. "The new NATO policy on reserves. A romanian project to implement it", in *Proceedings of The International Scientific Conference Strategies XXI - The Complex And Dynamic Nature Of The Security Environment*. 49-56. https://revista.unap.ro/index.php/XXI_CSSAS/article/view/2190/2135

The Romanian Parliament. 2026. Law no. 5 of January 9, 2026 amending and supplementing Law no. 446/2006 on the preparation of the population for defence. Published in the Official Gazette no. 10, January 9, 2026.

CCDCOE. 2025. "Maritime Port Cyber Security in the Black Sea". Policy briefing, July 2025.

CIMIC COE. 2024. "Seven basic requirements". CIMIC Handbook.

European Commission. 2025. "The new EU strategy for a safe, prosperous and resilient Black Sea region".

Journal of International Affairs. 2025. "Social Cohesion and Reserve Forces: A Systematic Review".

Leatherneck. 1968. "Twice the Citizen". March 1968 Issue.

NATO Public Diplomacy Division. 2024. "Resilience, Civilian Preparedness and Article 3".

Royal Society Interface. 2024. "Emerging social cohesion to cope with community disasters".

SECTION III
GLOBAL AND REGIONAL TRENDS

DOI: 10.53477/3045-2309-26-12

THE IMPACT OF AN ARMED CONFLICT ON CHILDREN

Marius Gabriel BOBOCEA,
Ministry of Foreign Affairs, Romania
E-mail address: marius.bobocea@mae.ro

Abstract**:** *The paper analyses the impact of armed conflicts, explicitly on children. Methodologically, the research is based on a qualitative case study approach, using documentary analysis of UN and UNHCR reports, resolutions and statements from international organisations, as well as the international and regional press information.*
The results of the analysis show the impact of an armed conflict on children, affecting their development and childhood. The paper shows the psychological consequences derived from the number of casualties and lack of provisions, such as medicine and food, and from the impact of displacement.

Keywords**:** *children; armed conflict; UN; HRMU; UNHCR.*

Prolegomena

Armed conflicts redefine maps, destroy cities and lives and rewrite the future of states and people. For millions of children around the world, war is not just a headline in the newspaper, but a daily reality, one in which safety becomes uncertain, routine dissolves and maturation accelerates under pressure. Childhood, meant to be a season of discovery, becomes a terrain of survival.

Recent wars and conflicts have led to significant increases in mental health problems such as post-traumatic stress disorder (PTSD), anxiety, and depression across societies. Exposure to conflict and terrorism has prompted significant investment in psychological support, as well as the development of social cohesion strategies designed to foster resilience among the population. National measures and international cooperation contribute to strengthening resilience, with the potential to mitigate the multigenerational effects of trauma (S. Iancu 2024, 76). Because, more frequent than not, societies that fail to sustain the affected children risk reproducing sequences of trauma, violence and fragility across generations. The vicious cycle weakens the capabilities to form a strong resilience toward conflicts and violent events. Key factors identified for resilience include trust in government and state institutions, patriotism, and social integration. However, resilience is significantly influenced by psychological factors as well as societies' ability to adapt and recover from traumatic events (S. Iancu 2024, 71). Moreover, national resilience is most affected and declines during war, on a large scale.

Contemporary armed conflicts, characterised by their multidimensional, transregional, and protracted nature, as well as by the emergence of new-armed actors and the use of emerging technologies, continue to seriously affect the protection of children in conflict zones. (UN 2025, 2). Although, primarily conducted by states, these attacks can also be carried out by terrorist organisations with the necessary resources (S. Iancu 2024, 63). Children are directly exposed to violence, forced displacement, psychological trauma and deterioration of the security environment, consequences that more often than not exceed the actual duration of hostilities. In this context, the weakening of civil protection mechanisms and social cohesion amplifies the vulnerability of children, especially in states affected by instability and various types of hybrid aggression. Such actions generate significant risks to regional security and stability, with direct implications for the respect of children's rights in armed conflicts and the contemporary international order. Similarly, the prolonged

duration of conflicts, the continuous emergence of new armed actors, and, above all, the use of new technologies has negatively affected strategies for protecting children in conflict situations.

The latest study published by the Special Representative of the UN Secretary-General indicates an alarming increase in cases of children exposed to and affected by armed conflict, by approximately 25% in 2024 compared to 2023. (UN 2025, 2). The report also shows that non-state armed groups were responsible for almost 50% of violations of children's rights, but government forces were the main perpetrators of killings and maiming of children, attacks on schools and hospitals, and denial of access to humanitarian aid (UN 2025, 2).

The study verified 41,370[1] serious human rights violations, including collective violations such as attacks on schools and hospitals and denial of access to humanitarian aid. According to the study, in 2024, 22,495 children were affected by recruitment and use in armed conflict, abduction, killing and maiming, rape and other forms of sexual violence (14,383 boys, 7,320 girls, 792 of unknown sex) (UN 2025, 2).

In this study, we will analyse reports from the UN and UNHCR (United Nations High Commissioner for Refugees) to highlight the impact that armed conflict has on children, the most vulnerable category of people. The study analyses the impact through several criteria, such as: * death and physical injury; * lack of access to healthcare; * lack of access to education; * loss of home and relocation to a refugee center (displacement); * loss of parents or close relatives. Last but not least, a section is also dedicated to children who are recruited by militias to actively participate in a conflict.

At the same time, in order to highlight the elements discussed in each subsection, examples will be presented from two ongoing armed conflicts, those in Sudan[2] and Gaza[3].

1. Children as direct victims of armed conflicts

In armed conflicts, even though weapons have evolved (from swords to bayonets, from bows to machineguns and from catapults to drones), striking military targets does not eliminate the existence of civilian collateral victims. Harm caused by armed conflicts can be ranged from *direct injuries* caused by weapons (shooting, shrapnel or splinters), to *indirect injuries* (landmines, unexploded ordnance and injuries from damaged buildings and roads).

The UN Human Rights Monitoring Mission in Ukraine (HRMU) confirmed that in 2025, more than 2,500 civilians were killed and 12,142 were injured. The total number of civilians killed and injured in 2025 was 31%, which was higher than in 2024 and much higher (70%) than in 2023 (OHCHR 2026).

In Sudan, reports indicate that over 10 million children have been exposed to fighting, bombing, mortar and rocket attacks, as well as to direct attacks on civilians, with no accurate statistics on the number of people that died (Aljazeera 2024).

In Gaza Strip, the latest data, published by the *Gaza Government Press Office*, disclosed that at least 20,000 children (*approximately 2% of the child population in Gaza*) were actually killed, between October 2023 and September 2025. (Save the Children 2025). Moreover, Israeli forces have intensified their bombardment across the Gaza Strip, damaging […] 94% of the hospitals, killing and hurting children who are seven times more likely to die from blast injuries than adults (Save the Children 2025).

Obviously, the death of children in an area ravaged by armed conflict is not caused solely by weapons. They can also die from lack of food or medicine. In this sense, the famine in Gaza is a major problem for the Palestinian population trapped in the Gaza Strip. Over a million people, about half of whom are children, are already facing widespread famine. More than 130,000 children under the age of

[1] 36,221 acts against children were committed in 2024 and 5,149 were committed in previous years but verified in 2024.
[2] On April 15, 2023, an armed conflict broke out in Sudan between the Sudan Armed Forces (SAF) and the Rapid Support Forces (RSF). Fighting between the two combatant forces is still ongoing today (January 2026).
[3] The armed conflict in the Gaza Strip and Israel began on October 7, 2023, when the Palestinian military group Hamas launched a surprise attack on Israel, killing 1,195 Israelis and foreign nationals and taking 251 hostages. In response, Israel launched an offensive that killed more than 71,000 Palestinians in Gaza (almost half of them women and children) and wounded more than 171,000 (Al-Mughrabi și Farge 2025).

five are at risk of dying from acute malnutrition and at least 135 children have died from the lack of food since the start of the war (October 7, 2023) and since the declaring of famine on August 22, 2025, according to the Palestinian Ministry of Health (Save the Children 2025).

According to the *World Food Programme*, Sudan is statistically considered to have the world's worst famine. Famine conditions have been confirmed in Al Fasher[4] (~820 km W Khartoum) and Kadugli (~570 km SW Khartoum), with the risk of famine in 20 other areas in Greater Darfur[5] (~1000 km W Khartoum) and Greater Kordofan[6] (~550 km SW Khartoum). It is estimated that approximately 20 million people (41% of Sudan's population) face high levels of acute food insecurity (World Food Programme 2026).

2. Lack of access to government support facilities and its effects

War imprints itself deeply on the mind. Children exposed to violence, displacement, or the loss of family members frequently experience anxiety, depression, sleep disorders, and post-traumatic stress. Fear becomes habitual.

With regard to mental health issues, a study by the World Health Organization (WHO) distinguishes between pre-existing conditions, including mental health disorders such as depression, schizophrenia or harmful use of alcohol and other substances, from those induced by emergency situations, including grief, acute stress reactions, harmful substance use, depression, anxiety and post-traumatic stress disorder and those induced by the humanitarian response, including anxiety caused by a lack of information on how to obtain food or access critical services (WHO 2026).

According to the WHO, efforts to improve mental health care, such as the establishment of psychosocial support centers and mobile clinics in proximity to conflict zones, play an essential role in strengthening societal resilience. These initiatives support individuals, including children, in managing trauma and contribute to maintaining social stability (S. Iancu 2024, 72). These problems are further exacerbated by a lack of medical facilities, which means limited or no access to quality medical care, the deterioration of clinics and hospitals during conflict or their non-existence, staff shortages or insufficient training and disruption to drug supply chains.

Another issue regarding the lack of care facilities for the war-affected children from all around the world regards not only the medical centers or psychological help, but also the lack of education institutions. In the war-affected areas, schools have been suspended and children have been left without any chance of education.

Schools are among the first buildings destroyed in an armed conflict. They are damaged, occupied by armed groups, or simply abandoned as civilians flee. Schools are targeted by armed groups because they are often used as command centers. Schools are compartmentalised, offer various facilities and are easy to defend in the event of a siege. Another vital factor is that terrorist groups take refuge in school and use children as human shields. Thus, in its Resolution no. 1998[7] of 2011, the UN Security Council urged parties to refrain from using schools and hospitals for military purposes, including as military barracks, weapons storage facilities, command centers, detention and interrogation sites and firing and observation positions.

The military use of schools and hospitals directly hampers children's right to education and health, but also turns safe havens for children into lawful targets for attacks, and changes community perceptions of schools and hospitals as places of learning and healing into places of violence and

[4] Capital of North Darfur District. On October 26, 2025, the RSF captured El Fasher, the capital of North Darfur District, the last major SAF stronghold in the region. The capture of the city followed a 500-day siege. Media reports focused on violent actions by the RSF, such as atrocities, mass killings, sexual violence, and the destruction of hospitals. (G4Media 2025).
[5] District in Sudan.
[6] District in Sudan.
[7] UN Security Council Resolution 1998 (2011), adopted unanimously on July 12, 2011, focused on protecting children in armed conflict, specifically targeting recurrent attacks on **schools and hospitals**, calling for them to be declared "off-limits" for military use.

insecurity (UN 2025, 4). Still, Israeli forces have intensified their bombardment across the Gaza Strip, damaging 97% of schools (Save the Children 2025).

According to the *Report of the Special Representative of the Secretary-General for Children and Armed Conflict to the General Assembly*, attacks on civilian objects and infrastructure, including schools and hospitals, significantly heightened the vulnerability of children and increased by 44% during 2024. A total of 2,374 attacks on schools and hospitals were verified, with most attacks verified in Ukraine, Israel and the Occupied Palestinian Territory and Haiti (UN 2024, 4).

In the *Children and armed conflict annual report of the Secretary-General* it is stated that, in 2024 there were registered 1,265 attacks on schools, with most affected countries: Ukraine, Israel and the Occupied Palestinian Territory, Haiti, Afghanistan and Myanmar (UN 2024, 3).

Education interruptions deprive children not only of knowledge but of structure, stability, and social connection. When schooling disappears, children are pushed prematurely into adult roles: working to support families, caring for siblings, or navigating displacement alone. In some conflicts, children are forcibly recruited as soldiers, porters, or messengers, blurring the line between victim and participant and exposing them to further trauma.

Education interruptions lead to months or years without structured learning. The losses compound over time: loss of literacy skills, unfinished schooling, and greatly reduced chances of future employment. For girls in particular, the disruption often becomes permanent, as early marriage, domestic work or displacement replace school.

3. Lost homes and refugee centers (displacement)

Armed conflicts are a major driver of forced displacement. Children make up a significant proportion of refugees and internally displaced persons. Uprooted from familiar environments, they lose homes, friends and cultural anchors. Life in camps or temporary shelters often means overcrowding, limited education, insecurity and heightened risks of exploitation, child labor or trafficking.

Forced displacement uproots children and youths at a time when their lives most need stability. Displacement also fragments family structures. Separation from parents or caregivers leaves children particularly exposed, both emotionally and physically, in environments where protection mechanisms are weak or overwhelmed.

Around the globe, an estimated 11.2 million to 13.7 million children have been internally displaced as a result of armed conflict (UNICEF 2025). By the end of 2024, the total number of children displaced by conflict and violence rose to 48.8 million, with large populations of children driven from home in places around the world: Sudan, Myanmar, the Gaza Strip, the Democratic Republic of the Congo and Afghanistan. This number included more than 19.1 million refugee children and asylum-seekers (*15 million refugees under UNHCR mandate and other children in need of international protection*[8]*, 1.7 million Palestine children registered as refugees with the United Nations Relief and Works Agency/UNRWA*[9]*, and approx. 2.7 million asylum-seeking children*), and an estimated 29.4 million children displaced within their own countries by conflict and violence (UNICEF 2025). Also, according to the UNICEF's data, at the end of 2024, an additional number of 4.4 million children were living in situations of internal displacement, because of disasters.

According to statistics, Sudan is the world's biggest displacement crisis with more than 12 million people, one in three Sudanese being forced from their homes by the conflict (World Food Programme 2026). This high number includes over 3 million people that have fled into neighbouring

[8] The category "Other people in need of international protection" (OIP) refers to "people who are outside their country or territory of origin, typically because they have been forcibly displaced across international borders, who have not been reported under other categories (asylum-seekers, refugees, people in refugee-like situations) but who likely need international protection, including protection against forced return, as well as access to basic services on a temporary or longer-term basis".

[9] In total, 6 million Palestine refugees are registered in Jordan, Lebanon, Syria, Gaza, and the West Bank with the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA). These refugees are outside of the mandate of UNHCR.

countries, including Chad, South Sudan and Egypt, and approximately 8.4 million individuals displaced within Sudan (UNHCR 2024). The conflict has had a shocking impact on food provisions, with over half the population facing acute hunger, while the rainy season worsened already dire conditions in overcrowded camps inside Sudan and in Chad, where widespread flooding contributed to outbreaks of cholera and malaria (UNHCR 2024).

Sudan's war between the Sudanese Armed Forces (SAF) and Rapid Support Forces (RSF), which began in April 2023, has become one of the world's deadliest conflicts (World population review 2026). According to the Armed Conflict Location & Event Data Project (ACLED), between August 2024 and August 2025, more than 20,000 people were killed, with many more unreported. The fighting has destroyed cities like Khartoum and El Fasher, displaced over 12 million people and triggered diseases, famine conditions amid attacks on hospitals and aid convoys (World population review 2026).

Regarding Gaza, the conflict between Israel and Palestinian factions, which sharply escalated in October 2023, continues to negatively overwhelm the Gaza Strip and parts of the West Bank. According to the Armed Conflict Location & Event Data Project (ACLED), between August 2024 and August 2025, approx. 21,417 people were killed, making it one of the deadliest conflicts in the world (World population review 2026). "Fighting, bombardments and humanitarian blockades have left tens of thousands more injured and displaced, while widespread damage to hospitals, schools and infrastructure has led the United Nations to label Gaza's humanitarian situation as catastrophic" (World population review 2026). UNHCR has repeatedly called for lasting ceasefires that would end the misery in Lebanon and Gaza and called for the renewal of critical funding to the UNRWA (UNHCR 2024).

4. Children recruited by military forces

Many children abandon their own home in order to avoid forced recruitment, only to find that displacement actually exposes them to the risk of recruitment, especially if they have no type of documents and if they travel alone. Mostly, in Syria, Afghanistan and Yemen, the vast majority of children who find themselves in conflict zones are deemed at risk of recruitment (Save the children 2021).

According to an UNICEF study, thousands of children are recruited and used in armed conflicts around the world. Between 2005 and 2022, more than 105,000 children were recruited by different groups/proxies/parties engaged in a conflict, although the actual number of cases is believed to be much higher (UNICEF 2021). Both girls and boys suffered extensive forms of exploitation and abuse. Parties to the conflict use children not only as combatants, but also in numerous other roles, such as spies, cooks, guards, even messengers and couriers and so on and so forth (UNICEF 2021). Furthermore, living among armed actors, children experience numerous forms of violence, starting from harrowing training to hazardous labour or to being forced to engage in combat, experiencing potential risk of chronic injury and death. Many, especially girls, are subjected to gender-based violence (UNICEF 2021).

Children become part of an armed force or group for various reasons. Some are abducted, threatened, coerced or manipulated by armed actors. Others are driven by poverty, compelled to generate income for their families. Still others associate themselves for survival or to protect their communities. No matter their involvement, the recruitment and use of children by armed forces is a grave violation of child rights and, no less, of international humanitarian law (UNICEF 2021).

Although they are part of an armed group, children in the war-affected areas are still subjected to forms of torture, discrimination and forced to commit crimes in order to better integrate into the group. Children are also subjected to forms of malnutrition, especially in the context of armed conflict, where groups have limited access to food[10].

[10] In armed conflicts, starvation is used as a weapon. The army, which belongs to and is loyal to the government, closes all the country's borders to stop the supply of resources to the country. Although this tactic helps, as the militias can no longer obtain supplies, it also affects the civilian population, which is left without food. For example, the Saudi-led coalition closed the borders with Yemen to stop supplies from reaching the Houthi rebels (McVeigh 2017).

Another important issue is the reintegration of the abused children in the war-affected areas, into their families. The impact of conflict on children does not end when the fighting stops. A generation raised amid violence may struggle with trust, civic engagement and, mostly, social cohesion. Lost years of education translate into reduced economic opportunities, perpetuating cycles of poverty and instability. Communities may be coping with their own challenges and trauma from conflict and are having trouble understanding or accepting children who have returned to their homes (UNICEF 2021). Psychological distress makes it difficult for children to process and articulate their traumatic experiences, especially when they fear stigma or people's reaction and prejudices. However, children affected by conflict often demonstrate extraordinary resilience. With adequate support, education and protection, many become powerful agents of recovery and peace within their communities.

Takeaways

War wears down childhood by interrupting safety, education, emotional development and the horizon of future possibilities.

Societies that fail to protect the affected children risk reproducing cycles of trauma, violence and fragility across generations.

Humanitarian organisations mitigate harm, but cannot compensate for structural neglect. Emergency interventions, while vital, cannot substitute for coherent national and international policies that prioritise children beyond crisis response.

Child protection must be understood as a long-term investment in peacebuilding. Education, psychosocial care and family reunification are not ancillary measures, but core components of post-conflict recovery and societal resilience.

Placing children at the centre of reconstruction strategies reshapes post-war societies. Therefore, recovery models that integrate children's needs contribute to a sustainable development of the future.

The measure of a conflict's aftermath lies in how childhood is restored. Rebuilding cities without restoring childhood risks creating a peace that is structurally hollow and morally incomplete. Those children will, inevitably, grow up, having in mind all the horrors of the war and the lack of life conditions they have already experienced. The lack of comparison might lead not to the restoring of a society, but to the construction of a society with no vision and goals.

BIBLIOGRAPHY:

Aljazeera. 2024. "Aljazeera." *More than 10 million children in line of fire as war rages in Sudan.* 4 10. Accessed 1 10, 2026. https://www.aljazeera.com/news/2024/4/10/more-than-10-million-children-in-line-of-fire-as-war-rages-in-sudan

Al-Mughrabi, Nidal, and Emma Farge. 2025. "Reuters." *How many Palestinians has Israel's Gaza offensive killed?* 7 29. Accessed 1 10, 2026. https://www.reuters.com/world/middle-east/how-many-palestinians-has-israels-gaza-offensive-killed-2025-03-24/

G4Media. 2025. "G4Media." *Avertismente severe de genocid după preluarea controlului asupra orașului El-Fasher din Sudan de către rebelii RSF.* 10 30. Accessed 1 10, 2026. https://www.g4media.ro/avertismente-severe-de-genocid-dupa-preluarea-controlului-asupra-orasului-el-fasher-din-sudan-de-catre-rebelii-rsf.html

Iancu, Sinziana. 2024. "Annals–Series on Military Sciences." *The psychological dimension of resilience in the Ukraine and Israel conflicts.* Accessed 01 10, 2026. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=3zJg5u0AAAAJ&citation_for_view=3zJg5u0AAAAJ:LkGwnXOMwfcC

_____. 2024. "Annals–Series on Military Sciences." *The psychological dimension of resilience.* Accessed 01 17, 2026. https://www.aos.ro/wp-content/anale/MTVol16Nr2Art.6.pdf

_____. 2024. “Monitor Strategic.” *Building Resilience in the Context of Russian Hybrid Threats*. Accessed 01 12, 2026. https://scholar.google.com/citations?view_op=view_citation&hl=en& user=3zJg5u0AAAAJ&citation_for_view=3zJg5u0AAAAJ:5nxA0vEk-isC

_____. 2024. “Revista de Ştiinţe Militare.” *Factorii psihologici care influenţează reziliența în societăţile afectate de război.* Accessed 01 11, 2026. https://www.ceeol.com/search/article-detail?id=1290629

Iancu, Sînziana. 2024. “The psychological dimension of resilience in the Ukraine and Israel conflicts.” *Annals–Series on Military Sciences*, 70-82.

McVeigh, Karen. 2017. “The Guardian.” *Closure of Yemen's borders to aid deliveries is 'catastrophic', UN warns*. 11 7. Accessed 1 10, 2026. https://www.theguardian.com/global-development/2017/nov/07/closure-of-yemen-borders-to-aid-deliveries-is-catastrophic-un-united-nations-warns

OHCHR. 2026. “OHCHR.” *2025 deadliest year for civilians in Ukraine since 2022, UN human rights monitors find*. 1 12. Accessed 1 12, 2026. https://ukraine.ohchr.org/en/2025-deadliest-year-for-civilians-in-Ukraine-since-2022-UN-human-rights-monitors-find

2021. “Save the children.” *Stop the War on Children: A crisis of recruitment*. Accessed 01 23, 2026. https://resourcecentre.savethechildren.net/document/stop-the-war-on-children-a-crisis-of-recruitment

Save the Children. 2025. “Save the Children.” *Gaza: 20,000 children killed in 23 months of war - more than one child killed every hour*. 09 06. Accessed 1 10, 2026. https://www.savethechildren.net/news/gaza-20000-children-killed-23-months-war-more-one-child-killed-every-hour

2025. “UN.” *Children and armed conflict*. 09 2. Accessed 1 10, 2026. https://docs.un.org/en/A/80/266

2025. “UN.” *Report of the special representative of the secretary general for children and armed conflict to the general assembly 6*. 7 25. Accessed 1 10, 2026. https://docs.un.org/en/A/80/266

UN. 2024. *Summary-of-the-Annual-Report-on-Children-and-Armed-Conflict*. Accessed 1 10, 2026. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://childrenandarmedconflict.un.org/wp-content/uploads/2025/06/Summary-of-the-Annual-Report-on-Children-and-Armed-Conflict.pdf

—. 2024. “UN.” *2023: Alarming levels of violence inflicted on children in situations of armed conflict*. 7 13. Accessed 1 10, 2026. https://childrenandarmedconflict.un.org/2024/06/2023-alarming-levels-of-violence-inflicted-on-children-in-situation-of-armed-conflict/

2024. “UNHCR.” *A Year of Turmoil: Conflicts, Crises and Displacement in 2024*. 12 26. Accessed 01 23, 2026. https://www.unhcr.org/news/stories/year-turmoil-conflicts-crises-and-displacement-2024

2023. “UNHCR.” *UNHCR: Forced displacement continues to grow as conflicts escalate*. 10 25. Accessed 01 25, 2026. https://www.unhcr.org/news/unhcr-forced-displacement-continues-grow-conflicts-escalate?gad_source=1&gad_campaignid=23232545219&gbraid=0AAAAA-Pr7kkRzrkUfJf6Ue_XpKavDLt5W&gclid=Cj0KCQiAm9fLBhCQARIsAJoNOcuebMH0WYjtTi3-8lLT-bvhSBvoyCC1sV_6Q-ZkvT7brr5ullhwarga

2025. “UNICEF.” *Close to 50 million children had been displaced due to conflict and violence globally by the end of 2024*. 06 01. Accessed 01 23, 2026. https://data.unicef.org/topic/child-migration-and-displacement/displacement/#footnote2

2025. “UNICEF.” *Displacement of children*. Accessed 01 23, 2026. https://childrenandarmedconflict.un.org/displacement-of-children/

UNICEF. 2021. “UNICEF.” *Children recruited by armed forces or armed groups*. 4 1. Accessed 1 10, 2026. https://www.unicef.org/protection/children-recruited-by-armed-forces

WHO. 2026. “WHO.” *Mental health in emergencies*. 5 6. Accessed 1 10, 2026. https://www.who.int/news-room/fact-sheets/detail/mental-health-in-emergencies

World Food Programme. 2026. “World Food Programme.” *Sudan*. 1 1. Accessed 1 10, 2026. https://www.wfp.org/emergencies/sudan

2025. “World Health Organization (WHO).” *Mental health in emergencies*. 05 06. Accessed 01 25, 2026. https://www.who.int/news-room/fact-sheets/detail/mental-health-in-emergencies

2026. “World population review.” *Countries Currently at War 2026*. Accessed 01 23, 2026. https://worldpopulationreview.com/country-rankings/countries-currently-at-war

DOI: 10.53477/3045-2309-26-13

SMART INFRASTRUCTURE, SMART DEFENCE: DIGITAL TWINS AND PREDICTIVE MONITORING FOR RESILIENCE

Maria Niamh BRATCOVICI,
MA in Protection of Critical Infrastructure,
"Carol I" National Defence University, Bucharest, Romania.
E-mail address: bratcovicimaria@gmail.com

Abstract*: The increasing digitalisation of civil and defence infrastructure is reshaping how resilience is conceived and maintained in contemporary security environments. This paper investigates how digital twin technology and predictive monitoring systems enhance the operational stability of critical assets such as bridges, energy facilities, and transport networks. Using a theoretical and comparative approach, it examines the integration of satellite imagery, IoT sensors, and artificial intelligence for real-time assessment, anomaly detection, and predictive maintenance. The study argues that the adoption of digital twins transforms resilience from a static, reactive process into a dynamic, data-driven capability. It demonstrates the strategic utility of smart infrastructure in defence planning and crisis management, proposing that predictive analytics and interdisciplinary collaboration can significantly strengthen national and allied resilience frameworks.*

Keywords: *smart infrastructure; digital twin technology; predictive monitoring; critical infrastructure resilience, data-driven defence; artificial intelligence in security.*

Introduction

In the context of an increasingly volatile security environment, characterised by rapid technological advancement, hybrid threats, and systemic interdependence, the demarcation between civilian infrastructure and defence capabilities has become progressively porous. Contemporary security architectures no longer rely solely on conventional deterrence and hard-power instruments but are increasingly underpinned by the resilience and adaptability of critical infrastructures. The notion of *smart infrastructure*, which can be broken down in a complex ecosystem of interconnected assets equipped with sensors, data analytics, and digital replicas- epitomises this paradigm shift. No longer passive backbones of national functionality, infrastructures have evolved into *active, cognitive systems* capable of perceiving, processing, and responding to environmental stimuli in near real time.

Against this backdrop, the present paper explores the strategic relevance of *digital twin* technology and *predictive monitoring* as transformative instruments in the pursuit of infrastructure resilience. These technologies enable decision-makers to visualise, simulate, and anticipate structural and operational vulnerabilities before they manifest, thereby converting uncertainty into strategic foresight. Situated at the intersection of defence innovation, cyber-physical systems, and strategic autonomy, this research advances the argument that data-driven infrastructure management constitutes an emergent domain of security power, one where information precision and temporal advantage are as decisive as kinetic capability.

The central aim of this paper is to demonstrate that integrating digital twin frameworks into the governance of critical infrastructures such as bridges, energy grids, and transport corridors, represents not merely a technological enhancement but a doctrinal evolution in national and allied defence postures. By transitioning from reactive maintenance paradigms to *anticipatory resilience*, states and institutions can pre-empt disruptions arising from cyber intrusions, environmental stressors, or hostile hybrid operations. Furthermore, the paper underscores the necessity of a cross-disciplinary approach that unites civil engineers, data scientists, and defence strategists in designing infrastructures that are not only intelligent but inherently secure, adaptive, and strategically relevant.

1. Anticipatory Resilience: Governing the Digital-Physical Continuum

The twenty-first century has ushered in an era where power is no longer defined solely by military expenditure or troop strength, but by the *resilience* of a state's interconnected systems. Critical infrastructure, such as transportation, energy, communication, and digital networks, that have become the backbone of national functionality and, by extension, of national security. The ability of these systems to absorb shocks, recover swiftly, and adapt to evolving threats represents the essence of contemporary strategic resilience. As NATO and the European Union (EU) have repeatedly underscored, infrastructure resilience is not merely a technical condition but a determinant of strategic autonomy and operational continuity in times of crisis (NATO 2023; European Commission 2022).

In traditional security paradigms, the defence establishment perceived infrastructure as a supporting domain: an enabler of logistics, force mobility, and energy supply. However, the emergence of hybrid warfare and the systemic vulnerabilities introduced by global interconnectivity have redefined this relationship. Today, infrastructure is simultaneously a *target*, a *weapon*, and a *strategic shield*. The disruption of pipelines, power grids, or transport corridors can produce cascading effects that paralyse state functions without a single shot being fired. Consequently, resilience - the capacity to anticipate, withstand, and recover from multidimensional disruptions, has evolved into a strategic imperative equal in importance to deterrence and combat readiness.

This transformation is deeply intertwined with the digital revolution. As infrastructures become increasingly *cyber-physical systems*, their operational logic depends on flows of data, sensors, and algorithmic decision-making. This integration brings both unprecedented situational awareness and new vulnerabilities. The same systems that enhance performance can be exploited through cyberattacks, misinformation, or technological sabotage. Hence, the strategic challenge of the 2020s and beyond lies not merely in defending territory, but in protecting the digital-physical continuum upon which modern life depends.

Infrastructure resilience is therefore a multidimensional construct, encompassing not only *technical robustness*, meaning the physical strength of structures, but also *functional continuity*, *information integrity*, and *institutional adaptability*. In this context, resilience extends beyond engineering design and enters the realm of strategic governance. The effectiveness of a state's resilience architecture depends on coordination among civilian agencies, military planners, private sector operators, and scientific institutions. This interdependence transforms infrastructure management into a domain of *whole-of-society defence*, reflecting a broader conception of security that merges technological foresight with social preparedness (OECD 2021).

Moreover, the geographical and geopolitical dimensions of infrastructure resilience cannot be overlooked. Global supply chains, transnational energy networks, and digital communication routes have created new theatres of strategic competition. Control over chokepoints, satellite constellations, and undersea cables has become as consequential as control over airspace or maritime routes. As a result, *infrastructure diplomacy* – the use of construction, connectivity, and digital corridors as instruments of influence – has emerged as a new vector of state power. In this context, resilience is not only defensive but also *projective*, shaping a state's ability to sustain operations, assert sovereignty, and extend influence across regions (Global Infrastructure Hub 2022).

The resilience of critical infrastructure thus functions as both a mirror and a multiplier of strategic power. A resilient state can absorb shocks without systemic collapse, preserve the integrity of its command structures, and maintain public confidence during crises. Conversely, the failure of resilience erodes deterrence credibility, disrupts economic stability, and exposes societal vulnerabilities to exploitation by adversarial actors. Therefore, developing infrastructures that are both *intelligent* and *secure*, and at the same time capable of self-assessment, early warning, and adaptive repair, constitutes one of the central challenges of modern defence planning.

This chapter establishes the conceptual foundation for understanding infrastructure resilience as a strategic asset. It also sets the stage for the subsequent analysis of *digital twin technology* and

predictive monitoring as practical mechanisms for operationalising this resilience. In doing so, it situates the argument within the emerging doctrine of *smart defence*, where data-driven systems, artificial intelligence (AI), and simulation-based planning converge to create infrastructures that are not only strong in structure but intelligent in function.

1.1. Resilience as a Strategic Enabler of Defence Readiness

Within contemporary security doctrines, *resilience* has transcended its original civil-protection meaning to become a strategic enabler of military readiness. Defence planners increasingly recognise that the credibility of deterrence and the sustainability of operations depend upon the robustness of national infrastructure networks. The ability of armed forces to project power, sustain logistics, and ensure command-and-control continuity is directly proportional to the resilience of energy grids, transportation corridors, and communication systems.

In NATO's conceptual framework, resilience constitutes one of the seven baseline requirements underpinning collective defence, standing alongside operational mobility and energy security (NATO 2023). This interdependence demonstrates that infrastructure resilience is not a passive attribute but an operational force multiplier. For instance, an airbase supplied by an adaptive, sensor-integrated energy system can maintain functionality under cyber stress or physical disruption, whereas a conventional grid-dependent facility may face operational paralysis.

From an operational standpoint, the integration of predictive monitoring systems and *digital twin* platforms offers a decisive advantage. By providing real-time situational awareness of structural conditions, these systems enable military engineers and commanders to assess the operational readiness of critical assets under both peacetime and crisis conditions. In theatres of operation, where the margin between stability and failure is narrow, such foresight allows for pre-emptive maintenance and resource allocation. (Hossain 2022)

Resilience, therefore, becomes a form of *strategic endurance* - the capacity to sustain military effectiveness over time despite environmental, cyber, or kinetic disruptions. This perspective aligns with the emerging *comprehensive defence* model adopted by several European and Indo-Pacific states, which advocates for the integration of civil infrastructure resilience into national defence planning. In this framework, resilience is not ancillary to power projection but intrinsic to it, forming a vital component of strategic deterrence through persistence (Global Infrastructure Hub 2022).

1.2. The Militarisation of Infrastructure Resilience in the Era of Smart Defence

The evolution of *smart defence* has redefined the relationship between technological innovation and military capability. Traditionally, the defence establishment relied on *hard-power asymmetries* - superior firepower, mobility, and industrial capacity - to maintain strategic advantage. However, in the digital age, asymmetry is increasingly determined by the ability to integrate civil technologies into defence ecosystems. The militarisation of infrastructure resilience thus reflects a doctrinal and structural shift: from platform-centric warfare to *system-centric security*.

Digital twins and predictive monitoring exemplify this transition. They transform infrastructures into *operationally aware entities*, more precisely into systems that can sense degradation, report anomalies, and simulate their own recovery processes. In military contexts, these capabilities extend beyond maintenance efficiency; they underpin decision superiority. By fusing data from sensors, satellites, and unmanned systems, digital twin frameworks allow commanders to visualise the real-time status of logistical routes, fuel depots, or bridge stability during rapid manoeuvres (Alharbey 2024).

Moreover, predictive analytics embedded within these systems contribute to *resilience intelligence*, a new domain of situational awareness that integrates engineering diagnostics with strategic assessment. This form of intelligence offers the military the capacity to forecast potential systemic failures and model their cascading effects across networks, that are essential for planning continuity of operations (COOP) and mission assurance.

The militarisation of resilience also introduces complex governance implications. As infrastructures become dual-use, serving both civilian and defence objectives, the lines of jurisdiction blur. The success of *smart defence* thus hinges on institutional cooperation among ministries of defence, civil engineering authorities, private-sector technology providers, and cybersecurity agencies. The creation of interoperable standards for predictive monitoring, data security, and infrastructure recovery will determine the degree to which allied nations can operationalise the concept of shared resilience.

Ultimately, *smart infrastructure* embodies a paradigm in which engineering excellence converges with strategic foresight. In this militarised conception, the resilience of a bridge, a port, or an energy grid is not measured solely in physical robustness, but in its ability to sustain national power projection and preserve strategic decision space under duress. As global competition increasingly targets vulnerabilities within the grey zone between war and peace, infrastructure resilience has become the first line of defence - quiet, data-driven, and decisively strategic (Technological trends in the 21st-century defense and security sector 2025).

2. The Digital Feedback Loop: High-Fidelity Synchronisation in Defence Engineering

In the evolving landscape of global security, technological innovation is no longer a peripheral asset, but the fulcrum upon which strategic advantage pivots. The defence sector, historically a crucible for high-stakes engineering, has become a dynamic interface between military imperatives and civilian breakthroughs. This chapter explores the dual-use nature of emerging technologies, the mechanisms of innovation transfer, and the implications for national resilience and operational superiority.

At the heart of this transformation lies a paradox: the most disruptive technologies of the 21st century such as: artificial intelligence, quantum computing, autonomous systems, are being developed in civilian laboratories, startups, and academic institutions. Yet, their strategic relevance is unequivocal. Consider the case of drone swarms: originally conceived for agricultural monitoring and logistics, they now form the backbone of next-generation battlefield tactics, capable of overwhelming traditional air defence systems through decentralised coordination and adaptive routing (Grieves 2017).

This convergence of civilian ingenuity and military application demands a rethinking of traditional R&D. Defence ministries and private contractors are increasingly adopting agile development models, where iterative prototyping and rapid deployment replace the slower, linear procurement cycles of the past. The result is a more porous boundary between sectors, one that enables faster adaptation but also raises critical questions about governance, ethics, and control.

The Architecture and Functional Logic of Digital Twin Systems in Defence Infrastructure

Digital twin technology embodies a paradigm shift in how complex infrastructure systems are designed, monitored, and protected. At its core, a *digital twin* represents a high-fidelity virtual counterpart of a physical asset, one that evolves continuously through real-time data synchronisation. This duality establishes an interactive feedback loop between the physical and the digital domains, transforming static engineering models into *living analytical systems*. Within the defence sphere, such systems enable comprehensive oversight of critical infrastructure such as bridges, energy networks, runways, or command facilities, whose operational continuity is essential to national resilience (Bolisani 2023).

A digital twin's architecture is typically structured around three interdependent layers: the physical layer, the data integration layer, and the cognitive layer (see Figure no. 1). The physical layer comprises sensors, actuators, and IoT devices that capture quantitative data on stress, temperature, vibration, and environmental factors. The data integration layer aggregates and standardises this information using secure communication protocols, ensuring interoperability between legacy and modern systems. The cognitive layer – the analytical engine – employs artificial intelligence (AI) and machine learning (ML) algorithms to generate predictive insights and adaptive recommendations for decision-makers (Ntalampiras 2023).

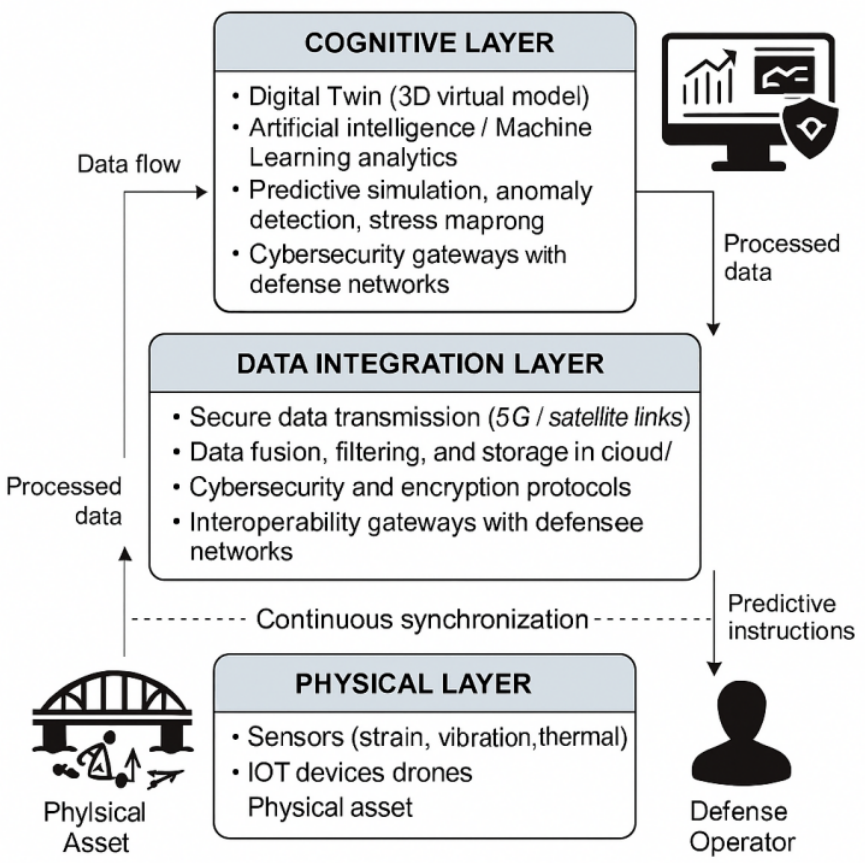

Figure no. 1: Conceptual Model of Digital Twin Architecture for Defence Infrastructure

3. Predictive Monitoring and Data-Driven Defence

The exponential growth of data generation, combined with advances in artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT) has transformed the informational environment in which modern defence systems operate. Predictive monitoring, the capacity to anticipate system behaviour, detect anomalies, and forecast potential failures before they occur have emerged as a cornerstone of *data-driven defence*. This paradigm marks a decisive shift from reactive maintenance and crisis management to anticipatory resilience and adaptive decision-making (Big Data and Artificial Intelligence for Military Decision Making and Logistics 2022).

In the context of critical infrastructure and defence planning, predictive monitoring integrates multisource data-satellite imagery, sensor input, environmental parameters, and structural analytics, into a coherent intelligence architecture. By translating raw data into actionable insights, it allows institutions to prioritise interventions, allocate resources efficiently, and mitigate cascading risks. This capability has become increasingly central in an age where the *tempo of disruption* often exceeds the capacity of human operators to respond effectively.

Predictive monitoring thus serves as both a technological enabler and a strategic amplifier. It enhances the *decision superiority* of military and civil authorities by providing foresight under uncertainty, reducing the cognitive burden of complexity, and enabling pre-emptive action across multiple operational domains (Digitalisation of Infrastructure for a Sustainable Future. 2022).

Operational Benefits and Strategic Metrics of Predictive Monitoring

Predictive monitoring generates measurable outcomes that directly contribute to defence readiness and cost-effectiveness. When applied to strategic infrastructures such as airbases, naval facilities, energy networks, the technology enhances structural integrity, operational efficiency, and cybersecurity posture simultaneously, not only strengthening the functional reliability of defence infrastructure but also reshapes the decision-making environment in which military and civil authorities operate.

By transforming disparate sensor readings, environmental parameters, and system diagnostics into coherent analytical outputs, predictive systems allow institutions to transition from linear maintenance cycles to continuously optimised operational planning. This shift enhances the agility of defence organisations, enabling them to anticipate capability degradation, adjust resource distribution pre-emptively, and maintain mission functionality even under fluctuating threat conditions.

At a broader strategic level, predictive monitoring contributes to the development of resilience intelligence, a data-driven understanding of how infrastructures behave under stress and how disruptions propagate across interdependent systems. This form of intelligence is essential for assessing critical vulnerabilities, modelling the consequences of hybrid threats, and strengthening cross-domain redundancy. As infrastructures become increasingly integrated within national defence ecosystems, the capacity to quantify resilience through measurable indicators provides a foundation for evidence-based planning and for aligning technological investments with operational priorities.

Table no. 1 illustrates a simplified framework that summarises the *strategic benefits and measurable indicators* associated with predictive monitoring in defence infrastructure.

Table no. 1: Strategic Applications and Performance Indicators of Predictive Monitoring in Defence Infrastructure

Operational Domain	*Predictive Function*	*Strategic Benefit*	*Key Performance Indicator (KPI)*
Structural Integrity	Early anomaly detection via vibration and stress sensors	Reduced unplanned downtime; extended asset lifespan	Mean Time Between Failures (MTBF); % reduction in critical incidents
Energy Infrastructure	Load forecasting using AI and environmental data	Optimised power allocation; improved energy security	Forecasting accuracy (%); downtime reduction (%)
Cybersecurity	Behavioural anomaly monitoring in network traffic	Prevention of cyber intrusion and system compromise	Mean Time to Detect (MTTD); False Positive Rate (%)
Logistics and Mobility	Real-time route and equipment condition monitoring	Enhanced operational continuity during crisis	Response time (min); resource reallocation efficiency (%)
Command & Control	Predictive analytics for mission assurance	Improved decision superiority and risk anticipation	Decision latency (s); situational awareness index

Conclusions

All in all, the analysis undertaken in this paper has demonstrated that the convergence of digital twin technology, predictive monitoring, and artificial intelligence represents a transformative frontier in defence resilience. Smart infrastructure no longer functions as a passive substrate of national power but as an active intelligence system, capable of perceiving, adapting, and responding to evolving threats across physical, digital, and cognitive domains.

From a strategic perspective, the adoption of data-driven systems redefines both the nature and scope of defence preparedness. Predictive monitoring introduces a paradigm in which resilience becomes anticipatory rather than reactive, enabling decision-makers to foresee disruptions and mobilise countermeasures before critical thresholds are reached. In this sense, the essence of security transitions from protection of assets to preservation of *continuity, functionality,* and *decision superiority*.

The study further suggests that digital twins serve not merely as engineering innovations but as doctrinal instruments. They integrate structural diagnostics, cyber resilience, and operational intelligence within a unified framework that strengthens both national and allied defence architectures. The ability to model, simulate, and forecast system behaviour transforms uncertainty into an operational variable, that can be measured, managed, and strategically exploited.

Ultimately, the evolution toward smart, adaptive infrastructure signifies the emergence of a new defence paradigm-one where the boundary between technology and strategy is increasingly indistinct. The resilience of future societies will depend not solely on the strength of their physical structures, but on the intelligence embedded within them. In this context, *smart infrastructure* becomes synonymous with *smart defence*, representing the next decisive step in achieving enduring security in an age of complexity and interdependence.

Additionally, the emergence of predictive, data-driven defence systems underscores the growing relevance of ethical and security frameworks governing the use of advanced technologies. The capacity to automate elements of risk assessment, mission assurance, and operational planning introduces questions concerning transparency, accountability, and human oversight. Ensuring that such systems remain aligned with democratic norms, strategic intent, and societal values will be essential for preserving legitimacy as defence infrastructures evolve toward higher levels of autonomy and computational reasoning.

Finally, the research presented in this paper highlights the need for long-term strategic investment in resilient, adaptive, and digitally integrated infrastructure ecosystems. As geopolitical tensions intensify and hybrid threats proliferate, the nations that succeed will be those capable of transforming technological innovation into enduring strategic advantage. Digital twins and predictive monitoring offer precisely such an avenue: they equip defence planners with the capacity to understand, anticipate, and shape complex operational environments. By embedding intelligence and foresight into the structural foundations of society, states strengthen not only their defence posture but their overall capacity to navigate an uncertain and interconnected future.

BIBLIOGRAPHY:

Grieves, M., & Vickers, J. 2017. “Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. In Transdisciplinary Perspectives on Complex Systems”. *Springer.*

Alharbey, Riad, Aqib Shafiq, Ali Daud, and Hussain Dawood. 2024. “Digital Twin Technology for Enhanced Smart Grid Performance: Integrating Sustainability, Security, and Efficiency”. *Frontiers in Energy Research*.

Bolisani, Ettore, and Enrico Scarso. 2023. “The Digital Twin in the Context of Industry 4.0: A Review of Its Role and Future Perspectives”. *Journal of Industrial Information Integration.*

Hossain, Eklas, and Mohammad Rahman. 2022. “Smart Infrastructure and Predictive Maintenance: A Systemic Review”. *IEEE Access.*

Kritzinger, Werner, Michael Karner, Georg Traar, Jan Henjes, and Wilfried Sihn. 2018. “Digital Twin in Manufacturing: A Conceptual Framework”. 101-107. Procedia CIRP 67.

Ntalampiras, Stavros, and Pasquale Daponte. 2023. “AI-Based Predictive Maintenance for Critical Infrastructure Protection”. Sensors 23 no.14.

2022. *Global Infrastructure Hub*. October 1. Accessed 23 2025, November . https://www.gihub.org/resources/publications/digitalisation-for-sustainable-infrastructure-the-road-ahead/

2025. *Technological trends in the 21st-century defense and security sector.* 03 17. Accessed 11 4, 2025. https://www.gmv.com/en-es/media/blog/defense-security/technological-trends-21st-century-defense-security-sector

2022. *Digitalisation of Infrastructure for a Sustainable Future.* Publications Office of the European Union, Brussels: European Commission.

2022. *Big Data and Artificial Intelligence for Military Decision Making and Logistics.* STO-TR-IST-160., Brussels: NATO Science & Technology Organization.

OECD. 2021. *Strengthening Critical Infrastructure Resilience:Policy Tools and Approaches*. Paris: OECD Publishing.

DOI: 10.53477/3045-2309-26-14

SECURING THE BLACK BOX: A TECHNO-DIPLOMATIC FRAMEWORK FOR AI INTEGRATION IN MODERN DEFENCE ALLIANCES

Dumitru-Cătălin VASILE, Dipl. Eng.,
PhD Candidate, National School of Political and Administrative Studies, Bucharest, Romania
Master's Student, "Carol I" National Defence University, Bucharest, Romania
E-mail address: catalin.vasile@outlook.com

Abstract*: Integrating Artificial Intelligence (AI) into modern defence alliances creates a serious trust issue: the "black box" problem. When algorithms are opaque, they undermine the inter-state trust that coalitions need to operate effectively. This paper examines the conflict between strict national data sovereignty and operational demands for shared intelligence. Using a qualitative approach that draws on recent developments from NATO's DIANA initiative and AUKUS Pillar 2, I propose a "Techno-Diplomatic Framework". The study argues that traditional hardware standards are insufficient for managing probabilistic machine learning. Instead, it suggests a governance model that utilises Privacy-Enhancing Technologies, specifically Federated Learning and Confidential Computing, as diplomatic enablers. By harmonising technical tools with normative alignment, alliances can achieve "cognitive interoperability". This approach allows nations to collaborate on sensitive training without exposing sovereign data, effectively transforming the black box from a vulnerability into a secured asset for collective defence*.

Keywords: *Techno-diplomacy; Artificial Intelligence; Interoperability; Black Box Problem; Federated Learning; NATO*.

Introduction

The contemporary global security environment is defined by the collision of kinetic threats and digital disruptions, forcing defence alliances to fundamentally reimagine the nature of collective security (Hadean, 2025). Central to this transformation is the integration of Artificial Intelligence (AI) into the military instrument of power. Unlike previous revolutions in military affairs, driven by gunpowder, the internal combustion engine, or nuclear technology, the AI revolution is cognitive (Jensen & Mishra, 2025). It promises to compress the OODA loop (Observe, Orient, Decide, Act) from minutes to milliseconds, analysing vast sensor arrays to predict adversary behaviour and optimise logistics with superhuman precision (Bozkurt et al., 2025). For alliances such as the North Atlantic Treaty Organization (NATO), the AUKUS partnership, and the Five Eyes intelligence consortium, the adoption of AI is not merely an option for modernisation; it is an imperative for survival in an era of "techno-strategic" competition with revisionist powers (European Parliamentary Research Service [EPRS], 2025).

The transition to AI-enabled warfare introduces a structural vulnerability that is as much diplomatic as it is technical: the "black box" problem (Sullivan & Ricket, 2024). The most potent AI systems, particularly those utilising deep reinforcement learning and large language models (LLMs), operate through internal logics that are often unintelligible to their human operators. In a sovereign defence context, this opacity complicates testing and evaluation. In a multinational coalition, it creates a crisis of trust. When a commander from Nation A is asked to authorize a strike based on a target identified by Nation B's algorithm, the inability to interrogate the system's reasoning to "open the black box" becomes a political and legal liability.

How can an alliance maintain unity of command when its constituent digital systems rely on opaque algorithmic processes whose outputs are inherently inexplicable? The data fuelling these systems is subject to increasingly stringent sovereignty regimes (NATO, 2025). The traditional model of intelligence sharing, predicated on the exchange of finalised reports or raw signals, is ill-suited for the era of machine learning, which requires massive, continuous datasets to train and refine models. Nations are rightfully wary of pooling sensitive data into centralized repositories due to security risks and the potential for "model inversion" attacks that could expose national secrets. This creates 'data silos'. These silos fragment the alliance's view, making us weaker together than we are apart.

We argue that resolving these challenges requires a new form of statecraft: "techno-diplomacy" (World Economic Forum [WEF], 2023). It argues that the technical architectures of AI systems must be elevated to the level of diplomatic protocols. By moving beyond the static "hardware interoperability" of the 20th century (standardised ammunition and fuel) to a dynamic "cognitive interoperability", alliances can secure the algorithmic bond (Belfer Center for Science and International Affairs, 2025). This research creates a unified Techno-Diplomatic Framework that leverages emerging privacy-enhancing technologies (PETs), specifically Federated Learning (FL) and Confidential Computing, to reconcile the competing demands of data sovereignty and collective intelligence.

The analysis proceeds in four parts: Chapter 1 dissects the "Strategic Black Box", analysing the operational and legal risks posed by opaque AI in coalition settings. Chapter 2 examines the "Data Sovereignty Crisis", exploring the friction between national classification regimes and the technical needs of AI training. Chapter 3 defines the emerging field of "Techno-Diplomacy" and evaluates current institutional efforts, such as NATO's DIANA and the EU-US Trade and Technology Council. Chapter 4 provides a technical analysis of the proposed solutions, Federated Learning and Trusted Execution Environments, demonstrating their utility as diplomatic tools. Finally, the paper synthesises these elements into the proposed framework, offering concrete recommendations for the "complex and dynamic" security environment.

This research employs a qualitative methodology to analyse the intersection of artificial intelligence technologies and coalition diplomacy, grounded in a comprehensive review of strategic literature and primary policy documents. The study focuses specifically on modern defence alliances, including the North Atlantic Treaty Organization (NATO), the AUKUS partnership, and the Five Eyes intelligence consortium. The research scope is defined by the "black box" paradox, addressing the fundamental tension between the operational necessity of collective algorithmic intelligence and the sovereign constraints of data security.

To resolve this paradox, the study adopts a dual-track analytical approach that bridges operational theory with technical architecture. First, it conducts a techno-strategic analysis to examine the operational and legal risks posed by opaque AI systems such as Deep Learning and Large Language Models within multinational coalitions, with a particular emphasis on the challenges of "cognitive interoperability" and compliance with International Humanitarian Law (IHL). Second, the research performs an architectural synthesis to evaluate the utility of emerging Privacy-Enhancing Technologies (PETs), specifically Federated Learning (FL) and Confidential Computing. These technologies are analysed not merely as technical tools, but as diplomatic enablers capable of resolving the "Third Party Rule" dilemma and mitigating data sovereignty conflicts.

Data sources for this analysis include official alliance publications, such as those on NATO's DIANA initiative and AUKUS Pillar 2 developments, as well as technical specifications for secure computing mechanisms, such as Trusted Execution Environments (TEEs) and Secure Multi-Party Computation (SMPC). By synthesising these diverse elements, the paper proposes a unified "Techno-Diplomatic Framework" that demonstrates how specific technical architectures can serve as the foundational bedrock for new diplomatic protocols in the era of algorithmic warfare.

1. The strategic black box: operational and trust challenges in coalition AI

The integration of Artificial Intelligence into the defence sector marks a definitive shift from platform-centric warfare, defined by the capabilities of tanks, ships, and aircraft, to data-centric warfare, defined by the superiority of algorithms and information flows (NATO, 2024). In this new paradigm, the "black box" problem is not merely a technical glitch to be debugged; it is a structural impediment to alliance cohesion that creates operational, legal, and strategic problems.

1.1. The opacity of deep learning and the crisis of explainability

The fundamental challenge of modern AI lies in the trade-off between performance and explainability. The most advanced systems, deep neural networks (DNNs) used for computer vision, signal processing, and predictive analytics, operate by processing inputs through millions or billions of parameters (weights) across multiple hidden layers (Sullivan & Ricket, 2024). While these systems can achieve superhuman accuracy in tasks such as target recognition or cyber anomaly detection, their internal architecture presents a unique challenge for coalitions. The pathway from input to output is not merely nonlinear in a mathematical sense, but relies on deep neural networks with millions of parameters in 'hidden layers' that defy reverse-engineering. Unlike a rule-based system where logic is transparent (if X, then Y), a deep learning model generates outputs based on high-dimensional feature correlations that are inaccessible to human operators. This creates a 'black box' phenomenon where the system provides a conclusion without an auditable chain of evidence, leaving the user with no mechanism to understand or reconstruct how the result was derived.

In a coalition environment, this opacity creates a severe "trust deficit" (Reynolds & Atalan, 2024). Interoperability has traditionally been built on deterministic standards: a NATO commander knows that a 5.56 mm round will fire from a compliant rifle because the physical specifications are standardised and verifiable. "Cognitive interoperability", the ability of systems to share understanding, lacks these physical guarantees. This technical opacity has immediate strategic implications. If a US-developed AI system deployed in a joint operations center identifies a potential threat, a German or French commander receiving that data has no mechanism to verify the assessment if the system cannot explain its reasoning. Unlike traditional intelligence sharing, where analysts can scrutinise source credibility and raw data to validate a conclusion, an opaque AI output demands an operational leap of faith. The allied commander cannot discern whether the target identification was driven by robust tactical indicators or a statistical artifact within the model's hidden layers. Consequently, the inability to interrogate the machine's logic creates a fracture in collective decision-making: the ally must either accept a high-risk automated judgment blindly, potentially violating their specific Rules of Engagement or hesitate, thereby negating the speed advantage the AI was meant to provide.

This crisis of explainability introduces severe operational risks, primarily manifesting in operator psychology and alliance cohesion. Operators may vacillate between "automation bias", in which they uncritically accept the AI's output under time pressure, and "algorithm aversion", in which they reject valid AI insights due to a lack of understanding. In a high-tempo coalition environment, this inconsistency can lead to disjointed decision-making and a breakdown in the OODA loop (Bozkurt et al., 2025).

A "lowest common denominator" effect may emerge, as alliances are composed of sovereign states with varying risk appetites. If an AI system serves as a black box, the alliance may be forced to default to the Rules of Engagement (ROE) of the most risk-averse member, effectively vetoing the use of advanced capabilities. As a result, a system that cannot demonstrate its adherence to specific national legal interpretations of "necessity" may be sidelined, negating the investment in the technology.

1.2. The legal quagmire: IHL and the black box

The application of International Humanitarian Law (IHL) to AI-enabled operations is perhaps the most contentious aspect of the black box problem, primarily because IHL principles, specifically distinction, proportionality, and precaution, are inherently subjective and context-dependent (Pollard, 2024). A critical challenge arises regarding the principle of distinction, which requires a system to distinguish between combatants and civilians. A black box model might identify a target based on opaque correlations – such as a specific radio frequency combined with movement patterns – that are statistically valid but legally insufficient. This creates a critical accountability asymmetry. When a human soldier makes a catastrophic error based on flawed intuition (as seen in the Daunte Wright case in Minnesota), the legal system can interrogate their intent, negligence, and adherence to training to assign liability. In contrast, an AI 'hallucination' offers no such recourse. If a commander authorises a strike based on a machine's opaque recommendation that turns out to be a school bus, the chain of responsibility ruptures: the commander can claim reasonable reliance on a certified system, while the developer can claim the system functioned within its statistical error rate, leaving the violation of International Humanitarian Law without a punishable perpetrator.

The principle of proportionality requires weighing the anticipated military advantage against the expected collateral damage, a task that remains a value judgment rather than a mathematical calculation. If an AI system recommends a strike, a human commander acts as the moral agent responsible for that judgment; if the commander cannot understand the parameters the AI used to estimate collateral damage, their ability to exercise "meaningful human control" is illusory. For NATO and its partners, this creates a diplomatic rift, as some allies may interpret "meaningful human control" as requiring an understanding of the system's internal logic. In contrast, others may accept statistical reliability as a proxy for control (Department of Defense [DoD], 2024). Without a framework to bridge these interpretations, the black box becomes a wedge issue that could fracture the alliance during joint operations.

1.3. Adversarial vulnerabilities: the poisoned box

The opacity of AI systems also expands the attack surface for adversaries. Because the decision-making logic of a black box is hidden, it is uniquely susceptible to "adversarial attacks", subtle manipulations of input data that cause the model to fail with high confidence. One primary method is data poisoning, in which an adversary can subtly corrupt open-source datasets often used to pre-train military models. A "Trojan" behaviour could be embedded in the model, triggered only by a specific visual or digital signal (Scaleout Systems, 2025). In a coalition, if Ally A's model is poisoned and shares erroneous targeting data with Ally B, the corruption spreads across the network. Because the model is opaque, Ally B has no easy way to audit the incoming data for integrity.

Additionally, adversaries can employ model evasion to exploit the "blind spots" of a black box model. For instance, applying a specifically crafted pattern of tape to a tank might cause an image recognition algorithm to classify it as a civilian truck. Without transparency into which features the model prioritises, coalition forces remain vulnerable to these cognitive exploits. A convergence of operational opacity, legal uncertainty, and adversarial vulnerability thus defines the strategic black box. Solving this requires more than better engineering; it requires a diplomatic architecture that can manage risk without demanding impossible levels of transparency.

2. The data sovereignty crisis: fragmentation in the age of fusion

If algorithms are the engines of modern warfare, data is the fuel. The efficacy of AI systems is strictly limited by the diversity and volume of the data upon which they are trained (DefenseScoop, 2025). For a defence alliance, the theoretical advantage is immense: a coalition of 32 NATO nations should theoretically possess a dataset 32 times richer than any single member. In practice, the reality is a landscape of fragmented "data silos" enforced by rigid sovereignty concerns and legacy classification regimes.

2.1. The "third-party rule" and intelligence barriers

The primary diplomatic barrier to AI integration is the "Third Party Rule", a foundational principle of intelligence sharing that dictates that information received from a partner cannot be shared with a third party without the originator's explicit consent. In the context of static documents, this rule is manageable. In the context of AI training, it is a bottleneck. Training a robust coalition model, for example, an acoustic detection model for submarines, requires aggregating raw sonar data from the US, UK, France, and Norway. Under current rules, moving this raw, classified data into a central "training lake" is legally fraught. It would require complex multi-lateral agreements that are slow to negotiate and difficult to enforce.

This means nations default to training their own models on their sovereign data (NATO, 2025). The result is that the US Navy trains its models on Pacific and Atlantic data, while the Norwegian Navy trains on Arctic data. When a US ship operates in the Arctic, its AI is effectively "blind" to the local environmental nuances that the Norwegian model understands perfectly. This lack of data interoperability creates operational seams that adversaries can exploit.

2.2. Techno-nationalism and the fear of exposure

Beyond intelligence handling rules, the rise of "techno-nationalism" has made states increasingly protective of their national data assets. Data is now viewed as a strategic economic resource. There is a palpable fear among defence ministries that sharing high-fidelity training data might inadvertently reveal critical vulnerabilities. First, high-quality training data reveals not only what a military can detect, but also what it cannot, exposing gaps in coverage. Second, regarding sensitive sources and methods, even anonymised data can sometimes be "deanonymised" or reverse-engineered to reveal the location or nature of the sensor that collected it, compromising the source. Finally, an industrial advantage concern exists; as AI becomes a driver of the defence industrial base, nations are incentivised to hoard data to give their domestic defence primes, such as Thales, Leonardo, or Lockheed Martin, a competitive edge in developing superior algorithms.

2.3. The legacy trap: case study of the eastern flank

The data sovereignty crisis is further complicated by the disparity in digital maturity across the alliance. As highlighted in the context of the Romanian administration, many allies rely on "legacy systems" and "cloud private" architectures segregated, on-premise infrastructure that are mandated by national laws for the protection of classified information, such as Romania's strict interpretation of OUG 89/2022 regarding government cloud interoperability (Curtea de Conturi a României, 2023).

This friction was palpably demonstrated during the recent NATO Coalition Warrior Interoperability Exercise (CWIX 25) in Bydgoszcz. While digitally mature allies like the US and UK demonstrated real-time data fusion using cloud-native APIs, detachments from the Eastern Flank often faced a "digital hard stop". Personal observations from the exercise floor revealed that operators were frequently forced to manually bridge the gap between national secure networks and the NATO Mission Secret network. Instead of automated data streams, critical intelligence often had to be moved via "air-gapped" procedures, physically transferring data on secure hard drives, to comply with sovereign data laws.

These legacy systems are often physically incapable of the high-speed data transfer required for centralised AI training. The lack of standardised data labeling and metadata (as required by STANAG 5636) means that even if the political will to share data existed, the technical capability to ingest it is effectively absent (NATO Allied Command Transformation, 2025). This reality creates a "two-speed alliance" where data-rich, digitally mature nations accelerate away from data-poor or digitally distinct allies, fracturing the very interoperability that is the alliance's center of gravity.

3. Techno-diplomacy: the new statecraft of alliance management

To close the gap between the technical reality of the black box and the political reality of data sovereignty, a new form of statecraft is emerging: "techno-diplomacy" (Bano et al., 2024). This practice integrates the technical governance of digital infrastructure with the strategic objectives of foreign policy, acknowledging that in the 21st century, technology standards are the new treaties.

3.1. Defining techno-diplomacy in a defence context

Techno-diplomacy differs from "science diplomacy" (which focuses on scientific cooperation for peace) and "digital diplomacy" (using digital tools for public messaging). It is the strategic negotiation of the rules, norms, and architectures that govern critical technologies. For defence alliances, techno-diplomacy serves three critical functions. The first is normative harmonisation, which involves aligning the ethical and legal frameworks that govern AI use to ensure that allies share a common understanding of "responsible use" (DoD, 2024). The second function is regulatory alignment, which aims to coordinate export controls, investment screening, and certification standards to create a trusted "technology zone" where innovation can flow freely. The third function is architectural consensus, which requires agreeing on the technical designs, such as zero-trust architectures or federated networks, that will underpin shared systems. This shift is visible in the appointment of "Tech Ambassadors" and the restructuring of foreign ministries, such as the US State Department's Bureau of Cyberspace and Digital Policy, to explicitly address the geopolitics of technology (WEF, 2023).

3.2. Institutional vehicles for AI governance

Several key institutions are currently pioneering techno-diplomacy, serving as laboratories for the framework proposed in this paper. NATO's DIANA and Innovation Fund serve as a prime example. The Defense Innovation Accelerator for the North Atlantic (DIANA) establishes a network of test centers and accelerators across the alliance, creating a mechanism for "interoperability by design" (NATO, 2021). It allows a startup in Estonia to validate its AI model on a test range in Portugal, ensuring that the technology is compatible with allied standards from inception. The €1 billion Innovation Fund complements this by providing "sovereign capital", reducing reliance on non-aligned investment and fostering a shared industrial base.

Additionally, the AUKUS partnership (Australia, UK, US) represents a "minilateral" acceleration of techno-diplomacy, particularly through Pillar 2, which focuses specifically on "advanced capabilities" including AI and autonomy (U.S. Department of War, 2026). By negotiating exemptions to strict export controls (like the US ITAR regime), AUKUS partners are creating a "free trade zone" for algorithms and military IP. This demonstrates that smaller, high-trust groups can achieve deeper integration than larger alliances, potentially serving as a pathfinder for broader NATO efforts. The EU-US Trade and Technology Council (TTC) serves as the primary forum for resolving the trans-Atlantic "regulatory gap". With the EU moving towards comprehensive regulation through the AI Act and the US favoring a risk-based, sectoral approach, the TTC works to align on definitions of "trustworthy AI" and coordinate on semiconductor security. This alignment is a prerequisite for military interoperability; without it, US-made military AI might fail to meet European legal certification standards, blocking its deployment in European theaters.

3.3. Project Maven: a model for coalition integration

Operationalising techno-diplomacy is best exemplified by the evolution of Project Maven. Originally a US initiative to automate the analysis of drone video feeds, Maven has evolved into the "Maven Smart System" (MSS), a platform now being extended to coalition partners (Atlantic Council, 2024). MSS acts as a techno-diplomatic bridge: it ingests data from diverse allied sensors, processes it through US-trained algorithms, and shares the insights (the "cognitive output") back to

the allies. This allows partners to benefit from advanced AI without needing to access the black-box algorithm itself or expose their raw data to a central US repository. It is a working prototype of the "Techno-Diplomatic Framework" in action.

4. Technical architectures for sovereign interoperability

While techno-diplomacy provides the political will, "Privacy-Enhancing Technologies" (PETs) provide the technical way. To secure the black box and resolve the data sovereignty crisis, alliances must adopt architectures that enable collaboration without mutual exposure. The framework relies on three specific technologies: Federated Learning, Confidential Computing, and Secure Multi-Party Computation.

4.1. Federated Learning (FL): bringing the code to the data

Federated Learning (FL) fundamentally reverses the traditional paradigm of machine learning. Instead of moving sensitive data to a central server for training an action that often violates sovereignty and classification protocols FL moves the *model* to the data (Gradiant, 2021). In this architecture, a central "aggregator" (e.g., managed by Allied Command Transformation) distributes a baseline AI model to the secure local clouds of participating nations. Each nation trains the model locally on its own classified data, computing only the mathematical updates (gradients) which are then sent back to the aggregator to update the global model.

To operationalise this, consider an Anti-Submarine Warfare (ASW) scenario in the Baltic Sea. A US Navy P-8 Poseidon deployment may arrive with acoustic detection models trained primarily on deep-water Atlantic or Pacific datasets, making them less effective in the shallow, brackish, and acoustically cluttered environment of the Baltic. Under an FL framework, the US model could be sent to a secure Norwegian or German naval cloud. There, it would "learn" from local, high-fidelity sonar logs capturing specific thermal layers and salinity profiles without those raw, highly classified logs ever leaving the host nation's custody.

This mechanism serves as a potent diplomatic enabler. The US P-8 flies with a smarter model that understands the Baltic environment, while the Norwegian Navy contributes to alliance security without violating the "Third Party Rule" or exposing its sensitive acoustic libraries. It resolves the dilemma of collective intelligence by sharing the *mathematical learnings* (the "cognitive output") rather than the raw intelligence itself. Since the central model is exposed to external inputs, FL needs strong safeguards against "model poisoning", which calls for incorporating the next technology: Confidential Computing.

4.2. Confidential computing and trusted execution environments (TEEs)

Confidential Computing protects data in use (Confidential Computing Consortium, 2025). Standard encryption protects data at rest (on disk) and in transit (over the wire), but data must typically be decrypted in memory before a CPU can process it. This "clear text" phase is a vulnerability. TEEs (hardware enclaves such as Intel SGX or AMD TDX) encrypt memory at the hardware level. The AI model and the data are loaded into this enclave and are invisible to both the host operating system and the cloud provider.

For techno-diplomacy, TEEs enable "Zero Trust" collaboration (Anjuna, 2025). A US-developed targeting algorithm can be sent to a Polish server to process local data. The algorithm runs inside a TEE; the Polish operators cannot see the US proprietary code, and the US developers cannot see the Polish raw data. The hardware guarantees the isolation. This allows for the deployment of "black box" systems on allied infrastructure with mathematical guarantees of IP and data security.

4.3. Secure multi-party computation (SMPC)

SMPC allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. Data is split into "secret shares" and distributed among the parties. No single party ever holds the complete data. They perform computations on these shares, and the results are combined to reveal only the final output. This is ideal for "Private Set Intersection" (PSI), allowing intelligence agencies to check if a suspect appears in each other's databases without revealing the broader dataset (Gradiant, 2021). This minimises the "blast radius" of intelligence sharing to the strict "need to know".

5. The techno-diplomatic framework: a proposed architecture

To secure the black box, alliances must integrate these technical enablers into a cohesive governance structure. This paper proposes a three-layered Techno-Diplomatic Framework.

5.1. The normative layer: defining the "Rules of the Road"

This layer establishes the political and ethical boundaries for AI use, building on NATO's Principles of Responsible Use. It begins with a harmonised risk taxonomy in which allies agree on a standard classification of AI risk. The EU AI Act's tiered model serves as a baseline but must be adapted for military contexts; a "NATO AI Risk Standard" should categorize systems based on the consequence of error (e.g., Kinetic-Lethal vs. Logistics-Non-Lethal) to determine the necessary level of TEV&V (Bozkurt et al., 2025). The framework necessitates context-appropriate Meaningful Human Control (MHC). To bridge the gap between US pragmatism and European caution, MHC is defined not as a static "man-in-the-loop" requirement, but as a dynamic variable that scales with risk: high-risk systems, such as Lethal Autonomous Weapons, require strict oversight, while low-risk systems, such as logistics optimisation, allow greater autonomy. Finally, to mitigate the black box trust deficit, allies must agree to share AI Bills of Materials (AI-BOMs). These documents certify the provenance of the training data (e.g., "trained on validated NATO-standard imagery") and the model architecture, providing a "nutrition label" for the algorithm without revealing the proprietary "recipe".

5.2. The technical layer: the federated interoperability backbone

This layer builds the infrastructure for the "Alliance Cloud". The Federated Interoperability Backbone (FIB) is a standing digital infrastructure that connects national AI centers via a secure, federated network. The FIB facilitates the exchange of model updates (via FL) and supports "containerised" deployment of AI capabilities. Critical to this is the adoption of standardised APIs; open, standardised Application Programming Interfaces ensure that an AI module developed by Nation A can plug into Nation B's Command and Control (C2) system, regardless of the underlying legacy hardware. Additionally, metadata standardisation via the full implementation of STANAG 5636 (NATO Core Metadata Specification) is required to ensure data is "AI-ready" and discoverable across the federation (NATO Allied Command Transformation, 2025).

5.3. The operational layer: continuous assurance

Trust must be continuously validated through rigorous testing. First, the alliance must expand on DIANA to create Joint AI Proving Grounds, acting as "sandboxes" where allies can red-team each other's models. These environments enable adversarial testing (e.g., attempts to spoof a vision system) to verify robustness before deployment (Atlantic Council, 2024). Second, to address the explainability gap in real time, the framework proposes deploying "Observer" modules alongside black-box systems. These are simple, rule-based AI agents that monitor the inputs and outputs of the complex model. If the black box suggests an action that violates a defined Rule of Engagement (e.g., targeting a protected site), the Observer acts as a "circuit breaker", flagging the decision for human review.

5.4. Limitations and technical challenges

While the Techno-Diplomatic Framework offers a path toward cognitive interoperability, its implementation faces significant technical and environmental hurdles. A primary limitation is the communication overhead associated with Federated Learning. In contested or degraded tactical environments, the high bandwidth required to continuously transmit model gradients between national clouds and an alliance aggregator can lead to significant latency, potentially desynchronising the collective intelligence. While Trusted Execution Environments (TEEs) provide hardware-level isolation, they are not immune to sophisticated side-channel attacks that may attempt to infer proprietary code or data through power consumption or timing analysis.

Additionally, the framework assumes digital maturity across all member states. The "two-speed alliance" problem remains a critical risk; nations relying on disconnected legacy systems may find themselves unable to participate in the Federated Interoperability Backbone, regardless of the diplomatic will to do so. Finally, the move toward "Zero Trust" collaboration via encryption and TEEs can complicate digital forensics and post-incident auditing. If an AI-driven decision leads to an unintended kinetic outcome, the very technologies used to protect sovereign data may make it more difficult for an alliance to conduct a transparent investigation into the algorithmic failure.

Conclusions

The integration of Artificial Intelligence into defence alliances is not a distant future; it is a current reality that demands a sophisticated response. The "black box" problem represents a critical vulnerability in this transition, threatening to fracture alliance cohesion through mistrust and operational paralysis. As this paper has demonstrated, the challenge is surmountable through the application of a Techno-Diplomatic Framework. By fusing the normative power of diplomacy with the architectural guarantees of Federated Learning and Confidential Computing, alliances can shift from a "need to know" to a "need to share" posture without compromising sovereignty. The shift from "hardware interoperability" (STANAGs) to "cognitive interoperability" (shared models and norms) is the defining task for the next decade of collective defence. The success of this framework depends on alliance leaders' willingness to engage with the technical nuances of AI and on technologists' willingness to design for diplomatic constraints. If successful, this approach will not only secure the black box, but also ensure the black box remains secure. But in the end, it will become the foundation of a stronger, smarter, and more united alliance that is well-equipped to face the complex challenges of the 21st century.

BIBLIOGRAPHY:

Anjuna. 2025. U.S. Navy charters secure AI course with confidential computing. https://www.anjuna.io/case-studies/united-states-navy

Atlantic Council. 2024. *A marketplace for mission-ready AI: Accelerating capability delivery to the Pentagon* (Strategic Insights Memo). https://www.atlanticcouncil.org/content-series/strategic-insights-memos/a-marketplace-for-mission-ready-ai-accelerating-capability-delivery-to-the-pentagon/

Bano, M., Chaudhri, I., & Zowghi, D. 2024. *Diplomacy in the age of generative AI* (arXiv:2401.05415). arXiv. https://doi.org/10.48550/arXiv.2401.05415

Belfer Center for Science and International Affairs. (2025, March 21). *Boosting interoperability of joint forces with AI: A unified language for joint warfighting*. https://www.belfercenter.org/research-analysis/boosting-interoperability-joint-forces-ai-unified-language-joint-warfighting

Bozkurt, M., Saylam, S., Saylam, R., & Gündoğdu, F. K. (2025, August 6). *Risk assessment of artificial intelligence support in the command and control cycle using spherical fuzzy z-number best-worst decision-making method*. NATO C2COE. https://c2coe.org/risk-assessment-of-ai-in-c2/

Confidential Computing Consortium. (2025). *Confidential computing: The future of data security*. https://confidentialcomputing.io/wp-content/uploads/sites/10/2025/11/US53866125.pdf

Curtea de Conturi a României. (2023). *Raport privind digitalizarea administrației publice* [Report on the digitization of public administration].

DefenseScoop. 2025, November 12. *Too much data, too few analysts: How AI offers a 'force multiplier' for intelligence analysts*. https://defensescoop.com/2025/11/12/too-much-data-too-few-analysts-how-ai-offers-a-force-multiplier-for-intelligence-analysts/

Department of Defense. (2024). *Responsible AI strategy and implementation pathway*. https://media.defense.gov/2024/Oct/26/2003571790/-1/-1/0/2024-06-RAI-STRATEGY-IMPLEMENTATION-PATHWAY.PDF

European Parliamentary Research Service. 2025. *Artificial intelligence in the military: Opportunities and challenges* (Briefing No. 769580). https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf

Gradiant. 2021. *Federated learning and secure multi-party computation: A powerful alliance for pri vacy-preserving AI*. https://gradiant.org/en/blog/trumpet-federated-learning-computation-secure/

Hadean. (2025). *Interoperability at the edge: The strategic imperative for NATO in an era of complex threats*. https://hadean.com/blog/interoperability-at-the-edge-the-strategic-imperative-for-nato-in-an-era-of-complex-threats/

Jensen, B., & Mishra, B. 2025. *Code, command, and conflict: Charting the future of military AI*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/research-analysis/code-command-and-conflict-charting-future-military-ai

NATO. 2021. *Summary of the NATO artificial intelligence strategy*. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy

NATO. 2024. *Summary of NATO's revised artificial intelligence (AI) strategy*. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

NATO. 2025. *Data strategy for the alliance*. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/05/05/data-strategy-for-the-alliance

NATO Allied Command Transformation. (2025, June 23). *CWIX 25 concludes*. https://www.act.nato.int/article/cwix25-concludes/

Pollard, M. 2024. *Autonomous weapons systems and the inherent right of self-defense* [Doctoral dissertation, University of Buckingham]. http://bear.buckingham.ac.uk/624/1/1404758%20Michael%20Pollard%20Final%20Thesis.pdf

Reynolds, I., & Atalan, Y. 2024, July 8. *Calibrating NATO's vision of AI-enabled decision support*. Center for Strategic and International Studies.
https://www.csis.org/analysis/calibrating-natos-vision-ai-enabled-decision-support

Scaleout Systems. 2025. *Defense and security: Secure intelligence for mission-critical applications*. https://www.scaleoutsystems.com/defense-and-security

Sullivan, A., & Ricket, T. 2024. The black-box problem in AI-based weapon systems. In *CyCon 2024*. NATO CCDCOE. https://ccdcoe.org/uploads/2024/05/CyCon_2024_Sullivan_Ricket-1.pdf

U.S. Department of War. (2026, January 12). *Artificial intelligence acceleration strategy*. https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF

World Economic Forum. (2023, February). What is tech diplomacy? Experts explain. https://www.weforum.org/stories/2023/02/what-is-tech-diplomacy-experts-explain/

Centre for Defence and Security Strategic Studies &
Interdisciplinary Doctoral School,
"Carol I" National Defence University

DOI: 10.53477/3045-2309-26-15

TWO PARADIGMS OF ALGORITHMIC SECURITY GOVERNANCE: CENTRALISED INTEGRATION AND INTEROPERABLE FRAMEWORKS IN THE USE OF AI FOR STATE SECURITY

Mara-Mihaela MEREANU
Student, Babeș-Bolyai University, Cluj-Napoca, Romania,
Scholar at Shanghai Jiao Tong University, Shanghai, China
E-mail address: mara.mereanu@yahoo.com

Abstract*: Artificial intelligence (AI) plays an increasingly important role in counterterrorism by enabling the rapid processing of large volumes of data and the identification of patterns, anomalous behaviours, and emerging risks. This article examines two paradigms of algorithmic security: the centralised Chinese model and the decentralised, interoperable Israeli model. Adopting a comparative and primarily descriptive approach, the study draws on academic literature, policy documents, and native authors to analyse how AI is embedded within different institutional architectures A brief case study of the 2019 Hong Kong protests examines how predictive technologies were deployed in an urban context officially framed as a matter of security and public order. The analysis shows that the strategic impact of AI depends less on technological sophistication alone and more on governance structures, institutional coordination, and legal frameworks. The study also acknowledges limitations related to restricted data access and the evolving nature of AI-driven security systems.*

Keywords*: Artificial intelligence; counterterrorism; digital surveillance; large language models; national security.*

Introduction

In the past few decades, artificial intelligence (AI) has begun playing an increasingly important role in the field of security and counterterrorism. In the past, data analysis was a slow process that was also fully reliant on human resources, but nowadays the new era of AI technology allows high-speed processing of large quantities of data, thus significantly changing the way both state and non-state actors manage their threats. Through the ability to identify patterns, correlations and atypical behaviours, AI systems provide authorities with additional tools to anticipate risks and implement preventive interventions. In many situations, the response to critical incidents is no longer just reactive, but can be based on predictive analytics, which substantially changes the traditional logic of security management.

By comparing the way in which the states and the violent non-state groups are implementing the use of AI, we can observe a few key elements that are influencing both operational efficiency and strategic stability. Overall, the focus is not confined to equipment and technological infrastructure, or even to the quantity of collected data, but also expands to the way institutions work together, the existing legal framework and coordination mechanisms between security agencies.

In this regard, China represents a particularly relevant case, given how it integrated AI both in a very systematic way and on a multitude of levels. Thus, the state, intelligence agencies, and the technology sector work closely together. Chinese systems combine multi-source data analysis, predictive tools, and digital surveillance, all under the umbrella of centralised governance that aims to prevent, control, and anticipate asymmetric threats.

1. The Chinese model of integrating AI into security and counterterrorism

China is often viewed (Mereanu și Mereanu 2025)as an example when discussing the extensive integration of artificial intelligence into security and counterterrorism. What distinguishes this model is the high degree of coordination between the state, intelligence agencies, and technology companies, which operate within a centralised and well-structured framework. From this perspective, the use of AI in China can be interpreted as part of a broader state-led approach to national security governance rather than as a set of isolated initiatives. Official policy documents present these applications as serving the dual purpose of maintaining internal order and preventing threats, framing them within an integrated vision of risk management.

In practice, the Chinese model involves combining predictive tools, data analysis from various sources, digital surveillance and the use of algorithms capable of identifying behaviours considered atypical or potentially risky. Technology is not treated only as technical support, but as part of the security decision-making mechanism. Thus, AI becomes an integrated element in the process of anticipating and managing threats, both internal and external. (Weber 2025)

In the Chinese security system, the People's Liberation Army (PLA) plays the main role as the armed force of the People's Republic of China. In addition to its traditional duties related to the protection of sovereignty, the PLA has responsibilities in the field of cybersecurity and provides support in the management of internal and external crises. The Ministry of State Security (MSS), on the other hand, functions as the central intelligence and counterintelligence agency. Its activities include monitoring internal and external threats, coordinating anti-terrorist operations, and using digital analysis and Social Media Intelligence (SOCMINT) in situations with an impact on national security. Complementarily, the Ministry of Public Security (MPS) acts as a law enforcement and domestic oversight institution. Although it is not an intelligence agency in the classical sense, the MPS has an important role in combating terrorism, maintaining public order, and monitoring organised crime. In addition, the ministry manages cybersecurity and digital space monitoring, using SOCMINT tools to prevent domestic risks and identify potential threats to social stability. The MPS also manages a vast network of nationwide video surveillance cameras, integrated with local facial recognition systems, which allows it to respond quickly to various security situations. These functions are frequently associated with the "weiwen" (维稳) paradigm – commonly translated as "maintenance of social stability" – which is described in the literature as a central component of China's domestic security (Jun 2010, 29-34).

Thus, by collaborating, the MSS and the MPS practically form the civilian core of China's intelligence system. They work closely with the PLA's military structures, under the coordination of the Communist Party's Central Commission for Political and Legal Affairs, which allows them to maintain a coherent strategy and react quickly in critical situations.

Besides managing security infrastructures, these institutions also tend to function as integration centres for emerging technologies. They coordinate the implementation of predictive systems, advanced behavioural analysis models, and digital surveillance platforms. Given this background, data and algorithms no longer remain just information, thereby functioning as concrete operational tools, capable of supporting the prevention, anticipation, and strategic control of risks. In this context, AI plays a role of efficiency that is difficult to match in other international contexts. A centralised architecture may facilitate the concentration of information flows, reduce institutional fragmentation, and accelerate decision-making processes. In contrast, many Western governance models are characterised by institutional pluralism and divided competences, which can introduce additional procedural constraints. These differences illustrate distinct approaches to integrating AI not only at a technical level but also within broader institutional frameworks.

China has invested significantly in the development and refinement of large language models (LLMs) and advanced machine learning algorithms, integrating them into a coherent multi-source analysis framework. These technologies allow for the simultaneous processing of data from a wide

variety of sources – public information, internal government streams, social media data, and other digital signals – creating a system capable of identifying and preventing terrorist threats, both domestically and internationally. LLMs are not only used for natural language interpretation; they also help uncover complex patterns in social interactions or networks considered at risk of destabilisation, providing authorities with a valuable tool for proactively assessing emerging risks. Furthermore, this analytical infrastructure is reliant on an extended network of international collaboration. China is pooling and integrating data streams with multinational security structures, including those dedicated to counterterrorism. Through the development of advanced tools, authorities are able to generate rapid and robust assessments that allow them to make informed strategic decisions and effectively coordinate operations at a multilateral level. In addition, Beijing seeks to harmonise international standards and best practices, which regulate the anti-terrorism legislative framework, investigative procedures and the protection of critical infrastructures, so that operational efficiency is complementary to respect for fundamental human rights (Mereanu and Mereanu 2025, 27-35).

China's approach is based on an integrated and well-structured governance, in which technology plays a central role in institutional coherence and in strengthening the capacity for rapid response. Large language models (LLMs) are used in an extensive system that includes behavioural analysis, anomaly detection algorithms and predictive digital infrastructures, all directly connected to the state's decision-making processes. Thus, AI does not remain just a technical tool, but becomes an essential structural component in the prevention, monitoring and management of asymmetric threats. (Weber 2025)

Through these mechanisms, China is strengthening its position both operationally and strategically. The combined use of LLMs and multi-source analytics transforms enormous amounts of data into real operational capabilities, facilitating active prevention, reducing uncertainty, and optimising decisions at the international level. This multi-dimensional integration reflects a holistic vision of security, in which emerging technologies and centralised governance complement each other, creating a proactive, coherent, and adaptable prevention model to the complexity of global threats. (Mereanu și Mereanu 2025)

In China's security and counterterrorism strategies, artificial intelligence is widely used in regions with ''ethnically sensitive populations'', such as Xinjiang (The State Council Information Office of the People's Republic of China 2019) and Tibet, but also in other autonomous regions, including Gansu and Qinghai provinces. Here, AI is integrated into a comprehensive surveillance system that combines facial recognition, real-time video monitoring, behavioural analysis, and risk-predicting algorithms.

These tools are described in official discourse as mechanisms for identifying behavioural patterns associated with radicalisation, extremism, or social instability. Proponents argue that such systems can enhance anticipatory risk assessment, assist in the allocation of response resources, and contribute to a more proactive model of security governance. Integrated technologies, including LLMs and multi-source analytics platforms, transform data collected from public sources, internal government streams, and digital communications into concrete operational tools. In this way, surveillance becomes more than a simple response to events; it takes on a proactive and strategic role, enabling the state to identify emerging threats and intervene before they materialize into real risks. (Weber 2025)

Conversely, the urban environment presents specific challenges and opportunities for the application of AI in internal security. Large cities such as Beijing, Shanghai or Chengdu, with high population density and extensive digital connectivity, are integrated into advanced intelligent surveillance systems (Jun 2010). These systems combine facial recognition, real-time video analysis, traffic flow monitoring and online data analysis. In this context, the use of AI is not limited to combating terrorism

itself but also aims to manage the risks related to online radicalisation, disinformation, information manipulation and the rapid mobilisation of social groups.

The 2019 protests in Hong Kong are widely regarded as a significant episode in the evolution of urban security governance. The scale, organisation, and persistence of the demonstrations highlighted potential limitations of predominantly reactive law enforcement models, which rely on physical deployment and post-event intervention. In response, there was an increased emphasis on the development of more technologically integrated systems capable of analysing social, informational, and spatial dynamics in real time to support the anticipation and management of potential escalations.

In the past, social mobilisations relied on community networks built over years, making them difficult to suppress. Today, however, unprecedented connectivity allows people to organise spontaneously – but also gives authorities the tools to track them accurately. As HoFung Hung, a professor at Johns Hopkins University, observed, "it's a double-edged sword": technology can support solidarity and coordination among participants, but it can also be used just as effectively for control and surveillance (Wong 2023). In this context, the Chinese authorities have begun to integrate predictive technologies, multi-source analysis platforms and Social Media Intelligence (SOCMINT) tools. These allow the simultaneous monitoring of online mobilisation, information flows and physical concentrations of people, providing concrete data for planning interventions and preventing the escalation of conflicts. However, these measures also raise numerous concerns at the international level, related to fundamental rights, the transparency of algorithmic decisions and the risk of digital discrimination. From the perspective of the authorities, however, the technologies are seen as preventive tools – intended to ensure regional stability and protection against asymmetric threats – in a vision of security in which prevention always takes precedence over reaction after the incident.

The Hong Kong protests illustrate how contested political events may contribute to shifts in state approaches to urban security governance. Artificial intelligence is no longer just a technical tool – it is becoming an integrative or coordinating mechanism between institutions, helping authorities to react quickly and understand in real time what is happening on the streets or in the digital environment. Advanced language models, behavioural analysis and anomaly detection algorithms work together, directly linked to the state's decision-making processes, transforming enormous volumes of data into concrete actions. In this way, prevention, monitoring and immediate response to threats become operational realities, not just theoretical concepts.

The Chinese case reflects a centralised governance structure in which digital technologies are integrated into state-articulated security strategies. By comparison, countries such as Israel, the United Kingdom, and the United States employ more decentralised institutional arrangements, involving multiple agencies and legal frameworks that regulate the use of surveillance and algorithmic decision-making tools. Looking at these models in parallel, we can see both the advantages and limitations of each approach. They show us how much the institutional structure and legal framework matter when it comes to the effectiveness and legitimacy of using emerging technologies in security and counterterrorism. The use of AI cannot be reduced solely to the idea of technological advancement; it is also reflected in the way the state employs it to prevent crises and maintain social stability.

2. Using artificial intelligence in security and counterterrorism

Israel is a distinct example of advanced integration of AI into national security, combining leading military capabilities, a highly active private technology sector, and an institutional culture focused on rapid innovation and adaptability in the field. In contrast to the Chinese model, which is based on centralisation and hierarchical governance, the Israeli approach focuses on flexible interoperability between intelligence

agencies, the military, and technology companies, with an emphasis on the immediate application of technologies in real-world operational situations.

A key pillar of this ecosystem is Unit 8200, the military intelligence structure of the Israel Defense Forces (IDF), responsible for collecting and analysing SIGINT information and conducting cyber operations. (Farhat 2025) Within the Israeli security architecture, the unit plays a central role in information warfare and in exploiting digital flows relevant to the operational environment (Farhat 2025). In recent years, according to press investigations, Unit 8200 has developed and trained large language models (LLMs) on considerable volumes of Arabic-language data, originating from intercepted communications, text messages and other digital sources, in order to improve analytical capabilities (Heller 2025).

These language models enable accelerated processing of large volumes of raw information, facilitating the identification of recurring patterns, the correlation of data from multiple sources, and the extraction of relevant clues for operational analysis (Heller 2025). Their integration into platforms that combine HUMINT, SIGINT, and other information flows contributes to the formation of a more coherent operational picture and the support of timely decision-making (Farhat 2025). In this sense, artificial intelligence functions as a multiplier of human analytical capacity, optimising the information cycle – from collection and sorting to evaluation and dissemination.

In parallel, the use of analysis algorithms and tools based on machine learning has also expanded in support of military operations, including in the process of identifying and prioritizing targets, as evidenced by discussions on the "Gospel" system and other similar applications (Heller 2025). These developments indicate an increasingly pronounced integration of AI technologies into operational planning and execution processes.

Compared to China, where the integration of artificial intelligence and generative models is subsumed under a highly centralised institutional architecture, Israel operates in a more fragmented framework but characterised by intense interaction between the public and private sectors.

A significant part of the Israeli technological ecosystem is fuelled by former members of Unit 8200, who, after completing their military service, established start-ups with a cyber and AI profile (Heller 2025). This innovation circuit allows for the relatively rapid transfer of solutions developed in the civilian environment to applications relevant to national security, reducing the distance between research and operational implementation.

At the same time, the expansion of the use of artificial intelligence in the security field is accompanied by debates on the ethical and legal implications of these technologies, especially regarding surveillance, data protection and the risk of algorithmic errors in sensitive contexts. While in the Chinese model the legitimacy of AI use is anchored predominantly in the discourse of stability and collective security, in Israel emerging technologies are subject to more visible public and legal scrutiny, even if the security imperative remains a determining factor in the policies adopted.

Overall, the Israeli case illustrates a model of integrating artificial intelligence into the fight against terrorism based on institutional agility, interoperability and accelerated innovation. In parallel, the comparison with the Chinese model highlights two different logics of organising the relationship between state, technology and security: one focused on centralisation and systemic integration, the other on flexibility and the dynamics of the technological ecosystem.

Conclusions

The comparative analysis of China and Israel suggests that artificial intelligence increasingly occupies a structurally significant position within contemporary security governance, extending beyond a merely supportive technological function. AI enhances the capacity to manage vast quantities of data, identify patterns, and assist in making predictions. This transformation shifts

counterterrorism from a primarily reactive approach to one that emphasises anticipation and prevention of attacks.

The previously explored aspects also show that the strategies will not necessarily work better just because technology gets better since the effects of AI depend a lot on the rules and structures of the organisations that use it. China's centralised government model enables the integration of systems, the management of vast populations, and the rapid implementation of predictive and surveillance infrastructures. In contrast, Israel works in a more decentralised but highly interoperable ecosystem where military, intelligence, and private-sector actors work together closely to shape the practical use of AI. These two approaches differ in their configurations, yet they both emphasise a common principle: the strategic advantage of AI arises from the effectiveness of collaboration and governance among institutions, rather than solely from the capabilities of the technology itself.

Nonetheless, the emergence of AI-driven counterterrorism brings forth numerous ethical dilemmas. As predictive analytics and algorithmic systems gain prominence in decision-making, the demand for transparency, accountability, proportionality, and the safeguarding of fundamental rights intensifies. Finding the appropriate balance between security requirements and civil liberties remains a significant consideration in determining the legality and longevity of these models.

In conclusion, artificial intelligence represents more than merely a novel technology; it fundamentally alters how nations perceive and manage security in the digital era. Its role in combating terrorism is set to expand, yet its effectiveness and ethical implications will hinge on the legal frameworks, institutions, and moral principles that regulate its application.

BIBLIOGRAPHY:

Farhat, Jawhar. 2025. *Unit 8200: Israel's Information Warfare Unit.* 03 12. Accessed 02 17, 2026. https://greydynamics.com/unit-8200-israels-information-warfare-unit/

Heller, Mathilda. 2025. "Unit 8200 created AI language learning tool from intercepted Palestinian Arabic comms - report." *The Jerusalem Post.* Accessed 02 12, 2026. https://www.jpost.com/israel-news/article-845128.

Jun, Tang. 2010. "A Study of Risk Administration in Maintenance of Social Stability." *Teaching and Research* 29-34. http://jxyyj.ruc.edu.cn/CN/Y2010/V/I5/29.

Mereanu, Vitia, and Mara Mereanu. 2025. "Strategia Chinei în combaterea terorismului: abordare holistică, cooperare internațională și utilizarea tehnologiilor avansate." *The European Union and the New Dynamic of Global Security* 27-35.

The State Council Information Office of the People's Republic of China. 2019. "Fan kongbu zhuyi he jiduan zhuyi yu renquan baozhang (Xinjiang)." *www.gov.cn.* Accessed 10 18, 2025. https://english.www.gov.cn/archive/white_paper/2019/03/18/content_281476567813306.htm

Wong, Tessa. 2023. *BBC NEWS*. 03 26. Accessed 02 12, 2026. https://www.bbc.com/news/world-asia-64300442

DOI: 10.53477/3045-2309-26-16

THE RISE OF NAVAL DRONES AND THE REDEFINITION OF THE MARITIME BATTLESPACE

Adrian NIȚĂ,
Commander, PhD Student, Doctoral School of Engineering Sciences,
Advisor, Euro-Atlantic Resilience Centre (E-ARC) Bucharest, Romania,
E-mail address: adrian.nita@e-arc.ro

Abstract*: Throughout the last century, naval power has relied on capital ships requiring years of design and billions in investment. This paradigm now faces unprecedented pressure from Unmanned Surface Vessels (USVs), commonly known as naval drones. The present paper aims to analyse how naval drones redefine the maritime battlespace in semi-enclosed seas and to derive implications for Romania's resilience in the Black Sea. The main objectives are: to trace the historical cycles of technological disruption in naval warfare, to examine the Black Sea as a live laboratory of naval drone employment, to extract lessons for similar theatres such as the Baltic Sea and the Taiwan Strait, and to develop a three-layer defence architecture for protecting critical maritime infrastructure such as the Neptun Deep project. Methodologically, the paper combines historical-comparative analysis, case studies (Ukraine, Baltic Sea, Taiwan), and doctrinal/strategic document review, integrated through a resilience-oriented analytical lens. The novelty of the study lies in linking operational-tactical drone employment with a concrete and scalable defence proposal for a NATO/EU coastal state whose Exclusive Economic Zone is outside the formal guarantees of Article 5. The expected outcome is a conceptual model of autonomous, multi-layered defence that can inform both Romanian and allied approaches to security in the Black Sea.*

Keywords*: naval drones; unmanned surface vessels (USV); Black Sea conflict; asymmetric warfare; maritime defence; Neptun Deep; autonomous defence architecture.*

Introduction

Throughout naval history in the last century, command of the seas has relied on the size, range, and survivability of fleets composed of destroyers, cruisers, and aircraft carriers. These capital ships, often requiring years of design and billions of dollars in investment, symbolise both military and political power. However, this paradigm is now under unprecedented pressure with the rapid emergence of Unmanned Surface Vessels (USV), often referred to as naval drones.

Initially developed as cheap, expendable reconnaissance platforms suitable for shallow or contested waters, USVs have rapidly evolved into armed systems capable of executing precision attacks. Equipped with explosive payloads, navigation sensors, and remote control links, they can penetrate defences and threaten ships of much higher value. Results observed in recent years, particularly in the Black Sea, signal not just a major improvement, but a paradigm shift in naval warfare, where cost asymmetry favours the attacker.

The conflict in the Black Sea transformed Ukraine, left without a naval fleet after the annexation of the Crimean Peninsula and the 2022 invasion, into a pioneer of asymmetric warfare with drones like Magura V5 and Sea Baby. These platforms struck major Russian ships, broke the grain blockade, and contributed to the retreat of the Russian fleet, demonstrating how swarms of small drones can saturate expensive defences and reverse the strategic balance.

The phenomenon transcends the Black Sea, offering lessons for similar theatres such as the Baltic Sea or the Taiwan Strait, where semi-enclosed geography amplifies the efficiency of

autonomous drones. Russia, China, the USA, Sweden, Türkiye, Australia, and others are investing massively in USVs, UUVs (unmanned underwater vehicles), and next-generation submarines, recognising that the naval future means distributed networks, not isolated ships.

Romania could transform this threat into a strategic advantage by adopting a multi-layered defence inspired by Ukrainian lessons: swarms of light USVs for continuous surveillance, autonomous interceptors with kinetic weaponry, and reactive mines designed to neutralise attacks, integrated into multi-domain operations (MDO, coordinated with aerial and terrestrial drone systems. An industrial partnership with neighbouring and partner countries, based on expertise in autonomous robotic systems and the capabilities of the Constanța-Mangalia shipyards, would generate 50-100 USVs annually. Such an initiative could be financed by revenues generated by the Neptun Deep project, complemented by EU/NATO funding mechanisms. In this way, Romania could transition from a vulnerable target into a regional provider of maritime security. This approach would ensure the protection of energy independence while redefining the role of the Black Sea as a bastion of European resilience.

This paper pursues four main objectives: (1) to place naval drones within the longer historical cycles of technological disruption in maritime warfare; (2) to analyse the Black Sea as a recent laboratory where Ukraine has operationalised USVs under conditions of conventional naval inferiority; (3) to extrapolate applicable lessons for other semi-enclosed theatres, notably the Baltic Sea and the Taiwan Strait; and (4) to propose a three-layer defence architecture for Romania aimed at protecting critical offshore infrastructure in a high-threat, hybrid environment. To achieve these objectives, the research employs a qualitative methodology based on historical-comparative analysis, open-source case studies, and the examination of official strategic documents and expert literature, interpreted through the conceptual lens of resilience and multi-domain operations. The study is structured as follows: Chapter 1 reviews past technological disruptions at sea; Chapter 2 analyses Ukrainian naval drone employment in the Black Sea; Chapter 3 develops parallels with the Baltic Sea and the Taiwan Strait; Chapter 4 synthesises the tactical-operational advantages of USVs; Chapter 5 presents Russia's response and selected Western countermeasures; Chapter 6 focuses on Romania's military and diplomatic response, with emphasis on a proposed three-layer defence model; the final chapter summarises the main findings and policy-relevant conclusions.

1. Historical Foundation: Cycles of Technological Disruption

For over a century, the balance of naval power has been based on the strength of capital ships - battleships, aircraft carriers, submarines, and missile destroyers. Each era was defined by a dominant platform that seemed unassailable, only to be ultimately replaced by a disruptive newcomer. The battleship sparked an arms race but was eclipsed by the aircraft carrier within a few decades. Submarines, initially viewed with scepticism, became critically important elements, threatening to sever transatlantic supply lines in both world wars. Guided missiles extended lethal range and reconfigured tactics during the Cold War, forcing naval forces to distribute risk across multiple escort ships rather than concentrating it in a few powerful vessels (Till 2018).

What unites these historical changes is the rhythm of paradigm rupture: fleets optimised for a particular paradigm are destabilised by an emerging technology that renders older investments insecure. Within this historical continuum, the rise of unmanned surface vehicles (USVs), popularly known as naval drones, represents more an echo of transformations than an abrupt break from the past. Just as submarines reshaped perceptions of invisibility, and aircraft carriers extended the battlespace vertically into the air, USVs embody a horizontal dispersion of power across cheap, expendable, yet adaptable vessels. Their emergence reflects both a military necessity and a technological opportunity.

The concept of uncrewed vessels is older than often assumed, with variants similar to contemporary designs emerged during both world wars, when engineers tested radio- and wire-guided boats packed with explosives, attempting to steer them toward port defences or anchored fleets.

(Osgood 2021) Rudimentary transmitters and short control ranges doomed most attempts, but they demonstrated the feasibility of delegating high-risk missions to uncrewed surrogates. The Cold War period brought gradual refinement: remotely operated vehicles, often tethered by cable or semi-autonomous, cleared naval mines, conducted near-shore reconnaissance, or simulated hostile targets during training. Like their aerial counterparts of that era - small target drones or reconnaissance prototypes - they occupied the periphery of warfare, proving useful but not decisive, and rarely integrated into doctrine.

By the end of the 20th century, three foundational pillars redefined the horizon: the precision of global positioning systems (GPS), the miniaturisation of optics and sensors, and digital communication links capable of reliably transmitting data through secure channels. These convergent technologies enabled small surface vessels to patrol independently, conduct intelligence-gathering missions, and transmit real-time local situational awareness. Initially, USVs resembled the UAVs of the 1990s: eyes in the sky - or, in this case, eyes on the water. Their strategic contribution remained modest, but the foundations of evolution were laid (Till 2018).

Armament inevitably followed. It was a short conceptual step from a reconnaissance hull carrying cameras to an expendable vehicle armed with an explosive payload. Where naval mines had long represented static threats, and torpedoes lacked the ability to loiter near targets for extended periods or self-guide over long distances, naval drones became mobile and intelligent equivalents - navigating autonomously to targets, adapting to defence systems, and evading interception. The design, combined with their low radar profile allowing surface navigation, posed a new challenge for defence systems optimised against aircraft or missiles, not swarms of small attack boats coordinating in fleets.

This shift fundamentally altered the cost calculus in naval warfare. A billion-euro frigate, laden with radars and defensive systems, might be forced to expend multiple million-euro missiles to destroy fast-moving attackers costing only a fraction of its value. This exchange asymmetry is precisely what made naval drones a disruptive power tool. Their expendable nature is not a limitation but an advantage - inverting the traditional logic that survivability is the primary attribute of naval design (Seligman and Berg 2023).

2. Black Sea: The Naval Drones Laboratory

The ongoing conflict in the Black Sea has provided the most visible demonstration. Ukrainian naval drones Magura V5 and Sea Baby have successfully struck Russian warships and strategic port facilities. These attacks demonstrate how vessels costing just tens or hundreds of thousands of euros/dollars can impose strategic costs far exceeding their price (Knickerbocker 2024).

Naval drones excel by exploiting gaps in conventional naval doctrine. Traditional ships rely on layered defence systems - radars, missiles, close-in weapon systems - optimised to defend against aircraft and manned vessels. However, small USVs, with low profiles and high speeds, are difficult to detect until they close to dangerously short ranges. Defending against a single drone is feasible; countering swarms of dozens arriving simultaneously from multiple angles presents a far more complex challenge. The psychological effect is also significant. Crews operating in contested waters now face persistent uncertainty, where any radar blip or fast boat could conceal a lethal drone. This constant threat reshapes operational behaviour, forcing ships to maintain distance or maximum alert status, reducing their effectiveness.

What makes the Black Sea unique as a framework for this transformation is its enclosed and semi-enclosed geography. Bordered by NATO members on one side and Russia on the other, the sea has historically served as a strategic buffer zone, with access strictly regulated by the Montreux Convention. This limited arena amplifies the effects of each attack, as there is little space for fleets to manoeuvre beyond detection range and reduced capacity to rapidly replace destroyed units.

The 1997 Treaty on the Status and Conditions of the Black Sea Fleet officially ended the dispute between Ukraine and Russia over the former Soviet Black Sea Fleet. Russia received

approximately 81.7% of the fleet's assets, while Ukraine received coastal infrastructure and 18.3% of the fleet, consisting of over 40 warships, approximately 100 support vessels, and significant shipbuilding capabilities. Ukraine agreed to lease naval facilities in Crimea to Russia for 20 years (until 2017), receiving approximately $97 million annually. A supplementary agreement, the Kharkiv Pact (2010), extended the lease until 2042 in exchange for discounts on Russian gas. For Russia, the Black Sea Fleet became the principal element of regional influence and coercion, aimed at controlling commercial and military traffic in the area (United Nations 1997).

For Ukraine, early 2014 brought a major blow to its territorial integrity following Russia's annexation of Crimea. Due to disputes over the price and payment of gas supplied by Moscow, as well as Russian nationalist claims viewing this majority - Russian population territory as part of the federation, an army of "little green men"/"flagless" soldiers executed a special annexation mission. Following this event, Russia began strictly controlling Ukrainian vessels' access to ports within the Sea of Azov and around the peninsula. In the subsequent years, Russian pressures became increasingly evident through the fleet's total superiority over naval traffic, with Crimea increasingly becoming an outpost for electronic warfare and aerial intimidation. In 2018, three Ukrainian ships were attacked and detained in the Kerch Strait area (International Tribunal for the Law of the Sea 2019). Movement restrictions across the entire Ukrainian coastal area made access to offshore drilling facilities impossible, further damaging the economy. The surprise launch of the 2022 attack took out the last significant ships, rendering Ukraine's naval forces irrelevant from the perspective of classical confrontation.

However, precisely this situation led to the discovery of alternative naval combat solutions. As the dominance of large Russian ships left no room for classical confrontation, Ukrainians saw maritime drones and coastal anti-ship missiles as the only method to rebalance the complicated combat situation in the Black Sea area. Once the possibility was discovered to use a Starlink terminal mounted on an aerial drone to establish long-distance communication, the idea emerged of using this system as a communication method on an explosive-laden boat to destroy Russian ships. Thus, Commander Oleksii Neizhpapa selected a small group of experts to support the maritime drone project. Their main role was to assist with calculations and, above all, to train drone operators in sea navigation, including in storm conditions and using old pilotage charts.

In June 2022, the first prototype - a standard motorboat with a Starlink system - that was constructed and successfully tested. By September 2022, the first drone team was operational and directed toward Sevastopol. The initial mission, however, failed due to the interruption of communications via Starlink satellites. This experience highlighted the necessity for multiple communication channels, and new models were equipped with three interconnected systems (Romaniuk 2024).

The night of 28-29 October 2022 marked the key moment of the first successful operation. Rain had subsided and sea conditions were favourable, allowing the modified drones to be deployed. Four drones were launched toward Sevastopol, while three others headed toward the southern peninsula where the frigate Admiral Makarov - the flagship of the Russian Black Sea Fleet following the sinking of the cruiser Moskva - was located. A Ukrainian drone successfully struck the ship's starboard side. The surprised crew attempted chaotic manoeuvres toward Sevastopol Bay. Two other drones pursued the frigate nearly to shore, though large waves prevented direct contact. The impact was serious - the ship was disabled.

Meanwhile, other drones penetrated Striletska Bay, but there an alarm was raised, a massive spotlight was used to target them, and they were countered. A Russian minesweeper, Ivan Golubets, appeared on an operator's screen, and the drones were ordered to destroy it with 108 kilograms of explosives. Other drones struck an oil facility in the area. In the confusion, Russian artillery also fired on its own flagship, resulting in friendly fire. Meanwhile, the remaining drones entered Sevastopol Bay. This may have been the first remote naval drone operation in modern history, and based on this success, it was decided that drones needed to be larger and carry more substantial explosive payloads to achieve greater impact (Romaniuk 2024).

With each new generation, the payload increased from 108 to 850 kilograms, and the drones were equipped with state-of-the-art communication systems, each costing over $300,000 USD/EUR. Their hulls became radar-invisible and received multiple other innovations, including a flamethrower system to make them more lethal against unprotected targets. In a landmark operation in May 2025, a Magura V5 drone achieved the first air-to-surface/naval drone victory, downing a Russian Su-30 fighter over the Black Sea (Grosswald 2025).

Ultimately, the philosophy changed: the intent became to segment the components of a large ship - air defence, weapons, defensive systems - and distribute them across multiple drones, fundamentally changing how fleet problems can be addressed, especially when building large ships is not feasible. This represents a new era of naval warfare, where strength is no longer defined solely by large, expensive ships, but by intelligent swarms of maritime drones capable of delivering rapid, precise strikes while seizing tactical initiative. Thus, drone operations, alongside new capabilities from shore-based anti-ship missiles, broke the maritime blockade to enable grain exports but also forced the Russian fleet's withdrawal from Sevastopol to the safety of Caucasian ports. This evolution marks the emergence of a new warfare paradigm: prolonged attrition warfare.

The scale and persistence of these attacks forced a third of the Russian Black Sea Fleet to be destroyed, disabled, or relocated, shattering the image of naval invulnerability (Allison 2025).

3. Applicable Lessons Beyond the Black Sea

The operational evolution in the Black Sea offers critical lessons for other geopolitically tense and narrow naval theatres, such as the Baltic Sea and Taiwan Strait, where geography, asymmetry, and the presence of strong maritime competitors create comparable dynamics and vulnerabilities (Till 2018).

The Baltic Sea shares numerous geographical and strategic characteristics with the Black Sea: both are semi-enclosed maritime theaters, relatively shallow (average 55m in the Baltic, 1,200m in the Black Sea), narrow straits, and dense fishing zones, bordered by NATO actors and Russia. The regional naval balance is profoundly influenced by the Russian Baltic Fleet, with its strategic bases in Kaliningrad and St. Petersburg, which dominate access to the Gulf of Finland, Danish Strait, and North Sea. In this constrained environment, with limited manoeuvre space and fragmented radar visibility, USVs capable of swarm operations represent an exceptional asymmetric tool for local naval forces.

These exploit shallow waters for natural camouflage, evade thermal and radar detection by traditional ships, and enable saturation attacks or persistent reconnaissance missions that disrupt Russian surface fleet operations without exposing human crews to risk. Recent naval confrontation experience reveals the defence paradox against USVs: it is much easier to attack than to defend. A swarm of small USVs, launchable from coastlines or civilian ports, can saturate the defences of a frigate or destroyer through the inability to destroy large numbers of naval drones with missile systems (CIWS, RAM) designed for aerial or ballistic threats, not agile and numerous surface targets.

The cost of a Ukrainian attack-type USV such as the Magura V5 (~$250,000 USD/EUR) is far lower than the price of a SeaRAM missile ($2M USD), creating a major economic imbalance (Seligman and Berg 2023). In the Baltic Sea, conventional layered defences - comprising torpedoes, barrage mines, and ASW aviation - must now anticipate rapid simultaneous attacks that outspace traditional sequential responses. This dynamic forces a radical rethinking of force positioning, distributed sensor networks, and autonomous systems, from cheap interceptor USVs to stationary barrage UUVs in critical straits like the Gulf of Finland or Øresund.

Fortunately, this region is not on the brink of open conflict - which would trigger Article 5 and a massive NATO response. The Russian Baltic Fleet, anchored at Kaliningrad and St. Petersburg, dominates access to the Gulf of Finland or Øresund, however, this fleet remains vulnerable to the Ukrainian combat model. Critical infrastructure, such as Gdańsk port (135 million tons of cargo annually), submarine cables (Baltic Connector), or pipelines (Baltic Pipe), becomes a priority target for hard-to-attribute attacks. Civil blockades masked as eco-protests or GPS jamming can hinder regional maritime traffic. Hybrid warfare

is Russia's preferred path, enabling political/economic advantages through ambiguity, social polarisation, and logistic chain paralysis without risking total escalation. Essentially, Baltic hybrid warfare will persist at the edge of open conflict, where critical infrastructure resilience - not brute naval superiority -dictates victory, demanding clear national strategies, persistent vigilance, and accelerated regional cooperation.

The rapid development of this topic prompted the Swedish navy to expedite operationalisation of a large unmanned underwater vehicle (LUUV) for monitoring submarine cables and energy pipelines. This directly addresses vulnerabilities demonstrated by recent incidents, including damaged cables linking Lithuania-Sweden, Germany-Finland, and multiple Estonia-Finland connections. Through autonomous platforms capable of persistent underwater surveillance, Sweden aims to detect potential sabotage operations before they can cause critical damage (Shumlianskyi 2025).

Taiwan's strategic situation amplifies these lessons on a global scale, presenting major similarities with Black Sea/Baltic dynamics but challenges on a much larger scale. Surrounded by the expanding naval capabilities of mainland China/People's Liberation Army Navy (PLAN), Taiwan's defence operates in a narrow theatre (130 km-wide Taiwan Strait), with shallow waters in landing zones and potential for intensive blockades or amphibious assaults. At the 2025 military parade, Beijing displayed heavy-tonnage naval drones and UUVs (AJX-002, HSU-001), signalling intent to dominate this domain (Naval News 2025).

Open-source reports estimate that the People's Republic of China, with its massive industrial capacity achieving 200:1 superiority in naval construction over the US, could produce thousands of USVs annually through civil-military integration (military-civil fusion), leveraging commercial production chains in Shanghai, Dalian, and Guangdong to rapidly scale from prototypes to industrial series. The Chinese military can use maritime drones as sacrificial pawns as landing vanguards, launching thousands of cheap USVs in massive swarms to saturate Taiwan's coastal defences and create safe corridors for debarkation. This "volume vs. volume" strategy exploits force asymmetry: defences based solely on autonomous defensive boats could be relatively easily saturated and eliminated by a Chinese numerical avalanche.

Unlike Russia, China is in continuous expansion of its military force projection in the maritime domain and seeks a formula to counterbalance the US Navy's classic format power. One of the boldest initiatives is launching the first drone-dedicated carrier – a USV-docking experimental catamaran, observed in 2024 and intensively tested in 2025 – capable of deploying dozens of aerial and naval drones simultaneously for swarm-coordination operations (Trevithick 2024). Additionally, Beijing converts commercial cargo ships into hybrid combat platforms equipped with advanced radars, modular containerised missile launchers, and EMALS catapults for VTOL drones, transforming its massive civilian fleet (world's second largest, over 5,500 cargo ships) into "Q-ships" - hybrid systems capable of surprise attacks from apparently innocuous vessels for blockade scenarios. Armed cargo ships represent a critical element of supersaturation for US Navy defences, which must disperse forces during a hypothetical intervention to support Taiwan support. Moreover, the inability to quickly distinguish legitimate commercial targets from masked military platforms generates lethal operational hesitation (Sutton 2026).

In a pure "volume vs. volume" fight, China has the potential to rapidly seize the initiative. A combined attack with thousands of Chinese USVs (potentially 5,000+, based on PLA-tested swarm coordination capabilities and industrial production) could neutralise Taiwan's defensive network of hundreds of autonomous units in hours (Taiwan plans 1,600 USVs), forcing rapid consumption of limited ammunition stocks and exposing launch/coordination platforms (News Desk 2025). The only way to restore balance is a multi-layered autonomous defence, with an aerial tier: swarms of kamikaze UAVs and loitering munitions to suppress Chinese USVs en masse; a surface tier: interceptor USVs with kinetic weapons and anti-USV missiles; and a subsurface tier: barrage UUVs and persistent sensors. However, the underwater domain remains the hardest to cover. Chinese numerical supremacy in large UUVs can rapidly saturate simple radio-magnetic or passive sonar detection systems without dedicated active countermeasures.

4. Tactical-Operational Advantages

Beyond their capacity to launch direct attacks, the strategic and operational advantages of naval drones (USVs) introduce new elements into maritime warfare strategies, shifting from dependence on massive, costly ships to a network-based approach where resilience and adaptability are the defining attributes.

Some of the most significant advantages are their remarkable accessibility and scalability. Unlike traditional ships, which require years of construction and massive investments, naval drones can be mass-produced rapidly and upgraded with new components at much lower cost. This production speed enables naval forces to expand capabilities far more agilely than would be possible with conventional fleets (Jones and Parker 2025). Moreover, USVs offer extreme role flexibility. Although their notoriety stems from attack missions, their potential is vast. They can be used for long-term surveillance, launching diversion operations to distract the enemy, executing countermeasures against mines in hazardous areas, or even ensuring logistical resupply in hostile environments without risking human lives.

This flexibility intertwines with swarm tactics, a concept that amplifies impact. By operating in large numbers, USVs can initiate saturation attacks designed to overwhelm and exhaust enemy ships' anti-missile defences and guns. Even if a significant number of drones are destroyed, the overall cost to the attacker remains sustainable, while the adversary depletes costly defensive ammunition and becomes increasingly vulnerable (Jones and Parker 2025). Ultimately, naval drone usage leads to a significant extension of a fleet's range. By deploying uncrewed vehicles at the vanguard, a naval force can project presence into dangerous areas without risking personnel. This creates a distributed network of sensors and attack points across an extended geographic area, ensuring superior situational awareness and faster response capability.

Although their combat capabilities have drawn attention, one of the most transformative applications of naval drones may lie in logistical support. In any maritime campaign, sustaining resupply for ships, coastal bases, or island outposts constitutes a strategically critical element. Traditionally, resupply missions expose crewed ships to high risk levels in contested areas. Naval drones can change this dynamic in several ways. First, resupply in hostile environments: Small USVs dedicated to logistics can transport fuel, ammunition, food, and medical materials to forward operating bases or ships at sea, even through areas under surveillance or attack threat. Their utility as expendable resources reduces the strategic risk of losing high-value resupply ships.

Second, distributed logistics chains: Instead of relying on large, vulnerable tankers or transport ships, naval forces could deploy fleets of autonomous vehicles that distribute loads across multiple units. This resilient resupply network prevents single points of failure and ensures continuous support under attrition conditions. Naval drones can also be configured to evacuate wounded personnel or deliver medical kits to isolated crews in adverse weather conditions or dangerous areas, such as offshore drilling platforms unsuitable for helicopters or crewed ships. In highly contested military zones, USVs can sustain logistical resupply through autonomous maintenance of supply lines along randomly generated routes, avoiding potential ambushes. This transforms not only how naval forces fight, but also how they endure. A fleet can project power only as long as it is supplied - a principle that uncrewed logistics vehicles could protect in future conflicts.

The true potential of naval drones lies not in their ability to operate in isolation, but in their integration across multiple domains of action. Modern military forces, particularly NATO, place increasing emphasis on "Multi-Domain Operations" (MDO), a doctrine where success depends on simultaneous coordination of effects across land, sea, air, space, and cyberspace. In this vision, naval drones integrate seamlessly, serving as a maritime component that fluidly connects with other uncrewed systems.

While aerial drones are designed to extend range by providing real-time surveillance, target identification, and electronic warfare coverage, uncrewed ground platforms enhance logistics, command-and-control nodes, and defensive fires from the coast. In turn, naval drones bring water

persistence, scalable attack capability, and flexible logistical support. The evolution lies in the ability to make all these systems collaborate. For example, aerial drones could identify enemy positions beyond the horizon, feeding real-time data to naval drones that could execute saturation attacks or deliver supplies under fire, while ground systems coordinate fires or secure coastal bases. In logistical scenarios, the same synergy ensures survival: ground drones deliver supplies to shore, naval vehicles transport them through contested waters, and aerial drones handle high-priority urgent deliveries.

This collaboration completely redefines the nature of the battlespace. Ultimately, future battles will not be fought solely by aircraft carriers and submarines, but by interconnected constellations of ground, aerial, and maritime drones cooperating within an MDO framework. Thus, naval drones will be considered not merely asymmetric attack assets, but an essential element in a broader system-of-systems that sustains resilience, ensures deterrence, and redefines what it means to control the battlespace.

5. Russia's Response and Western Countermeasures

The success of Ukrainian maritime drones did not go unnoticed in Moscow, prompting a comprehensive response that underscores both the strategic importance of this emerging domain and the rapidity with which states can mobilise autonomous capabilities when survival is at stake. Starting in April 2025, Russia established a high-level "Technical Council" for unmanned maritime systems, chaired by Admiral Alexander Moiseev and including members from the presidential administration, defence industry, and scientific community. In May 2025, the Russian Navy began forming specialised uncrewed regiments covering aerial, ground, surface, and subsurface domains, while in July the Kingisepp Machine Plant in St. Petersburg opened - a dedicated drone production complex manufacturing hulls, waterjets, and propulsion units, backed by a 2.7 billion ruble ($33 million) investment (Shumlyan'skyi 2025).

For submersible systems, Russia's capabilities present an even more sophisticated challenge. The "Main Directorate of Deep Sea Research" (GUGI), operating independently of the Russian Navy and reporting directly to the Ministry of Defence, maintains a range of deep-diving submarines, including titanium-hulled vessels "Losharik", "Paltus", and "X-Ray", capable of operating at extreme depths where sabotage damage would be particularly difficult to repair. European defence planners have not overlooked the implications of these Russian underwater capabilities, rapidly developing autonomous subsea systems to counter emerging threats to critical infrastructure.

Sweden recognised these threats and responded with a LUUV development project for the Swedish Defence Materiel Administration, a $6.3 million initiative with initial sea trials scheduled for summer 2026. The platform is designed to provide an autonomous sensor system capable of monitoring and mapping seabed infrastructure while simultaneously detecting and deterring subsea threats. The LUUV integrates Saab's "Autonomous Ocean Core" control system (Swedish defence systems manufacturer), enabling extended autonomous operations without direct human intervention - essential capabilities for countering Russia's sophisticated underwater warfare assets. Sweden's approach exemplifies this transformation, representing a fundamental shift in national defence philosophy from centuries of defensive strategy to what Rear Admiral Fredrik Lindén describes as "transforming into an offensive force to establish and maintain control in our area" (Naval News 2024).

Turning to persistence, the United States demonstrated with "Sea Hunter", produced under DARPA's ACTUV program, that uncrewed surface vessels can operate thousands of kilometres without crew. Initially designed for anti-submarine vessel tracking, Sea Hunter embodies the ambition to incorporate USVs as permanent operational assets, bridging intelligence missions and autonomous patrol. Türkiye's "ULAQ" represents another domain: a family of armed USVs developed locally with modular, interchangeable payloads for anti-ship missiles, electronic warfare packages, or surveillance. Its entry into regular naval service shows how mid-tier powers can bypass traditional large-ship bottlenecks while still demonstrating credible offensive capability in regional waters (Ekşi 2025).

Australia's "Ghost Shark" is a "very large uncrewed underwater vehicle" (uncrewed submarine/XLUSV) revealed in 2023 to counterbalance China's accelerated development in this

sector. Designed for endurance measured in months, Ghost Shark can carry modular payloads from surveillance systems to attack systems. Its stealth and persistence indicate that drones are no longer limited to tactical expendable roles; they are transforming into strategic force multipliers capable of complementing - or even replacing - top-tier conventional assets in certain missions (Australian Ministry of Defence 2024).

6. Romania's Military and Diplomatic Response

The Black Sea can become a theatre of hybrid operations where Russia employs maritime drones, sabotage submarines, and suspicious commercial vessels to disrupt critical infrastructure. Every night, between the scattered lights of platforms and the heavy shadows of cargo ships, the maritime space appears less a commercial frontier and more a grey zone where silence can be shattered anytime by an alarm signal or distant explosion. The explosion of the Ukrainian reconnaissance ship Simferopol, attacked and sunk by Russia at the Danube mouths on the Chilia arm, just a few kilometres from Romanian territorial waters, should have accelerated finding a solution for identifying this type of threat. The moment when Russian drones penetrated deep into the Danube Delta to strike a Ukrainian vessel shows that, beyond press releases and maps, confrontation is already here, in the immediate vicinity of Romanian ports, testing the vigilance of naval forces and NATO borders (Cochino 2025).

Repeated incidents of Russian aerial drones penetrating Romanian airspace - including one that loitered for 50 minutes over NATO territory in September 2025 - illustrate the region's vulnerability to autonomous attack systems (Ministry of National Defence 2025). The fact that an uncrewed platform can remain nearly an hour over allied territory reveals not only an air defence technical problem, but also a deliberate testing of political tolerance limits - a cynical exercise through which Moscow measures both military reaction speed and NATO's diplomatic prudence. More recently, on January 14, 2026, the Chief of Defence stated that Romania neutralised 150 drifting mines since the conflict began, highlighting the persistent threat to commercial routes and energy platforms. Each mine recovered or controlled-detonated means a grain convoy can depart, a tanker can anchor safely, one more day where the regional economy functions without being brought to its knees by an "accidental" incident (The Maritime Executive 2025).

Taken together, these incidents do not merely illustrate Romania's vulnerabilities; they also provide a concrete problem-set against which a proactive, resilience-based response can be designed. Rather than remaining a passive consumer of security, Romania can use the lessons of the Black Sea drone campaign to articulate a positive agenda built around autonomous surveillance, layered defence of critical infrastructure, and regional industrial cooperation in the maritime domain.

Returning to the Neptun Deep project, it is particularly vulnerable due to its complex architecture: fixed deep-water platforms in waters 1,500 meters deep and 160 km of subsea pipelines. This project, developed in partnership by OMV Petrom and Romgaz, will position Romania as the largest natural gas producer in the European Union, with first production planned for 2027, with an estimated volume of approximately 100 billion cubic meters of natural gas. The initiative represents a direct challenge to Russia's energy dominance and a pillar for national energy security (OMV Petrom 2023). However, Romania's Exclusive Economic Zone (EEZ) in the Black Sea, where these critical platforms are located, does not benefit from the guarantees of Article 5 of the NATO Treaty, leaving energy infrastructure exposed to Russian threats in a context of intensified hybrid warfare. The Chief of the Defense Staff, General Gheorghiță Vlad, explicitly warned on January 13, 2026, that this economic zone is not adequately protected, emphasising that concerns extend beyond Neptun Deep to communication cables, underwater power lines, and essential trade routes (Ababei 2026).

The Romanian Naval Forces possess defence and surveillance capabilities, but these do not appear sufficient to counter complex threats in the Black Sea, where Russia demonstrates advanced capabilities in underwater warfare, naval drones, and "false flag" operations. Romania's National

Defence Strategy from November 2025 emphasises strengthening Black Sea regional ties to protect energy projects from Russian threats. The strategy identifies specific risks: naval drones, drifting mines, attacks on commercial routes, and underwater sabotage operations, insisting on developing autonomous naval capabilities as central to hybrid defence (Presidential Administration of Romania 2025). For Romania, protecting Neptun Deep and the entire EEZ at sustainable cost requires a multi-layered autonomous defence model inspired by Ukrainian lessons and NATO Baltic exercises: Layer 1 consists of persistent surveillance via light USVs similar to Magura, with 200-500 km autonomy, positioned around platforms for continuous patrolling, complemented by UUVs monitoring deep pipelines, detecting suspicious vibrations or approaching threats, with redundant communication via Starlink/Iris2 satellites or NATO systems ensuring defence data chains function even when adversaries strike communications infrastructure. Layer 2 features autonomous interceptors - drones with kinetic weapons designed to neutralise enemy vessels - equipped with reactive autonomous mines for immediate platform perimeter defence, with scaling to EEZ level requiring autonomous fleets of 50-100 units, minimising human loss risk. Layer 3 encompasses multi-domain integration (MDO) where aerial drones provide real-time surveillance and target designation, coordinated from shore platforms at Constanța and Mangalia.

Romania, Bulgaria, and Türkiye have demonstrated exemplary military partnership through the Black Sea Mine Countermeasures Group (MCM BS TG), with rotating command transitioned on January 7, 2026. This partnership could expand to economic-technological cooperation for developing regional maritime drone production capacity, moving from operational logic to industrial-strategic logic (Presidential Administration of Romania 2025). This formula leverages complementarity between Turkish expertise in unmanned vehicles such as ULAQ and Romanian industrial infrastructure at Constanța-Mangalia shipyards. A strategic agreement could establish joint production lines capable of producing 50-100 USVs annually, equipped with underwater threat detection sensors, redundant communications, and kinetic weapons. Regional production could also support Ukraine's economic-military effort, creating a Black Sea security ecosystem where technology and experience flow bidirectionally. Financing would combine anticipated Neptun Deep revenues with EU and NATO funding, ensuring rapid operationalisation through integration into multinational exercises such as Sea Shield. Thus, the same energy infrastructure Russia attempts to turn into vulnerability becomes a source of funding for an autonomous maritime protection architecture.

Conclusions

Facing the paradigm shift in the maritime battlespace by the historical review of technological disruptions at sea that shows - naval drones are not just another weapon, but a system that reshapes how power is projected and how resilience is built in the maritime domain. Just as submarines and carrier aviation redistributed combat power in previous eras, USVs now redistribute it horizontally across more numerous, cheaper and expendable platforms, forcing navies to rethink fleet design, survivability and deterrence in semi-enclosed seas.

The Black Sea case study demonstrates that a state deprived of a conventional fleet can, through systematic employment of naval drones, impose disproportionate costs on a superior navy, break blockades and gradually erode an opponent's freedom of action. The parallels drawn with the Baltic Sea and the Taiwan Strait indicate that constrained maritime theatres are especially favourable to such asymmetric strategies, and that coastal states and alliances must anticipate saturation attacks against critical infrastructure, not merely react after the fact.

The paper proposes a three-layer autonomous defence architecture composed of: a persistent surveillance layer of USVs and UUVs around platforms and pipelines; an active interception and close-in protection layer of autonomous interceptors and reactive mines; and a multi-domain integration layer linking maritime drones with aerial and land-based systems in a unified command-and-control framework. This model is the main result of the analysis and shows how Romania can obtain sustainable protection levels by exploiting the same cost asymmetries that make drones attractive to attackers.

The examination of existing regional initiatives and industrial capacities suggests that the proposed architecture is implementable through a coherent program of capability development and cooperation with Türkiye and Bulgaria, backed by Neptun Deep revenues and EU/NATO funding. A regional production and operational framework generating dozens of USVs per year would move Romania from vulnerable periphery to active security provider in the Black Sea and would offer a transferable model for other semi-enclosed theatres. In this sense, naval drones emerge not only as a disruptive threat but also as an instrument through which Romania and its allies can strengthen Euro-Atlantic resilience at sea.

BIBLIOGRAPHY:

Ababei, Oana. “Romania’s Exclusive Economic Zone is Not Covered by NATO Article 5”. Adevărul, January 14, 2026. https://adevarul.ro/stiri-interne/evenimente/zona-econo mica-exclusiva-a-romaniei-nu-este-2500848.html

Allison, George. “Ukraine Has 'Significantly Degraded' Russian Black Sea Fleet”. UK Defence Journal, 2025. https://ukdefencejournal.org.uk/ukraine-has-significantly-degraded-rus sian-black-sea-fleet/

Australian Ministry of Defence. “First Autonomous Undersea Vehicle 'Ghost Shark' Prototype Ready”. April 18, 2024. https://www.minister.defence.gov.au/media-releases/2024-04-18/first-autonomous-undersea-vehicle-ghost-shark-prototype-ready

Cochino, Adrian. “Unprecedented Russian Attack at Romania’s Border”. HotNews, 2025. https:// hotnews.ro/atac-fara-precedent-al-rusiei-in-delta-dunarii-la-granita-cu-romania-video

Grosswald. “Ukrainian Magura V5 Naval Drone Shoots Down Russian Su-30 Fighter in First-Ever Sea-to-Air UAV Kill”. 2025. https://www.grosswald.org/ukrainian-magura-v5-naval-drone-shoots-down-russian-su-30-fighter/

International Tribunal for the Law of the Sea. Case Concerning the Detention of Three Ukrainian Naval Vessels (Ukraine v. Russian Federation). Provisional Measures. 2019. https://www. itlos.org/en/main/cases/list-of-cases/case-no-26/

Jones, Peter, and Jennifer Parker. “Maritime Warfare Technological Developments”. Naval Studies Group Primer No. 1. UNSW Canberra, 2025. https://www.unsw.edu.au/con tent/dam/pdfs/ unsw-canberra/hass/NSG%20Primer%201.pdf

Jones, Peter, and Jennifer Parker. “Maritime Warfare Technological Developments”. 2025.

Knickerbocker, Brad. “Written in Black and Red: Asymmetric Threats and Affordable Unmanned Surface Vessels”. War on the Rocks, 2024. https://warontherocks.com/ 2024/01/written-in-black-and-red-asymmetric-threats-and-affordable-unmanned-surface-vessels/

Ministry of National Defence, Romania. “Evaluation of the Incident Produced by the Penetration of a Russian Drone into National Airspace”. 2025. https://www.mapn.ro/ cpresa/18970

Naval News. “China to Reinforce Naval Pressure Over Taiwan Strait with New AJX002 Extra-Large Underwater Drone”. 2025. https://www.armyrecognition.com/news/navy-news/ 2025/china-to-reinforce-naval-pressure-over-taiwan-strait/

Naval News. “Sweden’s LUUV Development Project”. Naval News, 2024. https://www.nava lnews.com/naval-news/2024/sweden-luuv-development/

News Desk. “Taiwan Plans to Manufacture 1,600 Unmanned Attack Vessels Amid Rising Regional Tensions”. 2025. https://news.ssbcrack.com/taiwan-plans-to-manufacture-1600-unmanned-attack-vessels/

OMV Petrom. Final Investment Decision in the Neptun Deep Project: A Strategic Step for Romania. Sustainability and Development Report, 2023. https://www.omvpetrom.com/downloads/ 2025/05/capital-market-presentation-neptun-deep-fid-june-22.pdf

Osgood, Alexander. “Unmanned Pioneers: Remote Control Weapons in World War II”. Journal of Military History 85, no. 4 (2021): 921-44.

Presidential Administration of Romania. National Defense Strategy of the Country for the Period 2025–2030. Bucharest, November 2025. https://cdn.edupedu.ro/wp-content/uploads/2025/11/SNAT-2025-2030.pdf

Presidential Administration of Romania. National Defense Strategy of the Country for the Period 2025–2030. November 2025.

Romaniuk, Roman. "How Ukraine Created a Sea Drone Fleet That Made History". Ukrainska Pravda, January 1, 2024. https://www.pravda.com.ua/eng/articles/2024/01/01/7435326

Romaniuk, Roman. "How Ukraine Created a Sea Drone Fleet That Made History". Ukrainska Pravda, January 1, 2024.

Seligman, Lara, and Matt Berg. "A $2M Missile vs. a $2,000 Drone: Pentagon Worried Over Cost of Houthi Attacks". Politico, December 19, 2023. https://www.politico.com/news/2023/12/19/missile-drone-pentagon-houthi-attacks-iran-00132480.

Seligman, Lara, and Matt Berg. "A $2M Missile vs. a $2,000 Drone". Politico, 2023.

Shumlianskyi, Dmytro. "Sweden Develops Large Underwater Drone for Baltic Sea". Militarnyi, 2025. https://militarnyi.com/en/news/sweden-develops-large-underwater-drone-for-baltic-sea/

Shumlyan'skyi, Dmytro. "Advancements in Russian Naval Drones and Their Role in the Armed Forces". Black Sea News, 2025. https://www.blackseanews.net/en/read/233967

Sutton, H.I. "China's Q-Ship Containerized Weapon System". January 4, 2026. https://www.hisutton.com/Chinese-Q-Ship.html

The Maritime Executive. "Romania Destroys Sea Baby Drone Spotted in the Black Sea". 2025. https://maritime-executive.com/article/romania-destroys-sea-baby-mine-spotted-in-the-black-sea

Till, Geoffrey. Seapower: A Guide for the Twenty-First Century. 4th ed. London: Routledge, 2018.

United Nations. Agreement on the Status and Conditions of the Presence of the Black Sea Fleet of the Russian Federation on the Territory of Ukraine. Treaty Series, vol. 2498, 1997. https://treaties.un.org/doc/Publication/UNTS/Volume%202498/v2498.pdf

Trevithick, Joseph. "China's New Stealthy Trimaran Drone Ship: Our Best Look Yet". The War Zone, 2024. https://www.twz.com/news-features/our-best-look-yet-chinas-new-stealthy-trimaran-drone-ship

INDEX OF AUTHORS

AVETISYAN Rafik, PhD, 89
BOBOCEA Marius Gabriel, 129
BRATCOVICI Maria Niamh, 136
BRUMARU Adriana, 121
CHAMROVA Jana, 79
FLOREA Ana-Maria, 99
GRAD Marius, PhD, 62
GROSU Ruslana, PhD, 48
HOVHANNISYAN Artsrun, PhD, 9
IANCU Sînziana, PhD, 114
IOSIF Bogdan Daniel, 38
KOCHARYAN Tigran, PhD, 89
LAZĂR Aurel, PhD, 26
LICĂ Daniela, PhD, 99
LUȚAI Raluca, PhD, 62
MEREANU Mara-Mihaela, 154
NIȚĂ Adrian, 160
POPESCU Cătălin-Victor, 48
SCIPANOV Lucian Valeriu, PhD, 38
VASILE Dumitru-Cătălin, 144
ZODIAN Mihai, PhD, 19

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE

Director: Colonel Liviu Vasile STAN

The publication consists of 174 pages.

"Carol I" National Defence University Typography
Bucharest/Romania, sector 5, 68-72 Panduri Street
e-mail: editura@unap.ro
Phone: 00-40-021-319.48.80/0215; 0453

302/02545/2026 **C. 104/2026**