DOI: 10.53477/1842-9904-25-32

DETERRENCE STRATEGIES FOR SMALL AND MEDIUM-SIZED STATES ON NATO'S EASTERN FLANK: THE CASE OF ROMANIA IN THE NEW SECURITY CONTEXT

Sorin TOPOR, PhD*

The war in Ukraine has rewritten the parameters of international security and put military deterrence back at the heart of the European security architecture. Donald Trump's recent statements reflect an ambivalent approach to deterrence, combining pressure for increased defence spending by NATO allies and linking US political commitment to the Alliance's fundamental principles. All of this may increase the risk of misperceptions and strategic exploitation of internal fractures by a potential adversary.

This paper analyses the mechanisms by which a state in the proximity of the conflict – the case of Romania, can build a credible strategic deterrence posture in an environment marked by uncertainties regarding the cohesion of alliances and power asymmetries. Using a comparative methodology (MSSD) and the TOWS matrix, the study proposes the transition from norm-based deterrence to deterrence through denial, supported by societal resilience and advanced technological capabilities.

The conclusions of the paper argue the reality that Romania cannot compete symmetrically with a nuclear and cyber power (e.g. Russia). Nevertheless, Romania can attain a level of effective deterrence by combining internal defence development measures and the consolidation of political-military alliances (NATO, EU). These findings may represent relevant operational recommendations for the formulation of European security policy.

Keywords*: deterrence; NATO, Romania; Black Sea; European security; resilience; hybrid warfare.*

* ***Captain (Nv) (r) Sorin TOPOR, PhD, Hab is a Cyber Security Specialist at the National Institute for Research and Development in Informatics - ICI Bucharest and associate member of the Romanian Academy of Scientists, Bucharest, Romania. E-mail: sorin.topor@ici.ro***

Introduction: Reconceptualising Deterrence in Eastern Europe

European security is in a phase of accelerated re-militarisation driven by the War in Ukraine, which has demonstrated that the model of high-intensity conventional warfare remains a systemic threat. For the states on NATO's Eastern Flank, this reality requires a transformation of defence strategies, with the main direction of efficient combination of autonomous national capabilities with collective security guarantees.

The current strategic environment is marked by heightened uncertainty, such as volatile political discourses (e.g. Donald Trump's statements on the intention to take control of Greenland and the application of Article 5) as well as signals of reduced involvement of some major allies within NATO's consultative structures. Although such developments cannot be considered political certainties, they nonetheless influence perceptions of Alliance cohesion and impose greater strategic autonomy on member states, thereby creating potential opportunities for adversaries to exploit internal divisions.

The main aggregate effects on NATO are summarised in the following aspects:

1. Rapid transformation of conventional deterrence. It is clear that an increase in defence spending to 5% of GDP by 2035 (Presidential Administration 2025a) will lead to increased response capabilities of conventional military forces, whereas ambiguous messages regarding the reduction of American personnel in NATO structures and those regarding the application of Article 5 undermine the credibility of the collective commitment;

2. The role and position of the Alliance: statements on Greenland and trade tensions, especially with the Alliance states, generate the perception of instability of the US as the traditional leader of NATO. Discussions on the establishment of an independent European Pillar within NATO (Tardy, 2025) introduce additional variables into the deterrence equation. Such a scenario could be exploited by adversaries through wedge-driving strategies, aiming at capitalising on possible hesitations, decision-making dissonances, or ambiguities in the activation of mutual assistance commitments between transatlantic and European allies.

3. Validation of the robustness of strategic deterrence mechanisms : In general, deterrence does not only involve military spending but also political cohesion. The lack of strategic clarity on the part of an ally reduces the degree of political-military cohesion, which leads to risks of misinterpretations and encouragement of a state or non-state actor to initiate instability and new conflicts of claim.

To date, Romania has adopted a strategy of active defence and advanced deterrence (Presidential Administration 2025b), based on deepening its military alliance with the United States, promoting the development of a multinational NATO force, consolidating its strategic presence in the Black Sea region and becoming

a key defensive line to isolate Russia's actions in the Black Sea, but also in the Balkans. In the context of the new geopolitical content determined by the evolution of the war in Ukraine and its position in the proximity of Russian territory, it faces a major challenge, namely: *How can a superior military actor be deterred without entering into an arms race, impossible to sustain economically?*

In fact, this is the main theme on which this analysis was structured.

1. Theoretical Framework: From Classical to Integrated Deterrence

The classical concept of strategic deterrence represents the ability of a state actor to prevent hostile actions of an adversary by the credible threat of unacceptable retaliation (Schelling 1960, p. 187). During the Cold War, deterrence was founded almost exclusively on the military dimension, based on nuclear retaliation, being closely linked to the logic of the balance of forces – the concept of Mutually Assured Destruction – MAD (Straub 2019, Hussy 2025).

It was based on three essential pillars:

1. Capability – the existence of sufficient military means to cause significant losses to the opponent;

2. Credibility – convincing the adversary that these means will be used;

3. Communication – clearly conveying the intention to respond to aggression.

Unlike the classical approach, modern deterrence encompasses a holistic approach that integrates military, political, economic, informational and cyber tools in a NATO concept called *cross-domain deterrence* or *integrated deterrence* (Sweijs and Zilincik 2019, p.13) and includes:

- *Deterrence through punishment* – includes threats of unacceptable post-aggression retaliation;

- *Deterrence through denial* – refers to reducing the probability of successful aggression by strengthening defence capabilities (such as air defence systems, A2/AD capabilities, fortifications and military engineering, mobility, etc.), thereby rendering an attack excessively costly or difficult to undertake;

- *Deterrence through resilience* – is based on the level of societal capacity to absorb shocks and rapidly restore critical functions, while simultaneously retaining the ability to inflict significant damage on the aggressor through measures such as precision strikes, deep strikes, cyber capabilities, electronic warfare following an attack;

- *Normative deterrence* – is based on the existence or harmonisation of international legal and normative frameworks designed to undermine the legitimacy and reputation of the aggressor (Brown 2020).

Libicki pointed out that a defining element of modern deterrence will be its extension to non-kinetic domains (Libicki 2009). Currently, the major challenges of using cyberspace for deterrence relate to favouring attacks adopting new valences such as: anonymity, speed and asymmetry of threats (Rid and Buchanan 2014, pp. 4-37).

Particularly in the context of hybrid warfare, deterrence aims to limit the efficiency of the adversarrial information manipulation through targeted measuresin education, strategic communication, and the protectionof democratic processes (Pomerantsev 2019, p. 119).

Regarding the concept of collective deterrence within political-military alliances, NATO has adopted the adaptive deterrence model (NATO 2022, p.7). It combines the position of advanced military presence with societal resilience and cyber defence measures. Moreover, among the EU Allies, a complementary contribution of this direction is observed, through the use of economic and regulatory instruments, cybersecurity policies, as well as through measures designed to combat disinformation and external interference (Join /2017/0450 final 2017). This reflects the integrated and multidimensional character of contemporary deterrence.

Therefore, modern deterrence should be understood as a dynamic, adaptive and context-dependent concept. It provides an analytical and adapted framework for understanding state behaviour within the context of current strategic competition. It allows the assessment of the interaction between hard and soft power instruments, and it can determine how small or medium-sized states can compensate for conventional disadvantages through resilience, alliances and advanced technologies. This approach facilitates the transition from a deterrence based primarily on institutional norms and legal guarantees to a strategy based on denial capabilities and resilience tailored to national particularities. For small and medium-sized states on NATO's Eastern Flank, this change marks the transition from a passive to an active security, where technological capacity and societal cohesion become the main pillars of stability.

2. Method, Comparative Analysis and Case Studies (MSSD &MDSD)

To robustly validate the hypotheses and increase the replicability of the research, the study uses a qualitative security methodology, based on empirical data on military spending and national security capabilities. Comparison of resilience strategies between Romania, Poland, Estonia (Most Similar Systems Design – MSSD method), and Israel (Most Different Systems Design – MDSD method), enables a combinatorial approach to deterrence theory (Mazarr 2018; Freedman 2013, pp 9-11), supported by empirical data on defence expenditure, necessary spending to modernise and adapt military capabilities to counter hybrid attacks, as well as through consolidation of alliance policies that involve the presence of Enhanced Forward Presence Battle Groups (eFP) on national territory.

The three reference models are:

The Polish Model: based on *massive investments in military capabilities* (4.12% of GDP in 2024), for the domestic production of armored carriers and artillery (Rosomak, KRAB, Borsuk), for the modernisation and expansion of active military

forces, for massive acquisitions of modern equipment (Leopard 2, F-15, Patriot), as well as for supplement plans with Abrams, Patriot PAC-3 (USA), K2 and FA-50 (South Korea) equipment (Surwillo and Slakaityte 2024);

The Estonian Model: it demonstrates how *cyber defence, digital and societal resilience* can compensate the reduced size of conventional forces (Government 2010);

The Israeli Model: it emphasises *technological superiority*, active deterrence capabilities through *preemptive strikes* and the role of *intelligence services* (ISR) (Hayman, Rakocz and Kurz 2025).

To validate the model in the context of the Romanian security ecosystem, this study applies a sequential exploratory design of theoretical data to the operational realities identified in the selected case studies.

The analysis is structured around the following indicators:

1. *Denial Capability*: A2/AD systems, military mobility, critical infrastructure protection.

2: *Societal Resilience*: the capacity to absorb and recover from physical, cyber, and hybrid shocks;

3: *Degree of integration into allied structures*: assessed through the presence of Enhanced Forward Presence (eFP) forces and participation in decision-making mechanisms.

The research uses a sequential exploratory design, formulated in three correlated phases, which will ensure the validation of the working hypotheses:

- Bibliometric analysis (qualitative phase): This phase involved the examination of strategic documents issued by NATO and the EU, as well as the National Defense Strategy, reports and works indexed in international databases (Scimago, Web of Science, Scopus and Google Scholar). This process enabled the identification and extraction of key performance indicators relevant to the modern concept of strategic deterrence;

- Comparative analysis and case studies: This stage focused on the identification of strategic trends, analysis of empirical data (defence budgets, GDP shares, investments in R&D for security, etc.). The case studies allowed identifying the degree of maturity and current fragmentation of national security frameworks;

- Conceptual modelling and logical validation: Based on the data extracted, through the SWOT analysis, it validated the formulation of conclusions through which Romania can achieve a level of effective deterrence. At the same time, these can represent operational arguments for the development of internal resilience.

The systematic SWOT analysis is integrated into a broader decision-making model to overcome the threshold of subjective description regarding Romania's strengths, vulnerabilities, and strategic options. The TOWS matrix can generate strategic options for:

- SO Strategies: *How to use the strategic position on the Black Sea to attract new NATO investments?*

- WO Strategies: *How to compensate for the lack of nuclear capabilities by integrating into the European cyber shield?*

The study tests the following working hypotheses:

I1: Increasing the defence budget to the 5% of GDP threshold directly correlates with an exponential increase in the credibility of deterrence, provided that political cohesion within NATO is maintained and the mechanisms for applying Article 5 are clarified.

I2: Implementing a deterrence through denial strategy, based on advanced cyber technologies and NATO's seven basic requirements for societal resilience, can effectively offset Romania's conventional military asymmetry in relation to a hostile regional power.

I3: The integration of the eFP with national hybrid response mechanisms transforms the cost of a local aggression into a systemic risk for a potential attacker, thus validating the effectiveness of the adaptive deterrence model.

The main analysis tools and techniques employed in this study include:

- Comparative analysis using the MSSD and MDSD approaches: The Most Similar System Design (MSSD) method was used to compare Romania with Poland and Estonia (states with similar threats), while the Most Different Systems Design (MDSD) approach was employed in the case of Israel (in a non-NATO context).

- The set of qualitative indicators for civil resilience, based on NATO's seven baseline requirements for national resilience (Kunce, 2025), applied to case studies;

- Triangulating data by corroborating political statements by major European and US leaders with budget data and international strategic reports to eliminate subjectivity;

- The SWOT-TOWS strategic analysis determines the transition from a descriptive inventory of strengths and weaknesses to generating security and defence strategies, having as the main structural vulnerability naval asymmetry in the Black Sea and, as opportunities, capitalising on Romania's geostrategic position and integration into the European "cyber shield", by attracting NATO and EU investments.

The main limitations of the research were determined by the dynamics of political discourse (the statements of political leaders are in continuous evolution), access to data (some information is classified, especially in the field of cybersecurity capabilities or crisis management plans), a situation that imposed the use of only data obtained from open sources (OSINT) and the internet.

3. Strategic Analysis for ROMANIA (SWOT-TOWS)

The analysis performed is supported by the use of an integrated methodological model, which organises actions by areas according to Table No. 1.

Table No. 1: Organizing actions by areas of analysis

Domain	Deterrent tool	Strategic objective
Military (hard power)	eFP , A2/AD, 5% of GDP	Deterrence through punishment and denial
Cyberwarfare	Cyber-physical and hybrid systems, public-private partnership	Limiting anonymity and asymmetry
Societal	Education, combating disinformation	Increasing societal resilience
Political	Alliances (NATO, EU, regional), strategic communication	Maintaining clarity and cohesion

Following the structured analysis of the sources, the useful observations were extracted:

Table No. 2: Romania vs. Estonia and Lessons for Romania

Dimension	Estonia	Romania	Lessons for Romania
Cyber defence	Very advanced	In development	Rapid development of Cyber Defence Command/MoND (in Ro: CApC /MApN)
Societal resilience	Very high	Average	Education through institutional programs and mass media, social cohesion
Army Size	Small	Average	Developing public-private programs that combine military structures into national resilience systems

General observation: Estonia is a model of total resilience. It is developing cyber defence capabilities, has programs to training the population for crisis, is developing close cooperation with NATO, has implemented the digital society model and has relevant protective capabilities. The Estonian model demonstrates that digital and societal resilience can compensate for military vulnerabilities.

Table No. 3: Romania vs. Israel and Lessons for Romania

Dimension	Israel	Romania	Lessons for Romania
Intelligence services	Global leader	In development	Investments in ISR, satellites, etc.
Pre-emptive strikes	Central	Limited	Doctrinal changes
Military innovation	High	Moderate	R&D partnerships in the field of military sciences and technology

General observation: Israel represents a relevant model of technological superiority and preemptive strike strategies. To this end, it has developed highly advanced intelligence services, deep strike capabilities, total information integration capabilities, particularly between air and special forces, as well as clear doctrines of active deterrence. Israel demonstrates that deterrence comes from the demonstrated ability to strike decisively. In this regard, Romania could draw lessons from Israeli model, particularly in fostering a culture of innovation and integrating intelligence capabilities within military operations.

Table No. 4: Romania vs. Poland and Lessons for Romania

Dimension	Poland	Romania	Lessons for Romania
Defence budget	>3% of GDP	2.5% of GDP	The need to grow at least 3% of GDP
Land forces	Very strong	Moderate	Investments in Mech Inf Bde.
Air Force	F-35 (in progress)	Modernisation in progress	Accelerating modernisation programs
Presence in NATO	Regional leader	Regional center	Romania must assume a more proactive role

General observation: Poland is the state that has developed policies of accelerated militarisation. For this, it has established massive investments in defence, acquired modern military systems (HIMARS, tanks, F-35 aircraft, etc.), developed territorial defence systems, it developed policies and achieved a strategical approach with the USA. Thus, it has become a regional deterrent pole through rapid investments and solid alliances. Romania can compensate for these models through asymmetry, A2/AD and alliances.

It is evident that Romania cannot compete symmetrically with a nuclear power; however, it can achieve effective deterrence through denial. In general, deterrence through denial is a strategy that would cause a potential adversary to take into account the reality that any attempt to conquer the national territory would be extremely difficult or even impossible. Drawing on the lessons derived from the selected case studies, the Estonian model highlights the importance of societal resilience and the strategy of total war in case of aggression. The Israeli model, centred on technological superiority and pre-emptive strike capabilities, together with the Polish model, characterised by massive investments in territorial defence and precision-guided weaponry, both exemplify forms deterrence through denial. While certain elements of these strategies also facilitate deterrence trough punishment. These specific framerworks – alongside a third complementary model – serve as the foundation for a new, adaptive deterrence model that integrates their core strengths into a coherent approach suited to Romania's security environment.

In this context, the role of cybersecurity is extremely important, with cyberspace becoming a force multiplier. This is achieved by protecting critical national infrastructures (energy, telecommunications, water, transport, etc.), creating cyber counterattack capabilities, strengthening cooperation with NATO, EU and regional partners and, when possible, by participating in joint digital resilience exercises. A potential aggressor must recognise that the targeted state may be able not only to ensure a conventional military response, but also of coordinating internationally supported cyber responses. Therefore, the key to strategic survival is the size of alliances. Given that no small or medium-sized state can ensure complete strategic deterrence alone, it is imperative to strengthen the presence in alliances such as NATO, the EU, and regional ones. Furthermore, the deployment of allied troops on national territory increases the cost of a potential aggression through the logic of the "tripwire" effect, while simultaneously enhancing military interoperability through joint exercises.

However, the most important deterrent factor is the will of the citizens to defend the country. In modern history, there are numerous examples in which a small state deterred an aggressor if it demonstrated that its population resisted, that state institutions did not collapse, that the government did not capitulate, and that there were no internal societal fractures that could be explored. This is where appropriate measures to combat disinformation come into play.

In addition, this strategy can be supported by the application of deterrence through punishment policies, which include harassment and sabotage, techniques to cause major strategic losses to the aggressor. Ukraine has faced Russian aggression for four years by executing such measures.

A deterrence strategy can fail for many reasons:

- *Excessive strategic ambiguity* – the aggressor does not know what will trigger the response;

- *Lack of political will* – the adversary perceives political weaknesses and lack of consensus on the topic of national security;

- *Insufficient military capabilities* – deterrence becomes just rhetoric;

- *Internal divisions* – polarisation of society through disinformation.

To trigger an attack, an adversary will analyse a series of security indicators, such as:

- *Many small and medium-sized states have military structures only for drills*. For credible deterrence, they must structure their defence systems into mobile, dispersed and difficult-to-neutralise structures. Combat units must be small, autonomous and digitally interconnected. A2/AD, logistics, and mobilisation capabilities must be resilient and redundant. Ammunition and equipment depots must be decentralised. Collectively, these measures are intended to convince a hypothetical adversary that the objective of contemporary defence is not to maintain a continous defensive posture across the entire front, but rather to ensure that occupying and maintaining control of occupied territory would become extremely costly.

- *Lessons learned from military operations* Romania's military history offers numerous examples of leaders who adopted mobile defence, harassment tactics, ambushes, and rapid attacks with limited objectives in war. Such strategies contributed to resounding victories, including during the Dacian-Roman Wars (1st-3rd centuries AD), the Battle of Posada (1330), the medieval wars with the Ottoman Empire, the military campaigns of 1916-1917 (the battles of Mărăști, Mărășești, and Oituz), the actions of the Romanian Mountain Troops units in World War II, and many others. In the contemporary strategic environment, the model that many Eastern European states are moving towards, based on the lessons learned from the war in Ukraine, requires the extensive use of drones, highly mobile manoeuvre groups, the integration of special forces into national defence doctrines, cyber and electronic warfare capabilities, etc. Studying the level of endowment and the procedures for using new military equipment can produce a credible deterrent to the intention to launch an aggression.

- *Areas where the defender has strengthened its defence*. Modern deterrence is no longer just military. It combines the land domain (mobile and anti-tank defence), air (layered defence and drones), maritime (anti-ship capabilities), cyber (protection of critical infrastructure and cyber attack capabilities), and information (defensive PSYOPs and countering disinformation). A simultaneous approach to exercises in all these areas, even on a small scale, strengthens the level of deterrence. Therefore, a credible deterrence strategy for Romania does not mean that the armed forces must be stronger than the aggressor's, but that the entire country can make an aggression too costly, too risky, and too unpredictable to be attempted. It is not enough to threaten; you must also make the aggressor consider your will and ability to respond. Credibility must be translated into doctrines, structures, investments and exercises.

In the context of modern deterrence, we systematically analysed a series of benchmarks that we have grouped into SWOT elements (Figure no. 1). This analysis allows mapping the interactions between Romania's internal resources, external constraints and alliance architecture. Subsequently, the four SWOT dimensions were integrated into an explanatory matrix (TOWS) that links each category to the theory of deterrence.

The central argument of the SWOT-TOWS analysis is that Romania has solid foundations for deterrence, but its effectiveness depends on correcting structural vulnerabilities and strategically capitalising on Euro-Atlantic opportunities. Romania cannot compete symmetrically with a nuclear power, but it can achieve effective deterrence through denial. Romania's armed forces meet NATO standards, but many weapons in its arsenal are outdated, inherited from the Soviet-era Warsaw Pact. Without a doubt, Romania's most important security asset is its membership in NATO, which provides the ability to credibly signal the collective will to defend, without being obliged to match the offensive capabilities of an aggressor on its own.

Strengths	**Weaknesses**
S1. Membership in NATO, EU and regional alliances; S2. Increase the defence budget to 3% by 2030; S3. Modern defence capabilities (Patriot, HIMARS) S4. Geostrategic position on the Black Sea S5. Allied military presence on national territory (eFP)	W1. Major naval asymmetry in the Black Sea towards Russia (naval drones, frigates and corvettes equipped with Kalibr missiles, jamming and spoofing GPS etc.) W2. Fragmented cyber defence capacity W3. Domestic political polarisation and erosion of public trust in security institutions W4. Critical infrastructures vulnerable through dependence on unprotected networks W5. Dependence on imports of arms and military equipment and the lack of a robust defence industry
Opportunities	**Threats**
O1. EU and NATO funds for security O2. Strategic cooperation with the US, France and Germany O3. Regional alliances with Poland, the Baltic states, Bulgaria, Türkiye etc. O4. Development of the national defence industry O5. Increasing Romania's role in Black Sea security	T1. Russian aggression and the expansion of the conflict in Ukraine T2. Cyberattacks on energy and communications networks, as well as on electoral processes T3. Disinformation, manipulation campaigns and political interference T4. Weakening NATO cohesion and reducing collective deterrence T5. Economic and/or energy crises

Figure no. 1: SWOT analysis

Table No. 5: Strategic implications

Strategy	Strategic implication
S+O	Romania can evolve from a security receiver state to a regional leader on the Black Sea by capitalising on its geostrategic position and attracting investment
S+T	NATO must offset major external risks
W+O	NATO/EU investments can correct/overcome internal vulnerabilities
W+T	In the absence of structural reforms and strengthening internal cohesion, Romania remains exposed to hybrid warfare tactics and disinformation.

Synthesising the logic of deterrence through denial, the following conceptual formula fmay be proposed:

Credible Deterrence = Military Capability + Societal Resilience +
+ Strong Alliances + Cybersecurity + Strategic Clarity

Where: Without any of these elements, deterrence will be incomplete.

Based on the strategy of deterrence through denial, Romania should quickly develop a series of priority directions as follows:

- Increasing the defence budget to 3% of GDP by 2030: this measure would convey two key messages such as political will and material capacity that allows for modern acquisitions;

- Asymmetric modernisation: development of A2/AD systems, implementation of layered defence (Patriot/SHORAD), anti-ship capabilities in the Black Sea (coastal missiles, fast missile carriers, advanced maritime surveillance), modernisation of mobility and troop dispersal (more flexible mechanised units, additional HIMARS capabilities, anti-drone capacity, decentralised depots, etc.);

- Creating a Unified Cyber Command: Integrating the private sector into the security architecture to counter asymmetric attacks.

- Societal resilience through education: combating disinformation (national and mass education programs through the media), preparing the population for crisis management, strengthening trust in institutions.

- Industrial autonomy: revitalisation of the national defence industry, new jobs, technological innovation, and reduced dependence on external supply chains in the event of a conflict.

Conclusions and Strategic Recommendations

The present research confirms that an effective deterrence model for medium-sized states on the Eastern Flank, such as Romania, does not reside in parity of brute force, but in cost asymmetry. By integrating the lessons from the Israeli and Polish models, we have demonstrated that:

1. *Deterrence through denial*: is validated by transforming aggression into an unprofitable strategic act. This does not guarantee the absence of risk, however it eliminates the pragmatism of an attack by the certainty of operational failure or a prohibitive cost of occupation.

2. *Indivisibility of security*: Romania's national security is inextricably linked to the European architecture. Romania is not just a security beneficiary, but a strategic outpost of NATO, exercising an active deterrent influence in the geopolitics of the Black Sea basin.

3. *Pillars of credibility*: Credibility does not derive from political rhetoric, but from the triad: allied interoperability, targeted technological investments and societal will to protect the constitutional order.

To operationalise this adaptive model, the following priority measures are proposed:

Strengthening Societal Resilience (NATO Baseline 7) through:

− *Resilience audit*: Implementing a biannual audit mechanism for the 7 NATO baseline requirements, with a focus on energy independence and redundancy of communication networks.

− *Public-private partnership in cybernetics*: creating a national cyber defence hub that integrates the private IT sector into the state's rapid response mechanisms.

Optimising military and technological capacity through:

− *5% of GDP pillar*: using the budget surplus not only for procurement, but for research and development (R&D) in "game-changer" technologies (drones, AI, anti-access/A2AD systems).

− *Synchronization of eFP*: increasing the frequency of "snap check" exercises to test the immediate integration of allied forces with reservist and territorial defence units.

Cohesion and political will through:

− *Strategic communication*: developing a national civic education program on hybrid risks, to increase the population's immunity to disinformation and strengthen the "will to resist".

− *Clarification of article 5 mechanisms*: supporting automated response protocols for hybrid incidents that precede conventional armed conflict at NATO level.

In conclusion, Romania currently represents an essential component of the Euro-Atlantic defence architecture. The validation of this adaptive model demonstrates that, through smart investments and the strengthening of societal resilience, a medium-sized state can neutralise the hegemonic ambitions of a regional power, thus guaranteeing the stability of the broader European security environment.

Therefore, the present analysis is relevant not only for Romania, but for the entire European security architecture, representing a NATO outpost, a deterrent influence in international geopolitics. From the perspective of the Romanian model, credible

deterrence for a small and medium-sized state does not imply matching the brute force of a regional aggressor; rather, it depends on transforming aggression into an unprofitable strategic act. In this sense, credibility does not reside only in political declarations, but in allied interoperability, constant technological investments, and in the will of citizens to defend the democratic constitutional order.

BIBLIOGRAPHY:

Brown, Gerald C. 2020. "*Deterrence, Norms, and the Uncomfortable Realities of a New Nuclear Age*", War on the Rocks, Accessed at 25.01.2026. https://warontherocks.com/2020/04/deterrence-norms-and-the-uncomfortable-realities-of-a-new-nuclear-age/

Freedman, Lawrence. 2013. "*The Primacy of Alliance: Deterrence and European Security*", Proliferation Papers 46, IFRI Security Studies Center, ISBN: 978-2-36567-155-2, Accessed at 02.02.2026. https://www.researchgate.net/profile/Lawrence-Freedman-2/publication/29991306_Nuclear_weapons_a_new_Great_Debate_EU-ISS_Chaillo t_Papers_48_July_2001/links/004635384a70204830000000/Nuclear-weapons-a-new-Great-Debate-EU-ISS-Chaillot-Papers-48-July-2001.pdf

Government, 2010. *"National Security Concept of Estonia"*, Republic of Estonia, Accessed at 25.01.2026. https://www.kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_eng_22.02.2023.pdf

Hayman, Tamir, Rakocz Boaz and Kurz Aanat. 2025. "*The State of Israel's National Security, Doctrine and Policy Guidelines for 2025-2026"*, The Institute for National Security Studies, Accessed at 24.01.2026. https://www.inss.org.il/wp-content/uploads/2025/02/SecurityPolicy-Version-ENG_digital-1.pdf

Huessy, Peter. 2025. "*Mutually Assured Destruction*", Global Security Review, Accessed at 25.01.2026. https://globalsecurityreview.com/mutually-assured-destruction/

Join /2017/0450 final. 2027. "*Resilience , Deterrence and Defense: Building strong cybersecurity for EU"*, Joint Communication to the European Parliament and the Council, EUR- Lex https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

Kunce, Beth.2025. "Beyond the Tornado: Strengthening Societal Resilience against Hybrid Warfare", Chapter Twenty-one, in *The Indo-Pacific Mosaic: Comprehensive Security Cooperation in the Indo-Pacific* from CSC 25-2 course, p. 508, https://doi.org/10.71236/JNMB4928

Libicki, Martin C. 2009. "*Cyberdeterrence and Cyberwar*", Santa Monica, CA: RAND Corporation, ISBN: 978-0-8330-4734-2, Accessed at 26.01.2026. https://scispace.com/pdf/cyberdeterrence-and-cyberwar-494xaap01d.pdf

Mazzar, Michael J. 2018. *"Understandig Deterrence"*, Santa Monica, CA: RAND Corporation, Accessed at 27.01.2026. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf

NATO. 2022. "*Strategic Concept"*, NATO Summit in Madrid, Accessed at 27.01.2026. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

Pomerantsev, Peter. 2019. "*This is Not Propaganda: Adventures in the War Against Reality"*, New York: Public Affairs, ISBN: 978-1-6417-6211-4.

Presidential Administration. 2025a. *Declaration of the Hague Summit , issued by the NATO Heads of State and Government participating in the North Atlantic Council meeting*, https://www.presidency.ro/ro/media/declaratia-summitului-de-la-haga-emisa-de-sefii-de-stat-si-de-guvern-nato-participante-la-reuniunea-consiliului-nord-atlantic

Presidential Administration. 2025b. *"National Defense Strategy of the Country for the Period 2025-2030, Independence and Solidarity - Romania's Vision for a Changing World"*, Accessed at 03.02.2025. www.presidency.ro/files/userfiles/Strategia%20Națională%20de%20Apărare%20a%20Țării%20pentru%20perioada%202025-2030.pdf

Rid, Thomas and Buchanan Ben. 2014. "*Attributing Cyber Attacks"*, Journal of Strategic Studies, 38(1-2), Accessed at 15.01.2026. https://doi.org/10.1080/01402390.2014.977382

Schelling, Thomas C. 1960. "*The Strategy of Conflict"*, Cambridge Massachusetts: Harvard University, London, Accessed at 08.01.2025. https://dokumen.pub/qdownload/the-strategy-of-conflict-0674840313.html

Straub, Jeremy. 2019. "*Mutual assured information destruction influences and cyber warfare: Comparing, contrasting and combining relevant scenarios"* , Technology in Society, vol. 59, Accesed at 26.01.2026. https://doi.org/10.1016/j.techsoc.2019.101177

Surwillo, Izabela and Slakaityte Veronika. 2024. "*Power moves east: Poland's rise as a strategic European Player"*, DIIS Policy Brief, Danish Institute for International Studies, Accessed at 26.02.2026. https://www.diis.dk/en/research/power-moves-east-polands-rise-as-a-strategic-european-player

Sweijs, Tim and Zilincik Samo. 2019. "*Cross Domain Deterrence and Hybrid Conflict"*, HCSS Security, The Hague Center for Strategic Studies, ISBN/EAN: 98949210270, Accessed at 20.02.2025. https://hcss.nl/wp-content/uploads/2021/01/Cross-Domain-Deterrence-Final_0.pdf

Tardy, Thierry. 2018. "*The European pillar of NATO, What French leadership?"*, Jacque Delors Institute – Policy Paper, DGRIS, Accessed at 04 02 2026. https://institutdelors.eu/content/uploads/2025/06/Note_de_consultance_Pilier_europeen_OTAN_Tardy_EN_2.pdf