Reform of the National Defense Mechanisms in the Context of the Dynamics of the International Security Environment: A Triangulated Analysis and Comparative Case Studies

Sorin TOPOR
National Institute for Research and Development in Informatics - ICI Bucharest
sorin.topor@ici.ro

Abstract: This paper critically and comprehensively analyzes the need for a profound reform of the national defense mechanisms, in an international context characterized by strategic instability, hybrid threats supported by state and non-state actors, global volatility and unpredictability. The applied methodology is based on the triangulation between three major sources: official strategic documents (example: NATO Strategic Concept 2022, National Defense Strategy of Romania 2020-2024), academic analyses and empirically validated case studies from Poland, Estonia and Israel. The article argues that an effective defense in the digital age goes beyond the modernization of equipment, involving the development of cyber capabilities, institutional reform, strategic adaptability and the active participation of civil society. ENISA and DNSC data reveal that Romania faces thousands of cyber-attacks annually, and 60% of them target critical infrastructures. Therefore, strengthening cyber defense and forming a culture of digital security become imperative. Case studies demonstrate the superior resilience of the states that have invested in these areas as a priority.

In addition, the paper proposes empirically validated reform directions, including adapting military doctrines to new types of conflict, digitizing defense infrastructures, institutional reorganization, and intensifying international cooperation through strategic partnerships. Thus, based on the operational reality and international best practices, case studies from Ukraine, Estonia, Poland, and Israel identify the main directions and propose some recommendations for stimulating innovation and research in the defense industry, for revising the strategic reserve preparation system, and for developing an integrated national security mindset.

Keywords: military reform, national security, hybrid warfare, cybersecurity, societal resilience, triangulation

https://doi.org/10.54851/v7i2y202506

INTRODUCTION

The international geopolitical evolution indicates an accelerated transition towards an unstable multipolar order, characterized by an unequal redistribution of power, an increasingly aggressive ideological and military revisionism, as well as a proliferation of asymmetric threats. In this context of uncertainty and volatility, the traditional national defense mechanisms are no longer effective in guaranteeing the security of a state. The paper critically argues for the need for a fundamental reform of the national defense, going beyond the classical security paradigm, through an integrative reconfiguration, adapted to the hybrid realities of a modern conflict.

The analysis is based on the triangulation of data from three sources: (1) official strategic documents (e.g. National Defense Strategy 2020-2024, NATO Strategic Concept 2022), (2) academic studies and international reports (RUSI, CSIS, ENISA, GCSP), and (3) comparative statistical data from institutions such as Eurostat, NATO, DNSC, and the World Bank. Case studies (Estonia, Israel, Poland, Ukraine) provide empirical evidence on the effectiveness of cyber and societal defense strategies, analyzed not only from a descriptive perspective, but also from a critical-reflexive perspective. For example, according to ENISA (2024), the cyber-attacks on the European critical infrastructures (energy and health) increased by 45% in the period 2022-2024. Also, over 70% of the defense exercises organized by NATO in 2023 included a cyber component. These data emphasize that the success in the face of new threats does not come exclusively from the military equipment, but also from a national security ecosystem that combines population training, infrastructure digitalization, societal resilience and doctrinal adaptation of the armed forces. An eloquent example is Estonia, which, after the 2007 cyber-attacks, implemented a unique integrated civil cyber defense system (Cyber Defense League), demonstrating the capacity of a small state to innovate in defense. Previous studies, in general, tend to approach the subject of the defense or security reform in the context of hybrid threats, but often do so from a fragmented perspective, specific to the scientific fields, predominantly focused on the conventional military dimension, without interconnecting them in a unified strategic framework. Thus, by critically assessing Romania's capacity to manage these emerging risks, data triangulation allows for a complete and interconnected picture of all the essential areas for an effective defense in the context of complex hybrid threats. Expanding the understanding of the defense reform beyond the classical military paradigm emphasizes the fundamental importance of the societal resilience and the active participation of the civil society as an integral part of the national defense mechanisms.

THE SCIENTIFIC RESEARCH METHOD AND WORKING HYPOTHESES

This paper adopts a qualitative documentary analysis approach, with empirical validation, specific to the qualitative investigations in the socio-political field, with an emphasis on data triangulation to ensure the validity and depth of the analysis. Over 150 relevant sources have been analyzed, addressing aspects in the fields of national defense, recent developments in contemporary conflicts and legislative initiatives in the field of security.

Triangulation, in this context, involves the use of three independent and complementary data sources, which converge to validate the hypotheses and provide a complete picture of the phenomenon studied. These sources are:

(1) Official strategic documents and national and international defense policies (e.g. the National Defense Strategy of Romania, NATO and EU documents, ENISA, OECD reports, etc.). They provide the doctrinal framework and official policy directions in the fields of defense and security;

(2) Academic analyses and security studies from specialized literature, in the internationally peer-reviewed publications and research reports from think-tanks (e.g. RUSI, CSIS, ENISA, GCSP), such as Global Studies Quarterly, Journal of Conflict Resolution, Romanian Cyber Security

Journal, etc. This component provides the theoretical foundation and current academic perspectives on the defense reform.

(3) Current quantitative and statistical data on the defense budgets, cybersecurity incidents, the structure of the armed forces, the degree of digitalization of the critical infrastructures, etc. such as Eurostat, NATO, DNSC, the World Bank. These data provide a solid empirical basis for arguing and validating the hypotheses.

Combining these sources allows for a multidimensional analysis, reducing the interpretation bias and increasing the robustness of the conclusions.

The working hypotheses guide the research and are tested throughout the analysis:

- The complexity of the contemporary threats requires a systemic reconstruction that goes beyond the conventional military framework and involves institutional, digital, educational and societal cohesion transformations.
- The states that strategically invest in the cyber capabilities and digital infrastructure demonstrate an increased resilience to the challenges of the modern, hybrid and asymmetric warfare, compared to those that remain dependent on the logic of the traditional militarism.
- The membership in international alliances (NATO, EU, etc.) is a necessary but not sufficient condition for guaranteeing the national security; vulnerabilities persist without deep internal reforms and the development of own capabilities in terms of cyber and societal security.
- Civil society, education and security culture are essential pillars of the national defense, contributing decisively to state resilience in the face of propaganda, disinformation and cognitive warfare.

Preliminary supporting data for triangulation:

- According to the ENISA Threat Landscape 2024 report, over 60% of the cyberattacks on Europe were associated with state-sponsored entities (mainly from Russia, China and Iran), targeting government institutions and critical infrastructure.
- According to the Estonia was ranked first in the EU in terms of cyber resilience (score 92.4/100), CSIS Global Cybersecurity Index, in 2024, while Romania is ranked 177th (score 71.3/100).
- According to the official NATO data (June 2025), 21 out of 31-member states increased defense spending above 2% of GDP, but only 7 allocated at least 10% of the budget for cyber capabilities and emerging technologies.

The countries selected in the case studies offer a multidisciplinary perspective on the defense reform, representing examples of complete best stories. By combining these cases, there can be extracted varied and complementary lessons on the military adaptability in war (Ukraine), the cyber resilience and digitalization (Estonia), the rapid and strategic modernization (Poland), the technological innovation and robust reserve (Israel).

The main methodological limitations of the paper relate to the fact that the data selection base does not include a series of interviews with the decision-makers, which may limit the depth of the operational details or internal perspectives that are not published. Although the case studies offer valuable lessons, each country has a specific geopolitical context, and the recommendations for Romania need to be adapted to the national resources, structures and challenges, valid for the current context, forming only strategic directions and not a detailed implementation plan. Therefore, the analysis focuses on the examples of rapid adaptation and does not exhaustively explore the domestic or political challenges that may slow or obstruct reforms in other contexts.

THE GENERAL CONTEXT OF THE CURRENT INTERNATIONAL SECURITY

The accelerated digitalization of the economy has expanded the scope of the cyberattacks, with the potential to cripple government networks, rail network systems, financial institutions, hospitals, and other critical infrastructure

(Ciupercă & Stanciu, 2023). Their impact on a state's defense, previously limited to the strike capability of the conventional weapons, is now profound. These trends are confirmed by the NATO Strategic Concept of 2022, which emphasized that "the world is changing rapidly and not necessarily for the better" (Lindley-French, 2022).

NATO alliance states simultaneously face diverse threats: Russia's aggression in Ukraine, the rise of China as a hegemonic power (military and economic), the persistence of terrorism in Africa and on the periphery of Europe, as well as global challenges generated by the integration of disruptive technologies into the military systems (state and non-state), pandemics, and climate change. These complex factors multiply the risks, testing the resilience of the societies and the essential infrastructures, potentially leading to unfair competition and instability manifested through low-intensity conflicts with regional and global effects.

Furthermore, the involvement of the non-state organizations, organized crime and hacker groups (sometimes state-sponsored, e.g. Sandworm and Fancy Bear, supported by Russia), significantly complicates the process of establishing the aggressor (Centre, 2024), in accordance with the Laws of War. These groups use sophisticated digital tools for cyber and economic espionage, for propaganda and counter-propaganda, as well as for launching ransomware and DDoS attacks, with the aim of undermining the defenses of the adversary. Consequently, the effects of the conventional weapons are amplified by massive cyber campaigns, integrated into hybrid attacks and propaganda campaigns.

In this context, data become strategic targets. Compromising the databases of hospitals, banks or other essential infrastructures can seriously affect the economy of the attacked state, with a major financial and reputational impact on the entire state system, not only the combatant forces. The globalization of the cyberattacks and their anonymous nature make it extremely difficult to identify the perpetrators, who speculate on any legislative gaps and the lack of harmonization of the international and national legal frameworks. It is worth noting that not only state institutions are targeted, but also citizens, through disinformation campaigns, online fraud, phishing, crypto-scams, etc., which facilitate the creation of destabilizing currents of opinion through fake news, deep fakes and hostile propaganda.

The critical analysis of the main developments generating conflict allowed the establishment of the following dimensions:

The transition from unipolarism to competitive multipolarism

The reconfiguration of the world order in the last two decades has been characterized not only by a change in the geopolitical paradigm, but also by a functional erosion of the multilateral institutions (UN, OSCE, WTO), unable to prevent or effectively manage the emerging conflicts. After a period of relative American hegemony post-Cold War, we are witnessing a rise of China, revisionist actions of the Russian Federation and other regional powers that challenge liberal international norms and promote authoritarian models, based on regional dominance and strategic autonomy.

China has become the main strategic competitor of the US, from economic, military and technological perspectives. Initiatives such as the Belt and Road, military expansion in the South China Sea, the accelerated development of cyber and space capabilities, along with the consolidation of authoritarian domestic policies, position China as an essential actor in the new global security equation. For example, China allocated over 224 billion USD for its military budget in 2024 (SIPRI, 2025), becoming the second largest global spender, surpassing NATO as a consolidated block. The expansion of the digital and space influence, the massive investments in emerging military technologies (AI, quantum computing, electronic warfare, etc.) reflect an agenda of a global technological hegemony.

The Russian Federation openly challenges the liberal international order, directly engaging

in aggressive actions in the post-Soviet space, in Syria, in African countries and, particularly, in the Western Balkans (the case of the War in Ukraine). In its destabilizing actions, Russia acts as a strategic destabilizer by using hybrid means for disinformation and information manipulation, for cyber-attacks (Jones, 2025) and for supporting authoritarian regimes. According to Jones (CSIS, 2025), approximately 45% of the cyberattacks attributed to Russia in 2023-2024 targeted critical infrastructures in the EU, NATO, and Ukraine.

At the same time, states such as India, Iran, Turkey (Ionova, 2025), and Brazil are seeking to redefine their role in shaping the new international order, demonstrating a more active involvement in implementing strategies and policies that are not always aligned with the West European vision. All these dynamics are taking place against the backdrop of a crisis in the multilateral system (UN, World Trade Organization, Human Rights Council), which is facing a series of political deadlocks, especially at the Security Council level, undermining the international community's ability to respond effectively to new types of threats (von Hippel, 2024). The emergence of alternative non-West European cooperation structures (BRICS, Shanghai Cooperation Organization and AUKUS) offers alternative platforms for cooperation, a fragmentation of the international architecture, the formation of multiple centers of geopolitical power, accentuating global dissensions and weakening the consensus on the collective security norms (Bunskoek, & Verburg, 2025).

In this context, small and medium-sized states, such as Romania, face increased pressure to adapt their defense and security strategies to an unpredictable international environment. Their ability to manage these challenges and protect their national interests depends on doctrinal agility, technological innovation and strengthening internal resilience. Therefore, the concept of defense must be reassessed and expanded to include not only military force, but also cyber, economic, social and diplomatic capabilities.

The persistence of the Russian-Ukrainian conflict – a laboratory of hybrid warfare and the redefinition of NATO doctrine

The Russian military aggression against Ukraine, launched in February 2022, represents not only a flagrant violation of the international law, but also a strategic turn in the assessment of European security risks. According to NATO data (The Hague Summit, 202), the collective defense spending in Europe increased by 30% in 2023 compared to 2021, signaling a doctrinal reorientation towards territorial defense, deterrence and cyber interoperability.

This confrontation validated the concept of "convergence of warfare" integrating conventional military actions, cyber-attacks, influence operations through social networks, sabotage and energy pressure, as well as attempts to undermine the social and political cohesion of some EU countries. The use of Sandworm, KillNet or Fancy Bear groups confirms the use of hybrid actors in achieving strategic objectives. In 2023-2024, over 160 DDoS and ransomware cyber incidents were attributed to these entities (DNSC, 2025). Its complex and multiple implications led to a significant revitalization of NATO, materialized by increased defense spending, increased troop presence on the eastern flank, and the accelerated accession of Finland and Sweden to NATO. The European Union also assumed an active role in the field of defense, adopting unprecedented sanctions packages against Russia and providing financial and military support for the defense of Ukraine. These developments generated a reconfiguration of international relations on a global scale. The war accelerated geopolitical realignments, determining a rapprochement of Russia with China, especially in the economic sphere, and shaped a repositioning of some states in the Global South towards the West.

This reality forced NATO to redefine its defense doctrine. At the Madrid Summit (2022), the Alliance adopted a new Strategic Concept, recognizing Russia as "the most significant and direct threat to the security of Allies, peace and stability in the Euro-Atlantic area". This strategic

document emphasizes the importance of collective defense, societal resilience and cyber capabilities as essential pillars of security, going beyond a strictly military approach.

For Romania, with a long border with Ukraine and on the front line of the confrontation with Russia, this conflict has direct and profound implications. It emphasizes the need to strengthen its defense capabilities in all dimensions (conventional, cyber, information), to develop internal resilience and to continuously adapt to emerging threats, including by intensifying its regional and international cooperation.

The proliferation of hybrid and cyber threats – the fragility of the states in the digital age

Cyberspace has become the fifth operational domain of conflict, alongside air, space, land and maritime (NATO, 2022). The use of emerging technologies – generative AI, deep fake, big data analytics, autonomous drones, hypersonic weapons, nano- and biotechnologies, 5G/10G communications, electronic warfare, etc. – has transformed the modern warfare into a cognitive and informational war, with a focus on undermining the trust in institutions and on social polarization.

Currently, states such as Russia, China, North Korea and Iran are increasingly accused of using cyberattacks on critical infrastructure, government and private institutions (DNSC, 2025), the main objective being the social polarization through propaganda and fake news. The democratic regimes and public trust in institutions are targeted by these means. Moreover, the use of the emerging and disruptive technologies creates new ethical and legal dilemmas. ENISA data (2024) reveal that: 53% of the cyberattacks in Europe in 2023 targeted public administrations and hospitals; 72% of the phishing attacks contained elements of political disinformation, integrated into pre-election influence strategies; Romania reported a 38% increase in attacks on education and the banking systems between 2022-2024. These attacks can disrupt essential services, paralyze critical infrastructures and generate significant economic losses. For example, the Colonial Pipeline attack in the USA (2021) demonstrated the vulnerability of the energy infrastructure, causing a regional fuel crisis, with effects on the national stability.

Thus, it becomes clear that any national defense can no longer be conceived without a robust cyber component, institutionally and doctrinally integrated into all levels of a strategic planning. This involves investments in the cybersecurity technology, education, the formation of a digital security culture among citizens and institutions, as well as an effective transnational cooperation in information exchange and incident response. Romania, with a low rate of digital literacy among the population and an increased vulnerability of critical infrastructures, faces significant challenges in this area (Ciubotă, 2025).

Climate crisis and resource insecurity – conflict multipliers

Although not considered direct security threats, the climate crisis and resource insecurity (water, food, energy) act as a systemic crisis multiplier, destabilizing regions and generating new challenges for national defense and security. Climate change, through extreme phenomena (prolonged drought, floods, violent storms), affects agricultural production, access to drinking water and essential infrastructure. This creates massive migratory pressures and exacerbates social and ethnic tensions (UNSD, 2025). According to Global Studies Quarterly (Cullum, 2024), 60% of the armed conflicts in the last 10 years had a component of ecological insecurity. For example, in sub-Saharan areas, the resource degradation has led to increased ethnic violence and terrorism (Ngcamu, 2023). In Europe, the effects of the climate change are generating tensions in border regions, such as the Western Balkans, where the access to water and energy resources is increasingly contested. Romania must also include the ecological security dimension in its defense strategy, especially in the context of the Danube Delta, energy security and the green transition.

The energy insecurity, determined by the dependence on fossil fuels and price volatility, represents a strategic vulnerability, especially in

the context of the EU's decreasing dependence on Russian gas. Thus, attacks on the energy infrastructure (e.g. gas pipelines, power plants, energy transport infrastructure, etc.), as well as the manipulation of the energy markets, can all be weapons in hybrid conflicts to destabilize a state. In view of these geopolitical, technological and social dimensions that define the current security environment, it can be established that, in the absence of a global consensus on the identification and adoption of innovative mechanisms for cooperation and strategic adaptation, the risk of escalating tensions and global destabilization remains at a considerable level.

For Romania, an agricultural country with an important hydrographic network, these aspects are crucial. Food and energy security are becoming essential components of the national security, requiring proactive adaptation strategies and investments in the green technologies and high-performance irrigation systems (FS, 2023).

CHANGES IN THE NATURE OF WAR AND STUDIES ON THE REFORM OF NATIONAL SECURITY SYSTEMS

War, as a socio-political and military phenomenon, is undergoing a fundamental transformation, from the conventional, interstate model to a hybrid, cybernetic and informational one. In this context, the analysis of the security environment can no longer be carried out exclusively through traditional grids, space and time (Weidmann & Ward, 2010), but through a multidimensional approach, adapted to the current reality. These radical transformations, in which the traditional distinctions between war and peace, civil and military, national and transnational are becoming increasingly difficult to identify, impose other landmarks to characterize this concept, which combine: conventional military force, cyber and electromagnetic attacks, informational and psychological warfare methods, economic and technological sabotage in a concept called „multi-domain operations" (MDO), adopted by NATO in 2022. It emphasizes that current warfare is carried out simultaneously in five environments, namely: physical, cyber, informational, cognitive and climatic. Thus, the rapid progress in emerging and disruptive technologies has shifted the center of gravity from conventional forces to surveillance, anticipation and decision-making, precision strike and communication maintenance capabilities. A concrete example is the use of autonomous drones coordinated by AI in the conflicts in Ukraine and Gaza.

Moreover, in contemporary conflicts, an increasingly reduced number of conventional troops is observed, in favor of information control and the digital operational environment. Cyber attacks target the critical infrastructures of the adversary, potentially affecting it both economically and reputationally, with a particular focus on manipulating the global public opinion (Cirnu, Rotundă, & Vasiloiu, 2023). Therefore, not only states but also non-state actors influence the security environment, and international organizations become essential platforms for cooperation and the generation of coordinated responses «for example: the economic program packages adopted by the EU, the UK, the US and other Western countries against Russia (Gill, 2025), including financial sanctions, trade and energy embargoes, individual and sectoral sanctions, etc.».

According to recent literature (Liang, 2025; GCSP, 2024), the dynamics of the contemporary warfare can only be understood through a systemic approach, which integrates the following dimensions:

- *Military:* development of digitally integrated offensive/defensive capabilities, new deterrence tactics, etc.
- *Cyber:* network defense, data protection, critical infrastructure defense, countering DDoS and ransomware attacks (e.g. EstCERT in Estonia).
- *Informational:* combating disinformation, protecting public opinion (e.g. Israeli Hasbara program for strategic communication).
- *Societal:* involving civilians in resilience (e.g. Estonia – Kaitsellit, Israel – Magen David Adom).

- *Economic:* security of natural resources, limiting strategic dependencies on external resources, critical infrastructure.
- *Climate:* energy security, adaptation to natural crises.

This approach supports a critical and integrative vision, according to which the defense is no longer the exclusive attribute of the army but a coordinated national ecosystem. For example, in addition to forms of a hybrid attack, the conditions of the rapid degradation of the pandemic and climate security situation can seriously affect the response capacities of the public health systems and the international solidarity mechanisms. Under such conditions, no state can be considered immune to external threats. Therefore, the international organizations such as NATO, UN, EU have become essential platforms for cooperation and coordinated responses to new types of threats (Youngs, Farinha, Linke, & Wetterwald, 2024).

In order to validate the hypotheses and provide concrete examples of good practices in the defense reform, the paper analyzes case studies, practical actions, and effective initiatives from the countries that have faced similar challenges. These include Ukraine, Estonia, Poland, and Israel, offering unique perspectives on how states can build resilience and digital defense capacity:

a) The Russian-Ukrainian conflict – resistance and transformation under the fire of war

This conflict is the most eloquent scenario of an accelerated defense adaptation in a context of full-scale conflict. Ukraine has also benefited from massive support from the global private sector, especially technology companies (e.g. Starlink/SpaceX, Microsoft, Google, Amazon).

According to CSIS (2025) and ENISA (2024):

- Ukraine neutralized over 2000 cyberattacks in the first 18 months of the war, many targeting energy and banking infrastructure.
- Implementation of rapid partnerships with the private sector (e.g. Microsoft, Palantir, AWS) allowed the protection of government data and critical networks by migrating to a secure cloud.
- It developed an ecosystem of „cyber resistance", including the involvement of civilian hackers in the national defense (e.g. IT ARMY of Ukraine).

Russia, on the other hand, exploited massive disinformation on social media, cyberattacks on Ukrainian infrastructure, and economic and energy pressures on Europe, illustrating the convergence of traditional and new methods. The conventional fighting in the Donetsk, Zaporozhye, Kherson, and Kursk regions was supported by cyberattacks and information maneuvers, below the classical threshold of war, such as cyber-orchestrated power outages and media-induced panic attacks (Brusylovska, 2025).

b) Estonia – pioneer in cyber defense and societal resilience

Estonia is a remarkable case study in strengthening an own national security through strategic digitalization and e-government. The country has reorganized its defense in an innovative style, emphasizing the concept of total defense. Aware that a digital governance brings new risks and vulnerabilities (illustrated in the 2007 cyberattack attributed to Russian hackers, which temporarily paralyzed banks, government institutions, and media, etc.), Estonia has implemented several measures, including:

- Established the Estonian Cyber Defense League in 2011 - the world's first voluntary cyber army working closely with the Ministry of Defense and the armed forces (Kaitseliit, 2007).
- Implemented a government cloud backup system (cloud embassy in Luxembourg) and digital identity cards, becoming a model of resilient digital governance.
- According to ENISA and Kaitseliit (2024):
  - 78% of citizens are familiar with digital hygiene rules and can identify phishing attacks.
  - Estonia organizes over 100 Cyberwar Games simulations annually (McLaughlin, 2022).
  - The cyber defense budget increased by 40% between 2020-2024.

Estonia has developed educational programs on online security to strengthen a culture of digital vigilance (Vevera & Vasiloiu, 2024), has

maintained compulsory military service for men (for women it is voluntary), and offers every citizen the opportunity to participate in periodic military training for the defense of the country. Due to its proximity to Russia, Estonia has facilitated the formation of voluntary paramilitary structures such as the Kaitseliit Defense League, composed of thousands of members involved in civic defense programs, established plans for continuing governance in the event of invasion or attack, developed programs to counter hybrid disinformation operations of the Russian services and strengthened the collaboration with the Russian-speaking community.

Estonia validates the hypothesis that cyber measures and civic engagement are multiplier factors of national resilience, even for small states.

c) Poland - accelerated reform in multiple directions

Poland reacted strategically to the regional security crisis, adopting, a new Defense Concept of the Republic of Poland in 2017, considering that any military conflict in its geographical region cannot be considered marginal or improbable (Paszewski, 2024). Russia's invasion of Ukraine (2022) amplified the perception of the threat and accelerated Poland's decisions to invest massively in defense, transforming it into one of the most important contributors to the security of NATO's eastern flank.

Poland has developed and strengthened its defense and security mechanisms, mainly in the following directions:

- Adoption of the National Defense Law in 2022, which provides for the allocation of 4% of GDP for defense.
- Establishment of the Cyber Command, a unit dedicated to offensive and defensive cyber defense.
- Launching a national military digital literacy program (Cyber-Mil) for 50,000 reservists.
- Civic engagement through training of the Territorial Forces and organizing local exercises in collaboration with schools, hospitals and critical infrastructure companies.

Poland shows that the synergy between military doctrine, technological capabilities and societal mobilization is a viable model for Central Europe.

d) Israel – a model of integrated societal security and military innovation

Since its formation in 1984, Israel has had to deal with threats from its neighbors and terrorist/extremist structures. In this context of national insecurity, it has reformed its defense system, developing a unique security culture, in which the entire society is involved. Israel maintains mandatory military service for most young people (including women), a continuous training program for reservists to maintain and develop military skills, as well as a rapid mobilization system.

The result is a latent, efficient military system that integrates the most advanced examples of defense, cybersecurity, and civil society involvement:

- The Iron Dome system is supported by a digital ecosystem of real-time detection and command.
- Unit 8200 (Cyber-Intelligence) is constantly developing offensive and defensive applications in the field of cybersecurity. It is recognized for transferring innovations to the private tech sector.
- Israel organized over 350 civil defense exercises in 2024, simulating missile and cyber-attacks (Heianut, 2024).
- Israel allocates 5.2% of GDP to defense, of which 18% is for digital technologies and military AI (World Bank, 2023). Massive investments in military research and development have transformed it into a center of innovation in areas such as drones, missile and anti-missile systems, artillery shells, electronic warfare and cyber systems.

In fact, personnel who complete the internship in Unit 8200 subsequently contribute to the creation of start-ups in the field of technology, strengthening the country's innovation ecosystem. Israel demonstrates that a coherent national security culture involves civic education, digitalization and preventive anticipation of threats. Air raid shelters were built/arranged, civilian initiatives that support

the security effort were developed such as organizations that assist law enforcement, medical volunteers, first responders in every region of the country - the Magen David Adom initiative (Heianut, 2024). The effects of these achievements can be observed in the way the war against Hamas (in all its phases) was conducted, in the Gaza Strip, as well as in the 12-day conflict against Iran.

These measures validate the hypothesis that the digital adaptability and public-private collaboration are crucial in the survival of a state under hybrid attack.

THE NEED FOR NATIONAL DEFENSE REFORM AND ADAPTATION TO NEW SECURITY CONDITIONS

Under the impact of the profound changes in the security environment (Presidential Administration, 2020), of increasingly diverse, unpredictable and interconnected risks and threats, Romania finds itself between a series of strategic gaps and the need for a system leap. Radical changes in both the geopolitical dimension (multipolarism, regional instability) and the operational dimension (emerging technologies, hybrid threats, cyber and information warfare) require an urgent, not cosmetic, reform of its defense system.

These reforms must go beyond the paradigm of the traditional militarism, moving towards an integrated security strategy, centered on societal resilience, technological innovation and civil-military partnerships.

According to the NATO Report (Hague Summit, 2025):

- Romania reached the threshold of 2.5% of GDP allocated to defense in 2023, but only 8 % of this budget is directed towards cyber capabilities and digitalization, below the European average (12.1%).
- DNSC reported over 2,300 cyber-attacks in 2024 on critical infrastructures, especially transport, energy and health – an increase of 46% compared to 2022.
- Romania is not in the top 10 European countries in the Global Cybersecurity Index (ITU, 2024), being surpassed by countries such as the Czech Republic, Estonia, Poland and Portugal.

These data indicate a systemic deficit, which cannot be correlated through simple budget growth, but through deep reforms, structured in the following directions:

Doctrinal adaptability and digitalization of military response

The national defense must be redesigned to be effective in all environments and battle spaces, by integrating digital and cognitive capabilities into the strategic planning. The armed forces must develop MDO capabilities, coordinated through secure networks, with a C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) infrastructure. The equipment provided must be state-of-the-art, combined with solid cyber capabilities and mechanisms to counter disinformation (NATO, 2022).

Recommended actions:

- Creation of C2 structures interoperable with similar NATO structures (similar to the Polish model).
- Adoption of the JADC2 integrated combat system at the tactical level.
- Development of cyber war gaming programs to test defensive and offensive responses in crisis scenarios.

This modernization requires smart investments. The increase in the resources allocated to defense, both as a result of commitments to NATO (the target of 2% of GDP, increased in the future to 5%, following the decision adopted at the summit in The Hague - June 25th, 2025) (NATO, 2025), and through one's own will to consolidate the defense, must be accompanied by structural reforms for efficiency.

Institutional reform of the defense system

The institutional dimension of the defense reform requires an efficient reorganization for institutional adaptation to the new realities and challenges of the 21st century. This will include

reviewing the military doctrines, improving the decision-making in crisis situations, strengthening the civil-military relationship and creating specialized structures to ensure the response to unconventional threats.

One of the greatest vulnerabilities of the national defense system is institutional inertia, determined by: outdated command structures, rigid bureaucratic procedures and a severe deficit of digital skills. According to a study conducted by the APSA Training Center (Roșu, 2024), in Romania, 29.8% of the state employees have basic digital skills. If we take this figure as a reference, we appreciate that many of the employees of the operational military structures in Romania are not familiar with the standard cyber defense procedures and have not participated in any digital exercises to date.

The main challenges for implementing such a reform are:

- *High initial costs:* the implementation of these technologies requires significant investments in infrastructure, equipment and personnel training. This justifies the increase in the budget allocated to 5% of GDP.
- *Cybersecurity:* the new technologies expose the defense institutions to more sophisticated cyber-attacks. It is crucial to protect the information systems and equipment with advanced security measures and, in general, cybersecurity costs a lot.
- *Institutional culture and resistance to change:* The institutional reorganization and the integration of new technologies may encounter resistance from the personnel or institutional leaders who are less familiar with digitalization and the emerging technologies.

Concrete proposals:

- Review of the training programs in the military academies, with the integration of AI, electronic warfare, big data analysis modules.
- Mandatory annual assessments of digital skills for all military personnel.
- Introduction of the position of Chief Cyber Security Officer in the decision-making departments.

Development of the intelligent military infrastructure and offensive and defensive cyber capabilities

A modern defense system requires not only armament but also integrated digital transformation. Romania must digitize its combat capabilities, logistics and communications through connected, encrypted and attack-resilient equipment.

Examples of implementation:

- Autonomous drone systems for reconnaissance and logistics (similar to those used in Ukraine).
- Intelligent combat systems (combat vehicles, aircraft, missiles, drones, etc., equipped with sensors and IoT devices that transmit data in real time);
- Real-time simulation platforms for joint military operations, interoperable with NATO applications;
- Digitalized weapon systems: fire systems that include advanced software for aiming, control and coordination of the execution of strikes;
- Analysis and early warning centers through AI and Blockchain for detecting cyber-attacks (similar to the Israeli model);
- Top cybersecurity solutions (encryption, blockchain, token, etc.), centralized command and control systems (NATO Command and Control System NC3S, Tactical Operations Center – TOC, Joint All-Domain Command and Control – JADC2 etc.);
- Cyber capabilities for active defense and attack, in a military context, such as: Intrusion Detection System – IDS, high-level firewall, end-to-end encryption, Network Behavior Analysis etc.

Strengthening human resources and combating digital functional illiteracy

As case studies (Estonia, Israel) have demonstrated, without a well-educated and adaptable human force, any technology is ineffective. In Romania, functional illiteracy (estimated at 42% according to PISA, 2022) also has an impact on the defense sector. These may

be people who cannot adequately apply the knowledge acquired to solve problems or make decisions in a concrete context. Often lacking the skills to synthesize information and without a minimum of critical thinking, they cannot extract the essential and accept information without analyzing or verifying it, making emotional decisions, especially in situations that require discernment. In addition, they can become informal leaders and can form or develop currents of opinion that strengthen the resistance to change.

Critical measures:

- High professionalization of the officers through master's and doctorate degrees applied in military sciences and national security;
- International experience exchanges and joint exercises with states with a high degree of digital maturity;
- Promoting an institutional culture of meritocracy, promoting the leadership based on qualitative assessment, not on seniority;
- Effective recruitment and retention systems, psychological support and reintegration programs for veterans and military reservists.

Involving the civil society in the architecture of resilience

As is the case in Israel and Estonia, without a prepared and involved population, the national defense is vulnerable. All citizens of a state play a crucial role in their national defense. Increasing the awareness of security risks requires that every citizen, regardless of the type of institution where they work and their professional position, be informed, educated and empowered in terms of protecting information, digital equipment and critical infrastructure. Digital threats are becoming increasingly sophisticated, ranging from phishing attacks to complex espionage or cyber sabotage operations. Without the adequate awareness, anyone can become a vulnerable point in the security chain.

In Romania, the level of security education is fragmented, without coherent programs at the pre-university or community level. Participation in community resilience programs can be a strategic national direction not only for military structures. These involve close collaboration between the military structures, local authorities, civic organizations and the private sector to protect the critical infrastructures and maintain the essential functionality of the entire society. Their effects will contribute significantly to increasing the capacity of the civil society to deal with crises and attacks on the critical infrastructures.

Civic education in the security culture aims to train a citizen aware of his rights and responsibilities in a democratic state, as well as his role in the civil defense, the protection of the constitutional values and national sovereignty. The main forms of citizen involvement in the civil defense initiatives are volunteering in civil protection structures, supporting education, from the youngest ages, on the response to disaster situations and attacks, the correct use of alerting and informing applications for the population, community initiatives for logistical support for crisis situations and emergency aid, etc. All these exercises complement the response capabilities of the armed forces, which can focus on the military component, leaving the population ready to provide logistical and humanitarian support.

Priority recommendations:

- Introduction of national and digital security courses in high schools and universities.
- Creation of a national volunteer program for civil defense, similar to Kaitseliit (Estonia).
- Integrated civic exercises (with hospital, schools, city halls), to simulate cyber crises, attacks or disasters.

CONCLUSIONS AND RECOMMENDATIONS

The reform of the national defense mechanisms is no longer an optional strategic objective, but a sine-qua-non-condition for state survival and the defense of a democratic order, in a century marked by instability, global fragmentation and multi-domain hybrid warfare. Empirical data, case studies and validations through triangulation

unequivocally support the hypotheses initially formulated and indicate clear directions of action for Romania.

Hypothesis 1: The complexity and fluid nature of the contemporary conflicts require a profound reform of the national defense – it is confirmed by the convergence of the new types of threats and the inadequacy of the current defense structure. Romania continues to operate on a military institutional architecture that does not fully integrate technology, the digital space and the logic of rapid response. The example of Poland underlines the importance of an accelerated and strategic military modernization, but this modernization must be part of a broader package, with priority investments in cybersecurity (the example of Estonia). In addition, the analysis of the security context (especially in Israel) reveals the flexibility, agility and strategic adaptation capacity of the institutions involved in national defense and security, a crucial aspect for maintaining the sovereignty and democracy of the state.

Hypothesis 2: States that invest strategically in a digital infrastructure and cyber capabilities demonstrate significantly superior resilience – validated by the examples of Estonia, Israel and Poland, which have adopted concrete measures: government cloud, voluntary cyber armies, digitalization of the military equipment and involvement of the civil society in defense exercises. In Romania, the development of cyber must become an absolute priority of the defense (the Estonian and Israeli model), the correlation of the strategic investments in specific infrastructure forming not only a consolidation of the resilience of the critical infrastructures but also an extended culture of digital security at the societal level, where risk awareness and good digital hygiene practices become a collective responsibility.

Hypothesis 3: Integration into alliances does not automatically guarantee the national security – Romania is a member of NATO and the EU, but remains vulnerable to cyber-attacks, lacking an implemented MDO doctrine, with a low degree of digital interoperability and a weak culture of response to hybrid crises. These threats target the internal resilience of a state, the economy, civil society and critical infrastructure, for which no alliance represents a deterrent to internal undermining. Case studies reveal that the basis of resilience is national, and the bridging of the societal resilience deficiencies is achieved only through dedicated national efforts, underlining the importance of aligning the burden sharing concept, established in the NATO Strategic Concept (2022). In addition, the lack of adequate national capabilities can generate particular vulnerabilities for other allied states.

Hypothesis 4: The civil society plays a crucial role in the national defense – supported by data on volunteer participation in Estonia and Israel, as well as NATO/ENISA analyses, which show that human errors (poorly informed citizens, lack of digital vigilance etc.) generate over 60% of the cybersecurity vulnerabilities. The experiences of Ukraine, Estonia and Israel provide clear examples of a holistic approach to defense. This means that the responsibility for security does not belong exclusively to the military, but is shared with the civilian institutions, the private sector and the ordinary citizens. In Romania, the civic education, based on defense training programs and teaching citizens to identify and counter hybrid threats (disinformation, cyberattacks) will represent a pillar of the national resilience, along with civil society involvement in territorial defense exercises, to strengthen the deterrence and response capabilities to hybrid threats.

Strategic recommendations:

- Doctrinal redefinition of defense by integrating the cyber, information and climate dimensions.
- Accelerated digitalization of the military infrastructure, communications and equipment (autonomous systems, AI, advanced encryption etc.).
- Professionalization and continuous training of the military personnel in emerging technologies and cyber operations.
- Creation of a national cybersecurity ecosystem, with public-private participation, interoperable with NATO standards.

- Active involvement of the population in the civil defense - through security education, volunteering and community exercises.
- Increase the budget for the digital defense to at least 15% of the DoD budget, not the average of the advanced NATO states.

We conclude that Romania cannot afford to approach a defense reform as a bureaucratic or reactive process. In a world where weapons are not only physical, but also digital, cognitive and ecological, the only viable option is the profound transformation of the state towards an intelligent, integrated and anticipatory defense. Thus, security will not be the sole prerogative of the army, but the responsibility of a conscious, educated and digitally resilient society.

We believe that this paper fills a specific gap in the existing literature by providing an integrated and holistic analysis of the national defense reform, focused on hybrid threats and the need for societal resilience, using a methodology of triangulating existing data and comparative case studies, with direct implications for the Romanian context.

REFERENCE LIST

Administrația Prezidențială. (2020) *Strategia Națională de Apărare a Țării pentru perioada 2020-2024.* pp. 18-19. https://www.cdep.ro/pdfs/oz/oz20200630/3_strategia.pdf [Accessed 10th June 2025]

Brusylovska, O. (2025) *Russian Narratives of the War in Ukraine 2024.* Odesa, Ukraine: Odesa I.I. Mechinikov National University . doi: 10.61097/29571553/CSU2/165-187

Bunskoek, R. & Verburg, S. (2025) *The BRICS and the Emerging Order of Multipolarity, Clingendael Policy Report, Clingendael & Global Governance in Flux.* https://www.clingendael.org/sites/default/files/2025-05/BRICS_Emerging_Order_Multipolarity.pdf [Accessed 19th July 2025]

Centre, NCSC UK. (2024) *UK and Allies uncover Russian military unit carring out cyber attacks and digital sabotage for the first time.* https://www.ncsc.gov.uk/news/uk-allies-uncover-russian-military-carrying-out-cyber-attacks-digital-sabotage [Accessed 09th July 2025]

Cirnu, C., Rotundă, C. & Vasiloiu, I. (2023) Comparative Analysis on Cyber Diplomacy in EU and US. *Romanian Cyber Security Joural.* 5(1). 77-86. doi:https://doi.org/10.54851/v5i1y202307

Ciubotă, D. (2025) *România are cea mai scăzută rată de competențe digitale de bază, dar investește mai mult în educație și formare profesorilor*, economedia.ro, https://economedia.ro/romania-are-cea-mai-scazuta-rata-de-competente-digitale-de-baza-dar-investeste-mai-mult-in-educatie-si-formarea-profesorilor.html [Accessed 09th July 2025]

Ciupercă, E. & Stanciu, A. (2023) Introducing the Profession of Cybersecurity Specialist for Automated Command-and-control Systems. *Romanian Cyber Security Journal,* 5(1), pp. 3-9. doi:https://doi.org/10.54851/v4i2y202201

Cullum, R. (2024). Making a World of Climate Insecurity: The Threat Multiplier Frame and the US. National Security Community. *Global Studies Quartely.* 4 (4). doi: https://doi.org/10.1093/isagsq/ksae085

DNSC România. (2025) *Știrile săptămânii din cybersecurity* (12.06.2025). *Directoratul Național de Securitate Cibernetică.* https://www.dnsc.ro/citeste/stirile-saptamanii-din-cybersecurity-12-06-2025 [Accessed 09th July 2025]

European Union Agency for Cybersecurity (ENISA). (2024) *Threat Landscape Report*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 [Accessed 09th July 2025]

FS. (2023) *Planul Național Strategic pentru Agricultură și Dezvoltare Rurală, PNS PAC 2023-2027, Echipa Fonduri Structurale*, https://www.fonduri-structurale.ro/programe-operationale/18/planul-national-strategic-pentru-agricul# [Accessed 09th July 2025]

Gill, O. (2025) *UE adopts 177th package of sanctions against Russia. European Commission.* https://romania.representation.ec.europa.eu/news/ue-adopta-cel-de-al-17-lea-pachet-de-sanctiuni-impotriva-rusiei-2025-05-20_ro?etrans=en&etransnolive=1 [Accessed 04th July 2025]

Heianut, M. (2024) *Magen David Adom summarizes 2024 in numbers.* https://www.mdais.org/en/news/311224-numbers [Accessed 09th July 2025]

Ionova, A. (2025) An Isolated Iran Looks to BRICS for Allies, Testing a New World Order. *The New Work Times.* https://www.nytimes.com/2025/07/05/world/americas/iran-brics-summit-rio-de-janeiro.html [Accessed 09th July 2025]

ITU (International Telecommunication Union). (2024) *Global Cybersecurity Index 2024.* https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx [Accessed 09th July 2025]

Jones, G. S. (2025). *Russia's Shadow War Against the West. Center for Strategic & International Studies - CSIS.* https://www.csis.org/analysis/russias-shadow-war-against-west [Accessed 09th July 2025]

Kaitseliit (Estonian Defence League). (2007) *History of the EDL CU.* https://www.kaitseliit.ee/en/history-of-the-edl-cu [Accessed 19th June 2025]

Liang, C. (2025) *Ten lessons from the Russia-Ukraine War.* Geneva: Geneva centre for Security Policy. https://www.gcsp.ch/publications/ten-lessons-russia-ukraine-war [Accessed 20th June 2025]

Lindley-French, J. (2022). *Strategic Concept 2022: Preservig Peace, Protectiv People.* https://www.gmfus.org/news/tag-nato-shadow-strategic-concept-2022-preserving-peace-protecting-people [Accessed 20th June 2025]

McLaughlin, J. (2022) *Estonia host NATO-led cyberwar games, with one eye on Russia, npr*. https://www.npr.org/2022/05/02/1095008257/estonia-nato-cyber-war-games-russia [Accessed 18th July 2025]

NATO. (2022) *NATO 2022 Strategic Concept.* https://www.nato.int/cps/en/natohq/topics_210907.htm [Accessed 08th July 2025]

NATO. (2025) *NATO concludes historic Summit in The Hague.* https://www.nato.int/cps/en/natohq/news_236516.htm [Accessed 09th July 2025]

Ngcamu, B. (2023) Climate change effects o vulnerable populations in the Global South: a systematic review. 118. *Nat Hazards*. doi:https://doi.org/10.1007/s11069-023-06070-2

Paszewski, T. (2024) *Poland defense policy and the coming stormy weather.* Institute of New Europe. https://ine.org.pl/en/poland-defense-policy-and-the-coming-stormy-weather/ [Accessed 21th June 2025]

Roșu, R. (2024) *Sondaj: Un sfert dintre angajați de la stat consideră că au competențe digitale avansate pentru că știu să navigheze pe Internet*. https://www.businessmagazin.ro/actualitate/sondaj-un-sfert-dintre-angajatii-de-la-stat-considera-ca-au-22359821 [Accessed 23th June 2025]

SIPRI. (2025) *Military Expenditure Database 2024.* https://www.sipri.org/databases/milex [Accessed 21th June 2025]

UNSD. (2025) *Recommendations on Statistics of International Migration and Temporary Mobility*, (Draft), United Nations Secretariat, Department of Economic and Social Affairs, Statistics Division. https://unstats.un.org/UNSDWebsite/statcom/session_56/documents/BG-3g-Migration-Recommendations_on_Statistics_of_International_Migration_and_Temporary_Mobility_v1.6-E.pdf [Accessed 21th June 2025]

Vevera, A., & Vasiloiu, I. (2024) E-Goverment in Romania and Estonia: Comparative Analysis and Future Directions. *Romanian Cyber Security Journal,* 6(2), pp. 73-83. doi:https://doi.org/10.54851/v6i2y202407

von Hippel, K. (2024) *Cooperation amid conflict: 5 question for RUSI director-General Karinn von Hippel.* (S. Feigold, Ed.) World Economic Forum LLC. https://www.weforum.org/stories/2024/02/cooperation-amid-conflict-security-rusi-director-general-international/ [Accessed 07th July 2025]

Weidmann, N. B. & Ward, M. D. (2010) Predicting Conflict in Space and Time. *Journal of Conflict Resolution*, 54(6) doi:https://doi.org/10.1177/0022002710371669

World Bank. (2023) *Military expenditure (% of GDP) – Israel*. https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS [Accessed 21th June 2025]

Youngs, R., Farinha, R., Linke, J. & Wetterwald, J. (2024) T*he EU's Triple-Nexus Challenge: Climate, Conflict, Democracy. Carnegie Endowment for International Peace*. https://carnegieendowment.org/research/2024/11/the-eus-triple-nexus-challenge-climate-conflict-democracy?lang=en [Accessed 23th June 2025]